Release Notes for Cisco IOS Release 15.2S

First Published: November 8, 2011
Last Updated: August 16, 2014
Release: Cisco IOS Release 15.2(4)S6
Part Number: OL-26035-03 Rev. H0

Introduction

These release notes support Cisco IOS Release 15.2S up to and including Cisco IOS Release 15.2(4)S6 for the Cisco 7600 series routers. The Cisco ME 3600X switch and the Cisco ME 3800X switch are supported with the release of Cisco IOS Release 15.2(2)S. With Cisco IOS Release 15.2(2)S1, the Cisco ME 3600-24CX switch is supported. The Cisco 7200 and Cisco 7301 routers are supported in Cisco IOS Release 15.2(4)S.

These release notes are updated as needed to describe new features, caveats, and related documents.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

System Requirements

This document describes the system requirements for Cisco IOS 15.2S releases and includes the following sections:

- Feature Support, page 3
- Memory Recommendations, page 4
- Supported Hardware, page 5
- Determining the Software Version, page 6
- Upgrading to a New Software Release, page 6

Feature Support

Cisco IOS software is packaged in feature sets that consist of software images that support specific platforms. The feature sets available for a specific platform depend on which Cisco IOS software images are included in a release. Each feature set contains specific Cisco IOS features.

Caution Cisco IOS images with strong encryption (including, but not limited to 168-bit [3DES] data encryption feature sets) are subject to U.S. government export controls and have limited distribution. Strong encryption images to be installed outside the United States are likely to require an export license. Customer orders may be denied or subject to delay because of U.S. government regulations. When applicable, the purchaser/user must obtain local import and use authorizations for all encryption strengths. Please contact your sales representative or distributor for more information, or send an e-mail to export@cisco.com.

Feature-to-image mapping is available through Cisco Feature Navigator. Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or by feature set (software image). You can compare Cisco IOS software releases side-by-side to display both the features unique to each software release and the features that the releases have in common.

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

www.cisco.com/go/cfn

For help with Cisco Feature Navigator, see the help information at the following URL:

http://www.cisco.com/web/applicat/CFNTOOLS/Help_Docs/help/cfn_support.html

Determining the Software Images (Feature Sets) That Support a Specific Feature

To determine which software images (feature sets) in a Cisco IOS release support a specific feature, go to the Cisco Feature Navigator home page and perform the following steps.

Step 1 From the Cisco Feature Navigator home page, click **Research Features**.

Step 2 Select your software type or leave the field as "All".

Step 3 To find a feature, you can search by either Feature or Technology (select the appropriate button). If you select Search by Feature, you can further filter your search by using the Filter By text box.

Step 4 Choose a feature from the Available Features text box, and click the **Add** button to add the feature to the Selected Features text box.

Note To learn more about a feature in the list, click the **View Desc** button in the Available Features text box.

Repeat this step to add features. A maximum of 20 features can be chosen for a single search.

Step 5 Click **Continue** when you are finished choosing features.

Step 6 In the Release/Platform Tree area, select either your release (from the Train-Release list) or your platform (from the Platform list).

Step 7 The "Search Result" table will list all the software images (feature sets) that support the features that you chose.

Note You can download your results into an Excel spreadsheet by clicking on the Download Excel button.

Determining the Features Supported in a Specific Software Image (Feature Set)

To determine which features are supported in a specific software image (feature set), go to the Cisco Feature Navigator home page and perform the following steps.

Step 1 From the Cisco Feature Navigator home page, click **Research Software**.

Step 2 Select your software type from the drop-down list and chose the **Release** button in the "Search By" area.

Step 3 From the Major Release drop-down list, chose the appropriate major release.

Step 4 From the Release drop-down list, choose the appropriate maintenance release.

Step 5 From the Platform drop-down list, choose the appropriate hardware platform.

Step 6 From the Feature Set drop-down list, choose the appropriate feature set. The Image Details area will provide details on the specific image. The Available Features area will list all the features that are supported by the feature set (software image) that you chose.

Note To learn more about a feature in the list, click the **View Desc** button in the Available Features text box.

Memory Recommendations

To determine memory recommendations for software images (feature sets) in your Cisco IOS release, go to the Cisco Feature Navigator home page and perform the following steps.

Step 1 From the Cisco Feature Navigator home page, click **Research Software**.

Step 2 Select your software type from the drop-down list and choose the **Release** button in the "Search By" area.

Step 3 From the Major Release drop-down list, choose the appropriate major release.

Step 4 From the Release drop-down list, choose the appropriate maintenance release.

Step 5 From the Platform drop-down list, choose the appropriate hardware platform.

Step 6 From the Feature Set drop-down list, choose the appropriate feature set.

Step 7 The Image Details area will provide details on the specific image including the DRAM and flash memory recommendations for each image. The Available Features area will list all the features that are supported by the feature set (software image) that you chose.

Supported Hardware

Cisco IOS Release 15.2S supports the following platforms, including the following models and supervisor engines:

- Cisco 7600 series routers (Cisco 7603-S, Cisco 7604, Cisco 7606, Cisco 7606-S, Cisco 7609, Cisco 7609-S, and Cisco 7613). The Cisco 7600 series routers are not supported with Cisco IOS Release 15.2(4)S3, but are supported with Cisco IOS Release 15.2(4)S3a.
- Cisco ME 3600X switch (introduced in Cisco IOS Release 15.2(2)S)
- Cisco ME 3600X 24CX (introduced in Cisco IOS Release 15.2(2)S1)
- Cisco ME 3800X switch (introduced in Cisco IOS Release 15.2(2)S)
- Cisco RSP720-10GE
- Cisco Supervisor Engine 32, Supervisor Engine 720, Route Switch Processor 720
- Cisco 7200 router (supported in Cisco IOS Release 15.2(4)S)
- Cisco 7301 router (supported in Cisco IOS Release 15.2(4)S)

Cisco 7600 Series Routers

For extensive information about all supported hardware for Cisco 7600 series routers, see the *Guide to Supported Hardware for Cisco 7600 Series Routers with Cisco IOS Release 15S*:

http://www.cisco.com/en/US/docs/routers/7600/Hardware/15_0s/7600_hwd.html

Cisco ME 3800X Switch and ME 3600X Switch

For detailed information about the Cisco ME 3600X switch, see the documents at the following location:

http://www.cisco.com/en/US/products/ps10956/index.html

For detailed information about the Cisco ME 3800X switch, see the documents at the following location:

http://www.cisco.com/en/US/products/ps10965/index.html

See the *Cisco ME 3800X and ME 3600X Switch Hardware Installation Guide* at http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/hardware/installation/guide/me3800x_hig.html

Cisco ME 3600X 24CX Switch

For detailed information about the Cisco ME 3600X-24CX switch, see the documents at the following location:

http://www.cisco.com/en/US/prod/collateral/switches/ps6568/ps10956/data_sheet_c78-708663.html

Cisco 7200 Router

For detailed information about the Cisco 7200 router, see the documents at the following location:

http://www.cisco.com/en/US/products/hw/routers/ps341/index.html

Cisco 7301 Router

For detailed information about the Cisco 7301 router, see the documents at the following location:

http://www.cisco.com/en/US/products/hw/routers/ps352/index.html

Determining the Software Version

To determine the version of Cisco IOS software that is running on your Cisco router, log in to the router and enter the **show version** EXEC command:

```
Router# show version

Cisco Internetwork Operating System Software
IOS (tm) 7600 Software (s72033-ipservices_wan-mz), Version 12.2(33)SRD, EARLY DEPLOYMENT
RELEASE SOFTWARE
```

Upgrading to a New Software Release

For information about choosing a new Cisco IOS software release, see *How to Choose a Cisco IOS Software Release* at the following location:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1834/products_tech_note09186a00800fb9d9.shtml

For information about upgrading the Cisco 7600 series routers, go to the following location:

http://www.cisco.com/en/US/products/hw/routers/ps368/tsd_products_support_install_and_upgrade.html

For information about upgrading the Cisco ME 3600X switch, go to the following location:

http://www.cisco.com/en/US/products/ps10956/tsd_products_support_install_and_upgrade.html

For information about upgrading the Cisco ME 3800X switch, go to the following location:

http://www.cisco.com/en/US/products/ps10965/tsd_products_support_install_and_upgrade.html

For information about upgrading the Cisco 7200 router, go to the following location:

http://www.cisco.com/en/US/products/hw/routers/ps341/tsd_products_support_install_and_upgrade.html

For information about upgrading the Cisco 7301 router, go to the following location:

http://www.cisco.com/en/US/products/hw/routers/ps352/tsd_products_support_install_and_upgrade.html

For Cisco IOS upgrade ordering instructions, go to the following location:

http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/957_pp.htm

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Limitations and Restrictions

This chapter describes limitations and restrictions in Cisco IOS 15.2S releases.

Limitations and Restrictions in Cisco IOS Release 15.2(4)S6

There are no new limitations and restrictions in Cisco IOS Release 15.2(4)S6.

Limitations and Restrictions in Cisco IOS Release 15.2(4)S5

There are no new limitations and restrictions in Cisco IOS Release 15.2(4)S5.

Limitations and Restrictions in Cisco IOS Release 15.2(4)S4

There are no new limitations and restrictions in Cisco IOS Release 15.2(4)S4.

Limitations and Restrictions in Cisco IOS Release 15.2(4)S3a

There are no new limitations and restrictions in Cisco IOS Release 15.2(4)S3a.

Limitations and Restrictions in Cisco IOS Release 15.2(4)S3

There are no new limitations and restrictions in Cisco IOS Release 15.2(4)S3.

Limitations and Restrictions in Cisco IOS Release 15.2(4)S2

There are no new limitations and restrictions in Cisco IOS Release 15.2(4)S2.

Limitations and Restrictions in Cisco IOS Release 15.2(4)S1

There are no new limitations and restrictions in Cisco IOS Release 15.2(4)S1.

Limitations and Restrictions in Cisco IOS Release 15.2(4)S

There are no new limitations and restrictions in Cisco IOS Release 15.2(4)S.

Limitations and Restrictions in Cisco IOS Release 15.2(2)S2

There are no new limitations and restrictions in Cisco IOS Release 15.2(2)S2.

Limitations and Restrictions in Cisco IOS Release 15.2(2)S1

There are no new limitations and restrictions in Cisco IOS Release 15.2(2)S1.

Limitations and Restrictions in Cisco IOS Release 15.2(2)S

There are no new limitations and restrictions in Cisco IOS Release 15.2(2)S.

Limitations and Restrictions in Cisco IOS Release 15.2(1)S2

There are no new limitations and restrictions in Cisco IOS Release 15.2(1)S2.

Limitations and Restrictions in Cisco IOS Release 15.2(1)S1

There are no new limitations and restrictions in Cisco IOS Release 15.2(1)S1.

Limitations and Restrictions in Cisco IOS Release 15.2(1)S

There are no new limitations and restrictions in Cisco IOS Release 15.2(1)S.

Features and Important Notes for Cisco IOS Release 15.2(4)S

These release notes describe the following topics:

New and Changed Information

This section lists the new hardware and software features supported by Cisco IOS Release 15.2S and contains the following subsections:

New Hardware Features in Cisco IOS Release 15.2(4)S6

There are no new hardware features in Cisco IOS Release 15.2(4)S6.

New Software Features in Cisco IOS Release 15.2(4)S6

There are no new software features in Cisco IOS Release 15.2(4)S6.

New Hardware Features in Cisco IOS Release 15.2(4)S5

There are no new hardware features in Cisco IOS Release 15.2(4)S5.

New Software Features in Cisco IOS Release 15.2(4)S5

There are no new software features in Cisco IOS Release 15.2(4)S5.

New Hardware Features in Cisco IOS Release 15.2(4)S4

There are no new hardware features in Cisco IOS Release 15.2(4)S4.

New Software Features in Cisco IOS Release 15.2(4)S4

There are no new software features in Cisco IOS Release 15.2(4)S4.

New Hardware Features in Cisco IOS Release 15.2(4)S3

There are no new hardware features in Cisco IOS Release 15.2(4)S3.

New Software Features in Cisco IOS Release 15.2(4)S3

There are no new software features in Cisco IOS Release 15.2(4)S3.

New Hardware Features in Cisco IOS Release 15.2(4)S2

This section describes new and changed features in Cisco IOS Release 15.2(4)S2. Some features may be new to Cisco IOS Release 15.2(4)S2 but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.2(4)S2. To determine if a feature is new or changed, see the feature information table at the end of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

CISCO7613-S

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/Hardware/Chassis_Installation/7600_Series_Router_Installation_Guide/osr_over.html

Trifecta-ASA

Platform: Cisco 7600

For detailed information about this feature, see the documents at the following URLs:

http://www.cisco.com/en/US/docs/routers/7600/Hardware/15_0s/7600_hwd.html

http://www.cisco.com/en/US/docs/routers/7600/Hardware/Hardware_Guides/7600_Series_Router_Module_Guide/asasm.html

New Software Features in Cisco IOS Release 15.2(4)S2

There are no new software features in Cisco IOS Release 15.2(4)S2.

New Hardware Features in Cisco IOS Release 15.2(4)S1

There are no new hardware features in Cisco IOS Release 15.2(4)S1.

New Software Features in Cisco IOS Release 15.2(4)S1

There are no new software features in Cisco IOS Release 15.2(4)S1.

New Hardware Features in Cisco IOS Release 15.2(4)S

This section describes new and changed features in Cisco IOS Release 15.2(4)S. Some features may be new to Cisco IOS Release 15.2(4)S but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.2(4)S. To determine if a feature is new or changed, see the feature information table at the end of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

8x10G High Density ES+ Line Card for Cisco 7600

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/Hardware/Module_and_Line_Card_Installation_Guides/ES40_Line_Card_Installation_Guide/es40_hw_install_guide.html

12-in-1 Serial SPA Support on Cisco 7600-SIP400

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/76_4xt.html

T1/E1 Support on Cisco ME 3600X-24CS

Platform: Cisco ME 3600X, Cisco ME 3600X-24CX

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_4_S/chassis/configuration/guide/sw_T1-E1.html

New Software Features in Cisco IOS Release 15.2(4)S

This section describes new and changed features in Cisco IOS Release 15.2(4)S. Some features may be new to Cisco IOS Release 15.2(4)S but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.2(4)S. Links to feature modules are included. If a feature listed does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

6PE Support

Platform: Cisco ME 3600X, Cisco ME 3600X-24CX, Cisco ME 3800X

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_4_S/configuration/guide/sw6vpe.html

BFD—BFD Hardware Offload Support

Platform: Cisco ME 3600X, Cisco ME 3600X-24CX

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_4_S/chassis/configuration/guide/swbfd.html

BFD: BGP Multihop Client Support

Platform: Cisco 7200

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/15-2s/irg-multihop-cbit.html

BFD Hardware Offload for Cisco 7600

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URLs:

http://www.cisco.com/en/US/docs/ios/iproute_bfd/configuration/guide/irb_bfd.html

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap4.html

BFD Single Hop Authentication

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bfd/configuration/15-2s/irb-bfd-shop-auth.html

BGP—Add Path

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/15-2s/irg-additional-paths.html

BGP—Attribute Filter and Enhance Attribute Error Handling

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/15-2s/irg-attribute-filter.html

BGP Diverse Path Using Diverse-Path-RR

Platform: Cisco 7200

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/15-2s/irg_diverse_path.html

BGP: Graceful Shutdown

Platform: Cisco 7200

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/15-2s/irg-grace-shut.html

BGP IPv6 Client for Single Hop BFD

Platform: Cisco 7200

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/15-2s/irg-neighor.html

BGP IPv6 PIC Edge and Core for IP/MPLS

Platform: Cisco 7200

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/15-2s/irg_ipv6_pic_edge.html

BGP—mVPN BGP sAFI 129—IPv4

Platform: Cisco 7200

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/15-2s/irg-mvpn-safi.html

BGP—mVPN sAFI 129—IPv6

Platform: Cisco 7200

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/15-2s/irg-mvpn-safi-ipv6.html

BGP—Origin AS Validation

Platform: Cisco 7200

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/15-2s/irg-origin-as.html

BGP Per Neighbor Graceful Restart Configuration

Platform: Cisco ME 3600X, Cisco ME 3600X-24CX, Cisco ME 3800X

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/15-1sg/irg-grace-restart-neighbor.html

BGP RT Constrained Route Distribution

Platform: Cisco 7200

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/15-2s/irg-rt-filter.html

BGP Support for 4-Byte ASN

Platform: Cisco ME 3600X, Cisco ME 3600X-24CX, Cisco ME 3800X

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/15-1sg/irg-4byte-asn.html

BGP Support for Dual AS Configuration for Network AS Migrations

Platform: Cisco ME 3600X, Cisco ME 3600X-24CX, Cisco ME 3800X

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/15-1sg/irg-dual-as.html

BGP Support for IP Prefix Export from a VRF Table into the Global Table

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/15-2s/irg-prefix-export.html

BGP—Unified MPLS iBGP Client

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/15-2s/irg-unif-mpls-ibgp.html

Bidirectional MPLS-TP LSP

Platform: Cisco ME 3600X, Cisco ME 3600X-24CX

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_4_S/configuration/guide/swmp_transport_profile.html

Circuit Emulation over Packet Switched Network

Platform: Cisco ME 3600X, Cisco ME 3600X-24CX

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_4_S/chassis/configuration/guide/swpseudowire.html

Cisco-BGP-MIBv2

Platform: Cisco 7200

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/15-2s/irg-mibv2.html

DHCP—DHCPv6 Guard

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URLs:

http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_dhcp/configuration/15-2s/ip6-dhcpv6-guard.html

http://www.cisco.com/en/US/docs/routers/7600/ios/15S/configuration/guide/IPv6_Security.html

Distributed Frame Relay—Multilink (FRF.16)

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios/wan/configuration/guide/wan_dst_ml_fr.html

Dynamic ARP Inspection

Platform: Cisco ME 3600X, Cisco ME 3600X-24CX, Cisco ME 3800X

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_4_S/configuration/guide/swdynarp.html

EIGRP IPv6 MIBs

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_eigrp/configuration/15-2s/ire-mib.html

EIGRP Loop-Free Alternate Fast Reroute

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_eigrp/configuration/15-2s/ire-ipfrr.html

EVC MIB

Platform: Cisco ME 3600X, Cisco ME 3600X-24CX, Cisco ME 3800X

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_4_S/release/notes/ol27619.html

HSRP Aware PIM

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/ipmulti_pim/configuration/15-2s/imc_hsrp_aware.html

IGMP Snooping

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/ipmulti_igmp/configuration/15-2s/imc_igmp_snoop.html

IKEv2 Site-to-Site

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/15-2s/sec-cfg-ikev2-flex.html

IP Tunnel—SSO Cisco 7600

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap13.html

IPSLA Support for Ethernet Synthetic Loss Measurement in Y1731

Platform: Cisco ME 3600X, Cisco ME 3600X-24CX, Cisco ME 3800X

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_4_S/configuration/guide/swy1731pm.html

IPv6—Destination Guard

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URLs:

http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-2s/ipv6-dest-guard.html

http://www.cisco.com/en/US/docs/routers/7600/ios/15S/configuration/guide/IPv6_Security.html

IPv6 Port Access Control List

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/ios/15S/configuration/guide/Configuring_IPv6_PACL.html

IPv6 Router Advertisement Guard

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URLs:

http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-2s/ip6-ra-guard.html

http://www.cisco.com/en/US/docs/routers/7600/ios/15S/configuration/guide/IPv6_Security.html

IPv6 VPN over MPLS

Platform: Cisco ME 3600X, Cisco ME 3600X-24CX, Cisco ME 3800X

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_4_S/configuration/guide/sw6vpe.html

IPv6 VRF-Aware PBR Next-Hop Enhancement

Platform: Cisco 7200

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/mp_l3_vpns/configuration/15-2s/mp-mltvrf-slct-pbr.html

IS-IS BFD TLV

Platform: Cisco 7200

The IS-IS Bidirectional Forwarding Detection (BFD) Tag Length Value (TLV) feature provides a faster method to detect a loss of an IS-IS adjacency. Before, when an IS-IS adjacency reached the UP state (and therefore could be used for forwarding), a BFD session needed to be established with that neighbor. Now, a BFD session is maintained as long as the hello holddown timer for the neighbor does not expire, which is new for BFD TLV. The BFD session is only deleted if the neighbor hello times out. If BFD signals to IS-IS that a session has gone DOWN, the adjacency associated with that session will transition to DOWN state. Once the BFD session goes back UP, the adjacency state can transition back to an UP state.

For a given IS-IS topology, IS-IS determines if BFD is usable for a given neighbor on that topology. BFD is not usable when BFD is enabled on both sides and the BFD session is down. When there are multiple BFD sessions enabled for different address families, such as IPv4 and IPv6, if BFD is not usable for any address family, then BFD is consider not usable for the entire adjacency on that topology. For example, if both IPv4 and IPv6 BFD are enabled for single topology, if either the IPv4 BFD session is down or IPv6 BFD session is down, the neighbor state will be set to DOWN state. If BFD is not enabled for a given address family, then BFD is considered usable for that address family.

For single topology mode, the neighbor state is down when either the IPv4 or IPv6 BFD session is not BFD usable, that is, if BFD is enabled on both sides and the BFD session is DOWN. If BFD is not enabled on either side, BFD will be set to TRUE. For multi-topology mode, IS-IS adjacency will be in UP state as long as any topology is UP. However, the neighbor for the topology where BFD is consider not usable is considered down for that specific topology. For example, if both IPv4 and IPv6 BFD are enabled, and the IPv4 session is DOWN and IPv6 session is UP, then the IS-IS adjacency is still UP. In this case, the IPv4 neighbor is considered DOWN and ipv6 neighbor is considered UP.

IS-IS IPv6 Administrative Tag

Platform: Cisco 7200

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_isis/configuration/15-2s/ip6-route-isis-adm-tag.html

IS-IS IPv6 Client for BFD

Platform: Cisco 7200

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bfd/configuration/15-2s/ip6-bfd-isis-client.html

ITU-T G.8032 Ethernet Ring Protection Switching

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/cether/configuration/15-2s/ce-g8032-ering-pro.html

L2VPN: PW Status for Static PWs

Platform: Cisco ME 3600X, Cisco ME 3600X-24CX

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_4_S/configuration/guide/swmp_transport_profile.html

L2VPN Static to Dynamic PW Interconnection and PW Preferred Path for MPLS-TP Tunnels

Platform: Cisco ME 3600X, Cisco ME 3600X-24CX

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_4_S/configuration/guide/swmp_transport_profile.html

Low Cost DWDM XFP Support

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/Hardware/15_0s/7600_hwd.html

MPLS TE Static IPv6 Routes Over MPLS TE IPv4 Tunnels

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/mp_te_path_setup/configuration/15-2s/mp-te-static-ipv6-over-ipv4-tunnels.html

MPLS TP: IP-Less Configuration of MPLS TP Tunnels

Platform: Cisco ME 3600X, Cisco ME 3600X-24CX

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_4_S/chassis/configuration/guide/swmp_transport_profile.html

MPLS-TP OAM: Continuity Check via BFD

Platform: Cisco ME 3600X, Cisco ME 3600X-24CX

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_4_S/chassis/configuration/guide/swmp_transport_profile.html

MPLS-TP OAM: GACH

Platform: Cisco ME 3600X, Cisco ME 3600X-24CX

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_4_S/chassis/configuration/guide/swmp_transport_profile.html

MPLS-TP OAM: Ping/Trace

Platform: Cisco ME 3600X, Cisco ME 3600X-24CX

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_4_S/chassis/configuration/guide/swmp_transport_profile.html

MPLS-TP Path Protection

Platform: Cisco ME 3600X, Cisco ME 3600X-24CX

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_4_S/chassis/configuration/guide/swmp_transport_profile.html

MPLS-TP: PW Redundancy for Static PWs

Platform: Cisco ME 3600X, Cisco ME 3600X-24CX

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_4_S/chassis/configuration/guide/swmp_transport_profile.html

MPLS VPN—L3VPN over GRE

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URLs:

http://www.cisco.com/en/US/docs/ios-xml/ios/mp_l3_vpns/configuration/15-2s/mp-vpn-gre.html

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap6.html

MVPN

Platform: Cisco ME 3600X, Cisco ME 3800X

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_4_Sconfiguration/guide/swmcast.html

MVPNv6

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/ios/15S/configuration/guide/mvpn.html

NTPv4 MIB

Platform: Cisco 7200, Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/bsm/configuration/15-2s/bsm-ntpv4-mib.html

OSPF TTL Security Check

Platform: Cisco ME 3600X, Cisco ME 3600X-24CX, Cisco ME 3800X

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_4_S/configuration/guide/swospf_ttl.html

OSPFv3 MIB

Platform: Cisco 7200, Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/configuration/15-2s/iro-ospfv3-mib.html

OSPFv3 NSR

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/configuration/15-2s/iro-ospfv3-nsr.html

OSPFv3 Retransmission Limits

Platform: Cisco 7200, Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/command/iro-cr-book.html

OSPFv3 RFC 3101 Support

Platform: Cisco 7200, Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/configuration/15-2s/iro-cfg.html

OSPFv3 VRF-Lite/PE-CE

Platform: Cisco 7200

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/command/iro-cr-book.html

PIM Allow RP

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/ipmulti_pim/configuration/15-2s/imc_pim_allowrp.html

Policy Based Routing

Platform: Cisco ME 3800X

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_4_S/configuration/guide/swqos.html

SAToP over MPLS

Platform: Cisco ME 3600X, Cisco ME 3600X-24CX

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_2_S/chassis/configuration/guide/swclocking.html

Synchronous Ethernet: ESMC and SSM

Platform: Cisco ME 3600X, Cisco ME 3600X-24CX

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_4_S/chassis/configuration/guide/swclocking.html

Synthetic Frame Loss Measurement

Platform: Cisco ME 3600X, Cisco ME 3600X-24CX

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_4_S/configuration/guide/swy1731pm.html

Table Map QoS Functionality Phase 2

Platform: Cisco ME 3600X, Cisco ME 3600X-24CX, Cisco ME 3800X

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_4_S/configuration/guide/swqos.html

TTL Security Support for OSPFv3 on IPv6

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/configuration/15-2s/iro-ttl-sec-ospfv3.html

UDP-SLB IPv6 Support

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/slb/configuration/15-2s/slb-15-2s-book.html

V2 POS SPA Support on Cisco 7600

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/76ovwpos.html

VPLS over MPLS-TP

Platform: Cisco ME 3600X, Cisco ME 3600X-24CX

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_4_S/configuration/guide/swmp_transport_profile.html

VRRP MIB— RFC2787

Platform: Cisco ME 3600X, Cisco ME 3600X-24CX, Cisco ME 3800X

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_4_S/configuration/guide/swvrrp.html

MIBs

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use the Cisco MIB Locator found at the following URL:

http://tools.cisco.com/ITDIT/MIBS/servlet/index

If the Cisco MIB Locator does not support the MIB information that you need, you can obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

To access the Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

http://tools.cisco.com/RPF/register/register.do

Important Notes

The following sections contain important notes about Cisco IOS Release 15.2S:

- Cisco IOS Behavior Changes, page 25
- Deferrals, page 29
- Field Notices and Bulletins, page 29

Cisco IOS Behavior Changes

Behavior changes describe the minor modifications to the way a device works that are sometimes introduced in a new software release. These changes typically occur during the course of resolving a software defect and are therefore not significant enough to warrant the creation of a standalone document. When behavior changes are introduced, existing documentation is updated with the changes described in these sections.

Behavior changes are provided for the following releases:

- Cisco IOS Release 15.2(4)S3, page 25
- Cisco IOS Release 15.2(4)S2, page 26
- Cisco IOS Release 15.2(4)S1, page 27

Cisco IOS Release 15.2(4)S3

The following behavior changes were introduced in Cisco IOS Release 15.2(4)S3:

- Position of MP_REACH attribute in attributes list of BGP updates.

  Old Behavior: If the BGP Enhanced Attribute Error Handling feature is enabled, BGP places the MP_REACH attribute (attribute 14) at the beginning of the attributes list while formatting an update. If the feature is not enabled, BGP places the MP_REACH attribute at the end of the attributes list, which makes handling a malformed update more difficult for neighbor routers that are doing enhanced error handling.

New Behavior: Whether or not the BGP Enhanced Attribute Error Handling feature is enabled, BGP places the MP_REACH attribute (attribute 14) at the beginning of the attributes list while formatting an update. Enhanced error handling can function much more easily when the MP_REACH attribute is at the beginning of the attributes list.

- The SME default editor behavior is improved.

  Old Behavior: When a command of editor-type editor is configured, the router would copy the default profile to the default editor if the default editor was not modified.

  New Behavior: The editor-type editor command only changes the editor-type but never copies default profiles to default editors. If users want to reuse previous profile configurations, they can use the test sbc profile-to-editor sip which helps to generate editor configurations from the profile.

- Initial INVITE with 0.0.0.0 call flow is supported.

  Old Behavior: Initial INVITE with 0.0.0.0 is not supported unless ACK contains valid a IP address.

  New Behavior: This call flow is supported.

  Additional Information:

  http://www.cisco.com/en/US/docs/ios-xml/ios/voice/sip/configuration/15-mt/voi-sip-rfc.html#GUID-B6E5879A-D5DC-4E2C-BC97-AC927985E10E

- Transmission of IPsec Dummy Packets per RFC 4303

  Old Behavior: IOS devices do not conform to RFC 4303.

  New Behavior: IOS devices conform to RFC 4303 to enable transmitting dummy packets.

  Additional Information:

  Cisco IOS Security Command Reference: Commands A to C
  http://www.cisco.com/en/US/docs/ios-xml/ios/security/a1/sec-a1-cr-book.html

  Cisco IOS Security Command Reference: Commands S to Z
  http://www.cisco.com/en/US/docs/ios-xml/ios/security/s1/sec-s1-cr-book.html

- A new command of sck-pool-size was added to configure the SIP socket control buffer size.

  Old Behavior: SIP calls with TCP control-depleted stub control buffer.

  New Behavior: A new command of sck-pool-size was added to configure the SIP socket control buffer size.

Cisco IOS Release 15.2(4)S2

The following behavior changes were introduced in Cisco IOS Release 15.2(4)S2:

- A new keyword is added to the **hw-module slot** (7600) command.

  Old Behavior: The **mp-recovery-enable** keyword is not available for the **hw-module slot** command.

  New Behavior: The **mp-recovery-enable** keyword is available.

  Additional Information:
  http://www.cisco.com/en/US/docs/ios-xml/ios/interface/command/ir-f1.html#GUID-642623C0-B2E7-4C48-8163-534377F38142

- The NHRP syslog error message includes the IP address of the node where the error originates

  Old Behavior: The NHRP syslog error message does not include the IP address of the node where the error originates, the source NBMA, and the destination address.

  New Behavior: The NHRP syslog error message includes the IP address of the node where the error originates, the source NBMA, and the destination address.

Additional Information: http://cisco.com/en/US/docs/ios-xml/ios/sec_conn_dmvpn/configuration/15-s/sec-conn-dmvpn-tun-mon.html

- A CLI “rtp-media-loop count” is introduced to control the maximum loop count before media packets are dropped.

  Old Behavior: For IP-IP calls, there was no mechanism to limit the number of possible media loops before the media packets are dropped.

  New Behavior: A CLI “rtp-media-loop count” is provisioned globally under voice service voip configuration mode to control the maximum loop count before media packets are dropped.

  Addtional Information: http://www.cisco.com/en/US/docs/ios-xml/ios/voice/vcr3/vcr-r1.html

- The **interworking vlan** command for VPLS is now working.

  Old Behavior: The **interworking vlan** command does not work, which causes traffic failure.

  New Behavior: The **interworking vlan** command is now working. However, you must enter the **clear mpls ldp neighbor *** command before using the **interworking vlan** command the first time.

  Additional Information: http://www.cisco.com/en/US/docs/ios-xml/ios/mp_l2_vpns/configuration/15-s/mp-l2vpn-intrntwkg.html

Cisco IOS Release 15.2(4)S1

The following behavior changes were introduced in Cisco IOS Release 15.2(4)S1:

- The **show aaa servers** command output displays estimated Outstanding/throttled access/accounting transactions.

  Old Behavior: Outstanding access transactions are left unprocessed on RADIUS server.

  New Behavior: The **show aaa servers** command output displays the number of access, authorization, and accounting requests and estimated outstanding/throttled access/accounting transactions that are being processed. The **clear aaa counters servers all** command clears all counters except estimated outstanding/throttled access/accounting transactions. These values will automatically reduce.

  Additional Information: http://www.cisco.com/en/US/docs/ios-xml/ios/security/s1/sec-cr-s2.html#GUID-971F25CD-9424-4B5C-8B64-C344CBA0977D

  http://www.cisco.com/en/US/docs/ios-xml/ios/security/a1/sec-cr-c1.html #GUID-68BC9DC6-282E-4192-A4D1-B9DE80AD26A7

- The **snmp-server enable traps atm snmp-walk-serial** command, which is used to include missing ATM VC SNMP MIB objects of cAal5VccEntry type, is introduced.

  Old Behavior: Some ATM VC SNMP MIB objects of cAal5VccEntry type are not displayed when you use the snmpwalk application.

  New Behavior: The missing ATM VC SNMP MIB objects are displayed.

  Additional Information: http://www.cisco.com/en/US/docs/ios-xml/ios/snmp/command/nm-snmp-cr-book.htm

- BGP Processing of the Removal of Private AS Numbers from AS Path.

  Old Behavior: When the **neighbor remove-private-as** command is configured and a route-map without a continue clause is configured, the processing order is:

  1. neighbor remove-private-as processing

2. set as-path prepend or set as-path prepend last-as

However, if the route-map contains a continue clause, the processing order is reversed.

New Behavior: When the **neighbor remove-private-as** command is configured and a route-map is configured (whether it has a continue clause or not), the processing order is always:

1. neighbor remove-private-as processing
2. set as-path prepend or set as-path prepend last-as

- RTP signal processing is disabled by default.

  Old Behavior: RTP packets of payload type "123" can cause errors on Cisco AS5350 and AS5400 series platforms.

  New Behavior: RTP signal processing is disabled by default to prevent errors caused by RTP packets of payload type "123," and can be enabled when necessary using the **voice-fastpath voice-rtp-signalling enable** command.

  Additional Information: http://www.cisco.com/en/US/tech/tk652/tk653/technologies_tech_note09186a00800a96c1.shtml

- Able to apply VRF transfer for default sessions.

  Old Behavior: Support was not available for applying VRF service on default sessions and for vrf mapping from vrf 1 to vrf 2 for an unclassified IP session. Also, the **show subscriber lite-session** command did not display the "service vrf" field.

  New Behavior: Support is available for applying VRF service on default sessions and for vrf mapping from vrf 1 to vrf 2 for an unclassified IP session. Also, the **show subscriber lite-session** command displays the "service vrf" field.

  Additional Information: http://www.cisco.com/en/US/docs/ios-xml/ios/isg/configuration/xe-3s/isg-wlkby-supp.html

- Cable detection is extended to analog FXSLS, FXSGS, and FXOGS voice ports.

  Old Behavior: Cable detection existed on analog FXOLS voice port only.

  New Behavior: Cable detection is extended to analog FXSLS, FXSGS, and FXOGS voice ports, and a new CLI cable-detect-poll-timer is introduced to configure the cable polling timer value for background polling processes.

  Additional Information: http://www.cisco.com/en/US/docs/ios-xml/ios/voice/vcr1/vcr-c1.html

  http://www.cisco.com/en/US/docs/ios-xml/ios/voice/vcr4/vcr-s9.html #GUID-DDA37612-EDAE-42A4-B84E-1D1D345183B5

- IKEv2 default max in-negotiation CAC counter has been modified to 40.

  Old Behavior: IKEv2 default max in-neg CAC counter was 1000.

  New Behavior: IKEv2 default max in-neg CAC counter has been modified to 40 and is true for all platforms.

  Additional Information: http://www.cisco.com/en/US/docs/ios-xml/ios/security/s1/sec-cr-s3.html

- Old Behavior: ACL based IPv4 port feature can be applied on a trunk port in any mode.

  New Behavior: ACL based IPv4 port feature works only if the trunk port is configured in prefer port mode.

  Impact to customer: ACL based IPv4 port feature works only if the trunk port is configured in prefer port mode. Use the access-group mode prefer port command to configure the trunk port in prefer port mode.

Additional Information: http://www.cisco.com/en/US/docs/routers/7600/ios/15S/configuration/guide/pacl.html

- Missing threshold for logout calls in the queue display.

  Old Behavior: The threshold is missing for logout calls in the queue display. The CLI is **hunt-group logout** [**DND** | **HLog**].

  New Behavior: The **notify** keyword and **threshold** *number* argument are added in the **hunt-group logout** command to enable the indication of the calls in queue for logout agents using the Hlog Programmable Line Key.

  hunt-group logout [**DND** | **HLog** | **notify** | **threshold** *number*]

- Unable to lock out the background settings using the xml append file. Users cannot configure commonProfile xml content and comprise it with the callLogBlfEnabled enabled by "presence call-list".

  Old Behavior: Users cannot configure the commonProfile xml content.

  New Behavior: Introduced the following new CLI to set parameters under commonProfile section in IP phone SEP*.cnf.xml configuration files.

  service profile [phonePassword password | callLogBlfEnabled | backgroundImageAccess false]

- ICMP unreachable configuration for null interfaces is added for Cisco ASR 1000 Routers.

  Old Behavior: If a packet is sent to a null interface, a Cisco ASR 1000 Router does not respond with an ICMP unreachable packet.

  New Behavior: If a packet is sent to a null interface, a Cisco ASR 1000 Router responds with an ICMP unreachable packet.

  Additional Information: http://www.cisco.com/en/US/docs/ios-xml/ios/interface/configuration/xe-3s/ir-cfg-vir-if-xe.html#GUID-64A54530-30B1-43D7-A495-90065902E92D

- A new check compares the Virtual Access ID present in the binding before deleting the binding.

  Old behavior: When a request to free the binding is received the ODAP process searches for the IP and deletes it, due to which active bindings get deleted.

  New behavior: A new check now compares the Virtual Access ID present in the binding before deleting the binding in order to control the issue of duplicate IDs. The s**how ip dhcp server odap-statistics** and **clear ip dhcp server odap-statistics** commands have been introduced as part of this behavior change.

  Additional Information: http://www.cisco.com/en/US/docs/ios/ipaddr/command/reference/iad_book.html

Deferrals

Cisco IOS software images are subject to deferral. Cisco recommends that you view the deferral notices at the following location to determine if your software release is affected:

http://www.cisco.com/cisco/software/advisory.html

Field Notices and Bulletins

- Field Notices—Cisco recommends that you view the field notices for this release to see if your software or hardware platforms are affected. You can find field notices at http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html.

- Bulletins—You can find bulletins at http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/prod_literature.html.

Features and Important Notes for Cisco IOS Release 15.2(2)S

These release notes describe the following topics:

- New and Changed Information, page 31
- MIBs, page 40
- Important Notes, page 41

New and Changed Information

This section lists the new hardware and software features supported by Cisco IOS Release 15.2S and contains the following subsections:

- New Hardware Features in Cisco IOS Release 15.2(2)S2, page 31
- New Software Features in Cisco IOS Release 15.2(2)S2, page 31
- New Hardware Features in Cisco IOS Release 15.2(2)S1, page 31
- New Software Features in Cisco IOS Release 15.2(2)S1, page 32
- New Hardware Features in Cisco IOS Release 15.2(2)S, page 33
- New Software Features in Cisco IOS Release 15.2(2)S, page 33

New Hardware Features in Cisco IOS Release 15.2(2)S2

There are no new hardware features in Cisco IOS Release 15.2(2)S2.

New Software Features in Cisco IOS Release 15.2(2)S2

There are no new software features in Cisco IOS Release 15.2(2)S2.

New Hardware Features in Cisco IOS Release 15.2(2)S1

This section describes new and changed features in Cisco IOS Release 15.2(2)S1. Some features may be new to Cisco IOS Release 15.2(2)S1 but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.2(2)S1. To determine if a feature is new or changed, see the feature information table at the end of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

T1/E1 Support On Cisco ME 3600X-24CS

Platform: Cisco ME 3600X-24CX

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_2_S/chassis/configuration/guide/sw_T1-E1.html

New Software Features in Cisco IOS Release 15.2(2)S1

This section describes new and changed features in Cisco IOS Release 15.2(2)S1. Some features may be new to Cisco IOS Release 15.2(2)S1 but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.2(2)S1. Links to feature modules are included. If a feature listed does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

BFD—BFD Hardware Offload Support

Platform: Cisco ME 3600X-24CX

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_2_S/chassis/configuration/guide/swbfd.html

Circuit Emulation over Packet Switched Network

Platform: Cisco ME 3600X-24CX

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_2_S/chassis/configuration/guide/swclocking.html

Dynamic ARP Inspection

Platform: Cisco ME 3600X, Cisco ME 3600X-24CX, Cisco ME 3800X

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_2_S/configuration/guide/swdynarp.html

MVPN

Platform: Cisco ME 3600X, Cisco ME 3800X

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/ipmulti_mvpn/configuration/15-2s/imc_cfg_mc_vpn.html

SAToP over MPLS

Platform: Cisco ME 3600X-24CX

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_2_S/chassis/configuration/guide/swclocking.html

Synchronous Ethernet: ESMC and SSM

Platform: Cisco ME 3600X-24CX

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_2_S/chassis/configuration/guide/swpseudowire.html

Table Map QoS Functionality Phase 2

Platform: Cisco ME 3600X, Cisco ME 3600X-24CX, Cisco ME 3800X

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_2_S/configuration/guide/swqos.html

New Hardware Features in Cisco IOS Release 15.2(2)S

This section describes new and changed features in Cisco IOS Release 15.2(2)S. Some features may be new to Cisco IOS Release 15.2(2)S but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.2(2)S. To determine if a feature is new or changed, see the feature information table at the end of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

Cisco Catalyst 6500 16-Port 10 Gigabit Ethernet Copper Module with DFC3C (WS-X6716-10GT-3C); Cisco Catalyst 6500 16-Port 10 Gigabit Ethernet Copper Module with DFC3CXL (WS-X6716-10GT-3CXL)

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/Hardware/15_0s/7600_hwd.html

32k PVC Scale with Multipoint Bridging on SIP-400

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/76cfgatm.html

New Software Features in Cisco IOS Release 15.2(2)S

This section describes new and changed features in Cisco IOS Release 15.2(2)S. Some features may be new to Cisco IOS Release 15.2(2)S but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.2(2)S. Links to feature modules are included. If a feature listed does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

32k PVC Scale with Multipoint Bridging on SIP-400

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/76cfgatm.html

802.3ah Enhancements—Dying Gasp on ES+ and Remote Loopback Initiation and Response

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap4.html

Access Switch Device Manager Template

Platform: Cisco ME3600X, Cisco ME 3800X

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_2_S/configuration/guide/swsdm.html

ACL Syslog Correlation

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_data_acl/configuration/15-2s/sec-acl-syslog.html

BFD Support for EIGRP IPv6

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_eigrp/configuration/15-2s/ire-bfd-ipv6.html

BGP—Graceful Shutdown

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/15-2s/irg-grace-shut.html

BGP—iBGP NSR

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/15-2s/irg-nsr-ibgp.html

BGP—mVPN BGP sAFI 129—IPv4

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/15-2s/irg-mvpn-safi.html

BGP NSR Without Route-Refresh

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/15-2s/irg-nsr-autosense.html

Cisco IOS ACL Support for Filtering IP Options

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_data_acl/configuration/15-2s/sec-create-ip-al-filter.html

Control Plane Policing

Platform: Cisco ME 3600X, Cisco ME 3800X

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_2_S/configuration/guide/swcopp.html

DHCP Snooping

Platform: Cisco ME 3600X, Cisco ME 3800X

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_2_S/configuration/guide/swdhcp82.html

DHCPV6 Support

Platform: Cisco ME 3600X, Cisco ME 3800X

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_2_S/configuration/guide/swdhcp82.html

EIGRP IPv6 NSF/GR

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_eigrp/configuration/15-2s/eigrp-ip6-nsf.html

EIGRP Route Tag Enhancements

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_eigrp/configuration/15-2s/ire-en-rou-tags.html

Embedded Event Manager 4.0

Platform: Cisco ME 3600X, Cisco ME 3800X

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_2_S/configuration/guide/sweem.html

Enhanced Route Tags

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_eigrp/configuration/15-2s/ire-en-rou-tags.html

ES+T+XC-20G and ES+T+XC-40G

Platform: Cisco 7600

For detailed information about this feature, see the documents at the following URLs:

http://www.cisco.com/en/US/docs/routers/7600/Hardware/15_0s/7600_hwd.html

http://www.cisco.com/en/US/docs/routers/7600/Hardware/Module_and_Line_Card_Installation_Guides/ES40_Line_Card_Installation_Guide/es40_chap1.html

http://www.cisco.com/en/US/docs/routers/7600/Hardware/Module_and_Line_Card_Installation_Guides/ES40_Line_Card_Installation_Guide/es40_chap2.html

IGMP Snooping over PW

Platform: Cisco ME 3600X, Cisco ME 3800X

For detailed information about this feature, see the documents at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_2_S/configuration/guide/swigmp.html

IGMP Snooping v1, v2, v3 for Aggregated Links and LAG

Platform: Cisco ME 3600X, Cisco ME 3800X

For detailed information about this feature, see the documents at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_2_S/configuration/guide/swigmp.html

IP FRR

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_pi/configuration/15-2s/iri-ip-lfa-frr.html

IP SLAs TWAMP Responder v1.0

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/ipsla/configuration/15-2s/sla_twamp.html

IPv4 Multicast per VRF

Platform: Cisco ME 3600X, Cisco ME 3800X

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_2_S/configuration/guide/swiprout.html

IPv6 ACL Extensions for Hop by Hop Filtering

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-2s/ip6-acl-ext-hbh.html

IPv6 Routing—Unicast Routing

Platform: Cisco ME 3600X, Cisco ME 3800X

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_2_S/configuration/guide/swipv6.html

IPv6 Support for VSPA

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/vspa/configuration/guide/ivmvpn3.html

IRB Multicast

Platform: Cisco ME 3600X, Cisco ME 3800X

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_2_S/configuration/guide/swevc.html

IS-IS—Remote LFA FRR

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_isis/configuration/15-2s/irs-rmte-lfa-frr.html

L2 and L3 QoS ACL Classification for EVC on ES+

Platform: Cisco ME 3600X, Cisco ME 3800X

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_2_S/configuration/guide/swacl.html

L4 Port Match in QoS ACL

Platform: Cisco ME 3600X, Cisco ME 3800X

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_2_S/configuration/guide/swqos.html

MAC Limiting per VFI and BD

Platform: Cisco ME 3600X, Cisco ME 3800X

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_2_S/configuration/guide/swadmin.html

Minimum Link Support for Port Channel

Platform: Cisco ME 3600X, Cisco ME 3800X

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_2_S/configuration/guide/swethchl.html

Multicast Adjacencies Scale Reservation

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/ios/15S/configuration/guide/pfc3mpls.html

Multicast Service Reflection

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/ios/15S/configuration/guide/7600_15_0s_book.html

Object Groups for ACLs

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_object_group_acl.html

OPT-IF-MIB

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/technical_references/7600_mib_guides/MIB_Guide_ver_6/7600mib3.html

OSPF IPv4 Remote Loop-Free Alternate IP Fast Reroute

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/configuration/15-2s/iro-ipfrr-lfa.html

OSPFv3 VRF-Lite/PE-CE

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/command/iro-cr-book.html

PIM Snooping

Platform: Cisco ME 3600X, Cisco ME 3800X

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_2_S/configuration/guide/swsnooppim.html

Routed Pseudowire and Routed VPLS

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/mp_l2_vpns/configuration/15-2s/mp-rt-pw-rt-vpls.html

SSO Support for MPLS-TE Autotunnel-Automesh

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/mp_ha/configuration/15-2s/mp-sso-supp-mpls-te-autotun-automesh.html

Storm Control over EVC

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap4.html

Switch Port Analyzer—Distributed Egress SPAN

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/ios/15S/configuration/guide/span.html

Table Map Support Along with Policers

Platform: Cisco ME 3600X, Cisco ME 3800X

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_2_S/configuration/guide/swqos.html

V6 Security ACL for EVC

Platform: Cisco ME 3600X, Cisco ME 3800X

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_2_S/configuration/guide/swv6acl.html

VRF Aware IPv6 Tunnels over IPv4 Transport

Platform: Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap13.html

Y.1731 MIB Support Through Existing IPSLA MIBs

Platform: Cisco 7600, Cisco ME 3600X, Cisco ME 3800X

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/ipsla/configuration/15-2s/sla_mether3_y1731.html

Y.1731 Performance Monitoring for Cisco ME 3600 and Cisco ME 3800

Platform: Cisco ME 3600X, Cisco ME 3800X

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_2_S/configuration/guide/swy1731pm.html

MIBs

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use the Cisco MIB Locator found at the following URL:

http://tools.cisco.com/ITDIT/MIBS/servlet/index

If the Cisco MIB Locator does not support the MIB information that you need, you can obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

To access the Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

http://tools.cisco.com/RPF/register/register.do

Important Notes

The following sections contain important notes about Cisco IOS Release 15.2S:

- Cisco IOS Behavior Changes, page 41
- Deferrals, page 43
- Field Notices and Bulletins, page 43

Cisco IOS Behavior Changes

Behavior changes describe the minor modifications to the way a device works that are sometimes introduced in a new software release. These changes typically occur during the course of resolving a software defect and are therefore not significant enough to warrant the creation of a standalone document. When behavior changes are introduced, existing documentation is updated with the changes described in these sections.

Behavior changes are provided for the following releases:

- Cisco IOS Release 15.2(2)S2, page 41
- Cisco IOS Release 15.2(2)S1, page 42

Cisco IOS Release 15.2(2)S2

The following behavior changes were introduced in Cisco IOS Release 15.2(2)S2:

- The maximum value for cleanup-delay time that is configured using the mpls traffic-eng reoptimize timers delay cleanup-delay time command to delay the removal of old LSPs after tunnel reoptimization, is changed to 300 seconds.

  Old Behavior: The maximum value for cleanup-delay time that is configured using the mpls traffic-eng reoptimize timers delay cleanup-delay time command, is 60 seconds.

  New Behavior: The maximum value for cleanup-delay time that is configured using the mpls traffic-eng reoptimize timers delay cleanup-delay time command, is 300 seconds.

  Additional Information: http://www.cisco.com/en/US/docs/ios-xml/ios/mpls/command/mp-m4.html#GUID-B64630A1-3CD7-42DE-8E86-6CD47AC8981A

- The metadata service functionality is added to the SAF feature.

  Old Behavior: The metadata service functionality is not available.

  New Behavior: The Cisco SAF Forwarder can send service metadata to its neighbor SAF nodes. Metadata is XML information, and service data is information that a server communicates to a client about itself. The service metadata does not propagate in mixed Cisco IOS Release 15.1(3)S) and Cisco IOS Release 15.2(1)S environments until such time that the version of EIGRP and SAF is upgraded.

Additional Information:
http://www.cisco.com/en/US/docs/ios-xml/ios/saf/configuration/15-2s/saf-15-2s-book.html

- For the Carrier Packet Transport (CPT) system, an alert is displayed whenever a round-trip delay threshold violation occurs during an IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) operation.

  Old Behavior: When a round-trip delay exceeds the specified threshold, an event is sent and IP SLAs generates a notification to the network management application.

  New Behavior: For the CPT system, when a round-trip delay threshold violation occurs during an IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) operation, an alert is displayed in addition to IP SLAs sending a notification. The alert is cleared when the round-trip delay falls back below the specified threshold value.

  Additional Information: http://www.cisco.com/en/US/docs/ios-xml/ios/ipsla/command/sla_i1.html

- Taps on the same stream with different port range is accepted for RP based LI.

  Old Behavior: Taps on the same stream with different port range was rejected.

  New Behavior: Taps on the same stream with different port range is accepted.

  Additional Information:
  http://www.cisco.com/en/US/docs/routers/7600/ios/12.2SR/configuration/lawful_intercept/76LIch2.html

- The default mode for the default transform set is changed to tunnel.

  Old Behavior: The default mode for all transform sets, including the default transform set, is tunnel.

  New Behavior: The default mode for the default transform set is transport; the default mode for all other transform sets is tunnel.

  Additional Information:
  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/15-2s/sec-cfg-ikev2-flex.html

Cisco IOS Release 15.2(2)S1

The following behavior changes were introduced in Cisco IOS Release 15.2(2)S1:

- Changes are made to classification of PADI packets on ATM Auto Virtual Circuits.

  Old Behavior: All packets transmitted over ATM AutoVC are classified using the default class link type.

  New Behavior: PPPoE Active Discovery Initiation (PADI) packets transmitted over ATM AutoVC are classified using the PPPOE_DISCOVERY link type.

  Non-PADI packets continue to be classified using the default class link type. Each ATM cell of a PADI packet is punted as a separate packet, and is counted toward the PPPOE_DISCOVERY packet count.

  The **match protocol pppoe-discovery** command matches all PPPoE control packets that are sent to the control plane including the PADI packets.

  Additional Information:

  http://www.cisco.com/en/US/docs/ios-xml/ios/qos/command/match_access-group_through_mls_ip_pbr.html

- The **mode tunnels** command is disabled by default.

  Old Behavior: PfR automatically creates dynamic tunnels between all border routers.

  New Behavior: Dynamic tunnels are not automatically created between border routers.

Additional Information: http://www.cisco.com/en/US/docs/ios-xml/ios/pfr/command/pfr-h1.html

- For routed ports and switched virtual interfaces (SVIs) that are configured on a Cisco Ethernet switch port, the maximum number of inbound interfaces (IIFs) or outbound interfaces (OIFs) supported is now 128.

  Old Behavior: The maximum number of IIFs or OIFs supported is 64 for any of the following configurations: routed ports or SVIs that are configured on a switch port or for an Ethernet Flow Point (EFP).

  New Behavior: For routed ports and SVIs configured on a switch port, the maximum number of supported IIFs and OIFs is increased to 128.

- Virtual template lock functionality is changed.

  Old Behavior: A virtual template of the type tunnel with cloned virtual access interfaces can be configured. The virtual template dynamically updates the configuration to the cloned virtual access interfaces, thereby causing instability in some scenarios.

  New Behavior: A virtual template of the type tunnel with cloned virtual access interfaces cannot be configured.

  Additional Information:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_vpnips/configuration/15-2s/sec-ipsec-virt-tunnl.html

Deferrals

Cisco IOS software images are subject to deferral. Cisco recommends that you view the deferral notices at the following location to determine if your software release is affected:

http://www.cisco.com/cisco/software/advisory.html

Field Notices and Bulletins

- Field Notices—Cisco recommends that you view the field notices for this release to see if your software or hardware platforms are affected. You can find field notices at http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html.
- Bulletins—You can find bulletins at http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/prod_literature.html.

Features and Important Notes for Cisco IOS Release 15.2(1)S

These release notes describe the following topics:

New and Changed Information

This section lists the new hardware and software features supported by Cisco IOS Release 15.2S and contains the following subsections:

New Hardware Features in Cisco IOS Release 15.2(1)S2

There are no new hardware features in Cisco IOS Release 15.2(1)S2.

New Software Features in Cisco IOS Release 15.2(1)S2

There are no new sofware features in Cisco IOS Release 15.2(1)S2.

New Hardware Features in Cisco IOS Release 15.2(1)S1

There are no new hardware features in Cisco IOS Release 15.2(1)S1.

New Software Features in Cisco IOS Release 15.2(1)S1

There are no new software features in Cisco IOS Release 15.2(1)S1.

New Hardware Features in Cisco IOS Release 15.2(1)S

This section describes new and changed features in Cisco IOS Release 15.2(1)S. Some features may be new to Cisco IOS Release 15.2(1)S but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.2(1)S. To determine if a feature is new or changed, see the feature information table at the end of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

32k PVC Scale with Multipoint Bridging on SIP-400

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/76cfgatm.html

SPA-1xCHOC48-DS3 Support on Cisco 7600-SIP-400

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/sipspasw.html

New Software Features in Cisco IOS Release 15.2(1)S

This section describes new and changed features in Cisco IOS Release 15.2(1)S. Some features may be new to Cisco IOS Release 15.1S but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.2(1)S. Links to feature modules are included. If a feature listed does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

32k PVC Scale with Multipoint Bridging on SIP-400

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/76cfgatm.html

Any Transport over MPLS: ATM Cell Relay over MPLS: Packed Cell Relay

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/mp_l2_vpns/configuration/15-2s/mp-any-transport.html

ATM Port Mode Packed Cell Relay over MPLS

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/mp_l2_vpns/configuration/15-2s/mp-any-transport.html

BGP—Origin AS Validation

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/15-2s/irg-origin-as.html

CISCO-ENTITY-DISPLAY-MIB

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/technical_references/7600_mib_guides/MIB_Guide_ver_6/mibgde6.html

DHCP Snooping over Pseudo-MLACP

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap4.html

DHCPv6—Relay Chaining (for Prefix Delegation) and Route Insertion in FIB

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-2s/ip6-dhcp.html

EIGRP Dual DMVPN Domain Enhancement

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_eigrp/configuration/15-2s/config-eigrp.html

Extensible Messaging Client Protocol 2.0

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/saf/configuration/15-2s/saf-saf.html

Frame Relay Fragmentation

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/76cfgsip.html

GLC-EX-SMD, GLC-ZX-SMD

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/Hardware/15_0s/7600_hwd.html

IPoDWDM Proactive Protection Support for Cisco 7600

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap10.html

IPv6 Policy-Based Routing

For detailed information about this feature, see the documents at the following URLs:

http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-2s/ip6-pol-bsd-rtng.html

http://www.cisco.com/en/US/docs/routers/7600/ios/15S/configuration/guide/IPv6_PBR.html

L2VPN Resilient Pseudowire

For detailed information about this feature, see the documents at the following URLs:

http://www.cisco.com/en/US/docs/ios-xml/ios/mp_l2_vpns/configuration/15-2s/wan-l2vpn-pw-red.html

http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/76cfgatm.html

MPLS TE—Enhanced Path Protection

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_te_path_prot.html

MPLS TE—Interarea Tunnels

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_te_interarea_tun.html

MPLS TE—Inter-AS TE

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_te_inter_as_te.html

MPLS TE—Shared Risk Link Groups

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_te_shared_risk.html

MPLS VPN—L3VPN over GRE

For detailed information about this feature, see the documents at the following URLs:

http://www.cisco.com/en/US/docs/ios-xml/ios/mp_l3_vpns/configuration/15-2s/mp-vpn-gre.html

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_vpn_gre.html

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap6.html

Multichassis LACP IGMP Snooping State Sync

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap4.html

N:1 PVC Mapping to PWE with Nonunique VPI (ATMCOMMON)

For detailed information about this feature, see the documents at the following URLs:

http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/76cfgatm.html

http://www.cisco.com/en/US/docs/ios/atm/configuration/guide/atm_nto1_PVC_map_to_PWE.html

NTPv4 Orphan Mode Support, Range for Trusted Key Configuration

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/bsm/configuration/15-2s/bsm-time-calendar-set.html http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap6.html

Multichassis LACP IGMP Snooping State Sync

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap4.html

N:1 PVC Mapping to PWE with Nonunique VPI (ATMCOMMON)

For detailed information about this feature, see the documents at the following URLs:

http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/76cfgatm.html

http://www.cisco.com/en/US/docs/ios/atm/configuration/guide/atm_nto1_PVC_map_to_PWE.html

NTPv4 Orphan Mode Support, Range for Trusted Key Configuration

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/bsm/configuration/15-2s/bsm-time-calendar-set.html

Point to Multipoint MPLS-TE MIB

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/mp_em_and_mibs/configuration/15-2s/mp-p2mp-mpls-te-mib.html

Synchronous Ethernet: ESMC and SSM

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios/interface/configuration/guide/ir_synce.html

Video Monitoring MIB Support for Medianet Video Monitoring

This feature provides support for the use of the industry-standard Simple Network Management Protocol (SNMP) to monitor media streams. This support is implemented with the addition of the following Cisco proprietary SNMP Management Information Base (MIB) modules:

- CISCO-FLOW-MONITOR-TC-MIB—Defines the textual conventions common to the following MIB modules.
- CISCO-FLOW-MONITOR-MIB—Defines the framework that describes the flow monitors supported by a system, the flows that it has learned, and the flow metrics collected for those flows.
- CISCO-MDI-METRICS-MIB—Defines objects that describe the quality metrics collected for media streams that comply to the Media Delivery Index (MDI) [RFC 4445].
- CISCO-RTP-METRICS-MIB—Defines objects that describe the quality metrics collected for RTP streams, similar to those described by an RTCP Receiver Report packet [RFC 3550].
- CISCO-IP-CBR-METRICS-MIB—Defines objects that describe the quality metrics collected for IP streams that have a constant bit rate (CBR).

For detailed information about these MIBs, and to locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at http://www.cisco.com/go/mibs.

This feature also includes two new CLI commands and one modified CLI command. The commands are as follows:

snmp-server host—Enables the delivery of flow monitoring SNMP notifications to a recipient.

snmp-server enable traps flowmon—Enables flow monitoring SNMP notifications. By default, flow monitoring SNMP notifications are disabled.

snmp mib flowmon alarm history—Sets the maximum number of entries maintained by the flow monitor alarm history log.

For more information about these commands, see the *Cisco IOS Master Command List* at the following URL:

http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html

Voltage Table Support for CISCO-ENVMON-MIB

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/technical_references/7600_mib_guides/MIB_Guide_ver_6/mibgde6.html

VPLS MAC Address Withdrawal

For detailed information about this feature, see the document at the following URL:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_hvpls_npe_red.html

MIBs

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use the Cisco MIB Locator found at the following URL:

http://tools.cisco.com/ITDIT/MIBS/servlet/index

If the Cisco MIB Locator does not support the MIB information that you need, you can obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

To access the Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

http://tools.cisco.com/RPF/register/register.do

Important Notes

The following sections contain important notes about Cisco IOS Release 15.2S:

- Cisco IOS Behavior Changes, page 51
- Deferrals, page 54
- Field Notices and Bulletins, page 54

Cisco IOS Behavior Changes

Behavior changes describe the minor modifications to the way a device works that are sometimes introduced in a new software release. These changes typically occur during the course of resolving a software defect and are therefore not significant enough to warrant the creation of a standalone document. When behavior changes are introduced, existing documentation is updated with the changes described in these sections.

Behavior changes are provided for the following releases:

- Cisco IOS Release 15.2(1)S2, page 51
- Cisco IOS Release 15.2(1)S1, page 52

Cisco IOS Release 15.2(1)S2

The following behavior changes were introduced in Cisco IOS Release 15.2(1)S2:

- Configure "radius-server attribute 44 include-in-access-req all" instead of "radius-server attribute 44 include-in-access-req" if per vrf level attribute inclusion is not required.

  Old behavior: **radius-server attribute 44 include-in-access-req** command applies attribute 44 for all the sessions.

  New behavior: The command is modified to include the configuration of non-vrf sessions.

  Additional information:
  http://www.cisco.com/en/US/docs/ios-xml/ios/security/m1/sec-cr-r1.html#GUID-0C067786-2A4D-4D26-A429-0E7AA331E4CD

- Change in the **cns config retrieve** command.

  Old Behavior: The **cns config retrieve** command accepts an IPv4 or IPv6 address as a source for CNS communications.

  New Behavior: The **cns config retrieve** command does not accept an IPv4 or IPv6 address as a source for CNS communications. Instead, the **source interface** *name* keyword/argument pair is available.

  Additional Information:
  http://www.cisco.com/en/US/docs/ios-xml/ios/cns/command/cns-cr-book.html

- The **sub-application-table** keyword can be enabled in the option command in Flexible NetFlow flow exporter configuration mode.

  Old Behavior: The periodic sending of an options table, which allows the collector to map NBAR subapplication table information, is not enabled.

  New Behavior: The periodic sending of an options table, which allows the collector to map the NBAR subapplication tags, subapplication names, and subapplication descriptions provided in the flow records to application IDs, can be enabled by using the sub-application-table keyword in the option command in Flexible NetFlow flow exporter configuration mode.

  Additional Information:
  http://www.cisco.com/en/US/docs/ios-xml/ios/fnetflow/command/fnf-m1.html

- PfR syslog levels are added to minimize number of messages.

  Old Behavior: There are too many PfR syslog messages.

  New Behavior: PfR syslog levels are added to minimize the number of messages displayed, and a syslog notice is added to display when 30 percent of the traffic classes are out-of-policy.

Additional Information: http://www.cisco.com/en/US/docs/ios-xml/ios/pfr/configuration/15-1mt/pfr-15-1mt-book.html

- New CLI command added to enable/disable BFDv6 and BFDv4 session offloading.

  Old behavior: No CLI command.

  New behavior: **platform bfd disable-offload** added.

  Additional Information: http://www.cisco.com/en/US/docs/ios/iproute_pi/command/reference/iri_pi1.html

Cisco IOS Release 15.2(1)S1

The following behavior changes were introduced in Cisco IOS Release 15.2(1)S1:

- BGP-Origin AS Validation feature is changed in two ways.

  Old Behavior 1: The router may send serial query or reset query messages to an RPKI server at any time.

  New Behavior 1: The router will not send a serial query message or reset query message during the interval between when it sends a serial query or reset query message and when it receives an End of Data (EOD) message. Serial queries in this interval are stripped, and reset queries in this interval are sent upon receipt of the EOD message.

  Old Behavior 2: The Invalid state indicates the prefix is found, but either the corresponding autonomous system received from the eBGP peer is not the autonomous system that appears in the SOVC table or the prefix length in the BGP Update message is longer than the maximum length permitted in the SOVC table. The Not Found state indicates that the prefix is not among the prefixes or prefix ranges in the SOVC table.

  New Behavior 2: The Invalid state indicates that the prefix meets either of the following two conditions:

  1. It matches one or more Route Origin Authorizations (ROAs), but there is no matching ROA where the origin autonomous system matches the origin autonomous system on the AS-PATH.
  2. It matches one or more ROAs at the minimum length specified in the ROA, but for all ROAs where it matches the minimum length, it is longer than the specified maximum length. The origin autonomous system does not matter for condition #2.

  The Not Found state indicates that the prefix is not among the Valid or Invalid prefixes.

  Additional Information: http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/15-2s/irg-origin-as.html

- Change in BGP next-hop for redistributed recursive static routes.

  Old Behavior: A router advertising a locally originated route (from a static route with a recursive next hop) advertises the next hop to be itself. The local next hop (equal to next-hop-self) is kept.

  New Behavior: A router advertising a locally originated route (from a static route with a recursive next hop) advertises the next hop to be the recursive next hop of the static route.

- Switched Virtual Interface (SVI)-based Ethernet over MPLS (EoMPLS) now works with Transport Profiles (TPs).

  Old Behavior: SVI-based EoMPLS did not work for packets over TPs.

  New Behavior: SVI-based EoMPLS now works for packets over TPs.

  Additional Information: http://www.cisco.com/en/US/docs/ios-xml/ios/mp_l2_vpns/configuration/15-1s/mp-any-transport.html

- The IKEv2 profile name must be specified to disassociate it from a crypto map or IPsec profile.

  Old Behavior: The IKEv2 profile name does not need to be specified to disassociate it from a crypto map or IPsec profile.

  New Behavior: The IKEv2 profile name must be specified to disassociate it from a crypto map or IPsec profile.

  Additional Information:
  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/15-2mt/sec-cfg-ikev2-flex.html#GUID-DC2773B6-7E71-43F4-B4E7-25063C7D4851

- A command is added to truncate the downstream ANCP rate.

  Old Behavior: In situations where large number of unique Access Node Control Protocol (ANCP) rates generated result in a correspondingly high number of policy maps, the number of policy maps can exceed the maximum number of policy maps supported on a router.

  New Behavior: Use the **ancp truncate** command to reduce the ANCP rate.

  Caution: This command is to be used only in exceptional scenarios, such as when the number of unique rates generated result in exceeding the maximum number of policy maps supported on a router.

  Additional Information:
  http://www.cisco.com/en/US/docs/ios-xml/ios/ancp/command/ancp-a1.html#GUID-4AB51EAF-C9B7-48EB-A3E4-E18D2A576816

- CLI to tune ratelimit parameter for RP-based LI mode.

  Old Behavior: The command was not present in the command reference guide.

  New Behavior: Updated the command reference guide with the **li-slot rp rate** command.

  Additional Information:
  http://www.cisco.com/en/US/docs/ios-xml/ios/interface/command/ir-l1.html

- Optimization of ACL TCAM entry consumption on the Cisco 7600 platforms for Policy Based Routing under certain circumstances.

  Old Behavior: When configuring multiple PBR sequences (or a single PBR sequence with multiple ACLs) in which more than one PBR ACL contains DENY entries, the result of the merge is suboptimal in the terms of number of TCAM entries and masks used.

  New Behavior: Entering the new **platform ipv4 pbr optimize tcam** command allows for better optimization in the case described.

  Additional Information:
  http://www.cisco.com/en/US/docs/routers/7600/ios/15S/configuration/guide/layer3.html#wp1027016

- Cisco ASR 1000 BDI interface supports MTU size change.

  Old Behavior: The default maximum transmission unit (MTU) size is 1500 bytes and is not configurable.

  New Behavior: For a BDI, a MTU size from1500 and 9216 bytes can be configured.

  Additional Information:
  http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/chassis/bdi.html

- Fast Network Time Protocol (NTP) synchronization is achieved.

  Old Behavior: The burst and initial burst (iburst) modes are enabled manually.

  New Behavior: The burst and iburst modes are enabled by default.

Additional Information:
http://www.cisco.com/en/US/docs/ios-xml/ios/bsm/command/bsm-cr-n1.html#GUID-CC69EFC5-68A3-4C5D-90CD-67DE45D4A370

- The **telecom-solutions** keyword is not supported.

  Old Behavior: The **telecom-solutions** keyword in the **ntp refclock** command allows users to configure the reference clock driver.

  New Behavior: The **telecom-solutions** keyword, along with its options, is visible but cannot be configured.

  Additional Information:
  http://www.cisco.com/en/US/docs/ios-xml/ios/bsm/command/bsm-cr-n1.html#GUID-875B8F64-2179-4F71-8BC0-6BF103EBB22F

Deferrals

Cisco IOS software images are subject to deferral. Cisco recommends that you view the deferral notices at the following location to determine if your software release is affected:

http://www.cisco.com/cisco/software/advisory.html

Field Notices and Bulletins

- Field Notices—Cisco recommends that you view the field notices for this release to see if your software or hardware platforms are affected. You can find field notices at http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html.
- Bulletins—You can find bulletins at http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/prod_literature.html.

Caveats for Cisco IOS Release 15.2(4)S

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats, and only select severity 3 caveats are included in this section.

In this section, the following information is provided for each caveat:

- Symptoms—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.

Note If you have an account on Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com and go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl. (If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)

This section consists of the following subsections:

Using the Bug Search Tool

The Cisco Bug Search Tool enables you to filter the bugs so that you only see those in which you are interested. In addition to being able to search for a specific bug ID, or for all bugs in a product and release, you can filter the open and/or resolved bugs by one or more of the following criteria:

- Last modified date
- Status, such as fixed (resolved) or open
- Severity
- Support cases

For more information about how to use the Cisco Bug Search Tool, including how to set email alerts for bugs and to save bugs and searches, see Bug Search Tool Help & FAQ.

Note You must have a Cisco.com account to log in and access the Cisco Bug Search Tool. if you do not have one, you can register for an account.

To use the Cisco Bug Search Tool:

1. In your browser, navigate to the Cisco Bug Search Tool.
2. If you are redirected to a **Log In** page, enter your registered Cisco.com username and password and then, click **Log In**.
3. To search for a specific bug, enter the bug ID in the **Search For** field and press Enter.
4. To search for bugs related to a specific software release, do the following:
   a. In the **Product** field, choose **Series/Model** from the drop-down list and then enter the product name in the text field. If you begin to type the product name, the Cisco Bug Search Tool provides you with a drop-down list of the top ten matches. If you do not see this product listed, continue typing to narrow the search results.
   b. In the Releases field, enter the release for which you want to see bugs.

   The Cisco Bug Search Tool displays a preview of the results of your search below your search criteria. You can mouse over bugs to see more content about a specific bug.
5. To see more content about a specific bug, you can do the following:
   - Mouse over a bug in the preview to display a pop-up with more information about that bug.
   - Click on the hyperlinked bug headline to open a page with the detailed bug information.
6. To restrict the results of a search, choose from one or more of the following filters:

Filter	Description
Modified Date	A predefined date range, such as last week or last six months.
Status	A specific type of bug, such as open or fixed.
Severity	The bug severity level as defined by Cisco. For definitions of the bug severity levels, see Bug Search Tool Help & FAQ
Rating	The rating assigned to the bug by users of the Cisco Bug Search Tool.
Support Cases	Whether a support case has been opened or not.

Your search results update when you choose a filter.

All resolved bugs for this release are available in the Cisco Bug Search Tool through the fixed bug search.

This search uses the following search criteria and filters:

Field Name	Information
Product	Series/Model Cisco IOS and NX-OS Software => Cisco IOS
Release	15.4(2)S2

Field Name	Information
Status	Fixed
Severity	2 or higher

Resolved Caveats—Cisco IOS Release 15.2(4)S7

Table 1 Resolved Caveats—Cisco IOS Release 15.2(4)S7

Identifier	Description
CSCus48378	POODLE: CNS feature required to support TLS
CSCup34371	GETVPN GM stops decrypting traffic after TEK rekey
CSCul70788	Router crashes when calculating the best cost successor in EIGRP DUAL
CSCur13495	Service-data of a service change is not updated by SAF forwarder
CSCur43251	POODLE protocol-side fix: HTTPS Client
CSCuo84660	copy command yields DATACORRPUTION error
CSCuh07579	IPSec fails to delete/create SAs due to IPSec background process stuck
CSCuo95771	IPSec SA are deleted incorrectly by background process
CSCua01375	ldap VRF is not working with PKI
CSCus48386	POODLE related fix: LDAPv3 client REQUIRED to support TLS
CSCur23656	Cisco IOS and IOSd in IOS-XE: evaluation of SSLv3 POODLE vulnerability
CSCup32531	Both ESPs crash at AOM Parent when flapping 6K flexvpn sessions

Resolved Caveats—Cisco IOS Release 15.2(4)S6

- CSCtg57599

  Symptom: Lots of SNMP CPUHOG messages are seen and there is a crash due to a watchdog timeout:

  ```
  %SYS-3-CPUHOG: Task is running for (126004)msecs, more than (2000)msecs
  (252/37),process =SNMP ENGINE
  %SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = SNMP ENGINE
  ```

  Conditions: Device is configured with SNMP and is polled for Dot3Stats.

  Workaround 1: Use the following command: **no snmp-server sparse-tables**.

  Workaround 2: Block the objects in dot3 mib that contains this table from being polled:

  ```
  snmp-server view cutdown iso included
  snmp-server view cutdown 1.3.6.1.2.1.10.7 excluded
  ```

  Then to apply the view, use:

  ```
  no snmp-server community your_string_here RO
  no snmp-server community your_string_here RW
  ```

  and then put it back so it looks like:

  ```
  snmp-server community your_string_here view cutdown RO
  snmp-server community your_string_here view cutdown RW
  ```

Further Problem Description: Cisco IOS Software contains a vulnerability that could allow an authenticated, remote attacker to trigger a high CPU on the device via walking specific SNMP objects.

The vulnerability is due to an uninitialized variable in the code. An attacker could exploit this vulnerability by performing SNMP walks against objects on the affected device. An exploit could allow the attacker to cause high CPU on the affected devices.

This vulnerability is not consistently exploitable.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.3/5.2: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:S/C:N/I:N/A:C/E:F/RL:OF/RC:C

CVE ID CVE-2012-5030 has been assigned to document this issue.

Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtq23960

  Symptoms: A Cisco ISRG2 3900 series platform using PPC architecture crashes and generates empty crashinfo files:

  ```
  show flash: all
  -#- --length-- -----date/time------ path <<snip>> 2 0 Mar 13 2011 09:40:36
  crashinfo_<date> 3 0 Mar 13 2011 12:35:56 crashinfo_<date> 4 0 Mar 17 2011 16:14:04
  crashinfo_<date> 5 0 Mar 21 2011 05:50:58 crashinfo_<date>
  ```

  Conditions: The symptom is observed with a Cisco ISRG2 3900 series platform using PPC architecture.

  Workaround: There is no workaround.

- CSCtu42387

  Symptoms: Gigabit and 10 Gigabit Fiber link reporting threshold violation alarm in Cisco ME3600, Cisco ME3800, and Cisco 7600 devices. The "%SFF8472-3-THRESHOLD_VIOLATION: Gi0/11: Rx power high alarm" error message is seen on ports.

  Conditions: This symptom is observed on Cisco ME3600, Cisco ME3800, and Cisco 7600 devices. The messages are seen with the interface shut or no shut.

  ```
  SFF8472-3-THRESHOLD_VIOLATION Gi5/1: Rx power low alarm; Operating value: -28.5 dBm,
  Threshold value: -24.0 dBm
  ```

  Workaround: Fixing the fiber signal issue or disconnecting the fiber from the transceiver has been known to stop the messages.

- CSCtv21900

  Symptoms: Intermittent one-way audio occurs from an MGCP gateway to a Cisco IP phone.

  Conditions: This symptom is observed under the following conditions:

  - Encrypted call with SRTP - MGCP Controlled Gateway
  - Cisco IOS Release 15.1(4)M or later releases

  Phone logs show the following message:

  ```
  6622: DBG 23:29:50.256330 DSP: RTP RX: srtp_unprotect() again 6623: DBG
  23:29:50.257139 DSP: RTP RX: srtp_unprotect() failed with error code 7 6624: DBG
  23:29:50.276390 DSP: RTP RX: srtp_unprotect() failed with auth func 3
  ```

The "Rcvr Lost Packet" counter on the Cisco IP phone begins to increment as soon as the call connects.

Workaround 1: Downgrade the software to Cisco IOS Release 15.1(3)T or earlier releases.

Workaround 2: Perform a hold/resume on the one-way audio call. This mitigates the problem.

- CSCty16106

  Symptom: IKE/GDOI bypass policy entries (four entries) are downloaded to PAL dataplane SADB as part of the initial policy download. But, as IKE/GDOI traffic is never routed to tunnel interfaces, the entries are not required for tunnel protection cases.

  Conditions: This symptom is observed with IKE/GDOI bypass policy entries.

  Workaround: There is no workaround.

- CSCtz97771

  Symptom: During regular operations, a Cisco router running Cisco IOS release 12.4(24)T and possibly other releases experiences a crash. The crash info will report the following:

```
%SYS-2-FREEFREE: Attempted to free unassigned memory at 4A001C2C, alloc 4180794C,
dealloc 417616B0,
%SYS-6-BLKINFO: Attempt to free a block that is in use blk 4A001BFC, words 134, alloc
4180794C, Free, dealloc 417616B0, rfcnt 0,
```

  Conditions: This symptom is not observed under any specific conditions.

  Workaround: There is no workaround.

- CSCuc60868

  Symptom: A router randomly crashes either due to memory corruption at bgp_timer_wheel or memory chunks near bgp_timer_wheel (For example, BFD event chunks if BFD is configured or AtoM Manager chunks if LDP is configured). A crash occurs right after an LDP neighbor is up in the L2VPN setup.

  Conditions: This symptom occurs when **vpls bgp signaling** is unconfigured and then reconfigured. Both L2VPN and BGP are unconfigured and reconfigured after all L2VPN and BGP data structures are fully deleted (about 3 minutes for 5 BGP VPLS prefixes). For the repro on file, OSPF (for IGP) is also unconfigured and reconfigured. Both LDP and BGP signaling are affected by this caveat.

  Workaround: Avoid unconfiguring and reconfiguring BGP L2VPN.

- CSCud25043

  Symptoms: A WebVPN-enabled gateway crashes on Cisco IOS Release 15.1(4)M5 due to SSLVPN_PROCESS.

  Conditions: This symptom is observed under the following conditions:

  - Cisco IOS Release 15.1(4)M5
  - SSL VPN (WebVPN enabled)

  Workaround: There is no workaround.

- CSCud55435

  Symptom: Optimization of AAA and RADIUS function calls.

  Conditions: This symptom occurs when AAA APIs are optimized based on X-ray reports.

  Workaround: There is no workaround.

- CSCud62864

  Symptom: When the Mid-call Re-INVITE consumption feature is active, CUBE consumes Re-INVITE which should change the media state from "sendonly" to "sendrcv". This results in a one way or no way audio on the call.

  Conditions: This symptom occurs when the CUBE Mid-call Re-INVITE consumption feature is enabled.

  Workaround: There is no workaround.

- CSCud86991

  Symptom: On ASR1K, the IOSd process may crash with "crypto dynamic-map" configuration.

  Conditions: This symptom is observed When "crypto dynamic-map ..." configuration is entered from CLI.

  Workaround: There is no workaround.

- CSCue06450

  Symptom: If NTP is not configured on a Cisco ASR 1000 Series router, then PKI (Public Key Infrastructure) services such as auto enrollment and certificate rollover may not function correctly due to an invalid clock.

  Conditions: This symptom occurs if NTP is not configured, or if NTP is not synchronized to the NTP server.

  Workaround: Enable NTP on the router.

- CSCue23898

  Symptom: A Cisco router running Cisco IOS Release 15.3(1)T may crash with a bus error immediately after issuing the **write memory** command.

  ```
  Example: 14:44:33 CST Thu Feb 14 2013: TLB (load or instruction fetch) exception, CPU
  signal 10, PC = 0x228B2C70
  ```

  Conditions: This symptom occurs while updating the router's running configuration with the **write memory** command.

  It is caused by this CLI command "ccm-manager redundant-host A.B.C.D A.B.C.D". For example, "ccm-manager redundant-host 172.21.200.15 172.21.200.13".

  Workaround: There is no workaround.

- CSCug37304

  Symptom: The problem was experienced the first time on a UC560 that was upgraded to Cisco IOS Release 15.1(4)M5.

  At the end of the investigation, it was determined that this is neither specific to the platform nor does it apply to Cisco IOS Release 15.1(4)M5.

  This problem is platform independent and all releases leading to the most current release on Cisco.com in Cisco IOS Release 15.1(4)M (most recent release on Cisco.com at the time writing this explanation is Cisco IOS Release 15.1(4)M7) are affected by this issue.

  Conditions: Crash is seen specifically when FXS ports are in STCAPP controlled mode.

  Workaround: Use the standalone FXS Port, rather than STCAPP controlled. Configure the FXS port as a standalone FXS port, if possible.

- CSCug47401

  Symptom: An RP crash is seen with 128K PWLAN sessions.

Conditions: This symptom is observed after trying to authenticate simple IP sessions with CoA

Workaround: There is no workaround.

- CSCuh05259

  Symptom: Prompt is provided for configure replace command when **file prompt quiet** is configured.

  Conditions: This symptom is observed when “file prompt quiet” has been configured.

  Workaround: Use “force” along with the **configure replace** command.

- CSCuh36124

  Symptom: Service Routing/SAF in Cisco IOS Release 15.2.X.X is experiencing HIGH CPU during a failover condition where the active SAF forwarder looses connection to the network causing the clients to switch to the secondary forwarder. This issue occurs if the forwarder, that becomes active, still has an active neighbor that it needs to send updated registration data to (so more than two forwarders are required to observe this defect). Due to the high CPU condition during this failover, clients can experience longer registration times increasing the outage window.

  Conditions: It has been validated in the lab, that the condition only occurs when more than two forwarders are involved and all the forwarders are peered to each other via direct configured peers or network based EIGRP peers. The HIGH CPU is caused directly by the connection that exists between SAF forwarders to exchange data across the network, and not due to the client towards SAF forwarder data exchange.

  Workaround: There is no workaround.

- CSCuh56385

  Symptom: Very slow propagation of data across a network of SAF forwarders after a fail over condition is observed. More than two SAF forwarders are required to observe this defect.

  Conditions: This symptom occurs when there are more than two SAF forwarders in the network. After a fail over condition and the clients initiate advertising patterns into the standby forwarder, the propagation of these advertisements via update messages to the SAF peers can experience a 5 second inter-service advertisement delay.

  Workaround: There is no workaround. Once the forwarder that suffered the fail over condition returns and establishes its neighbor relationships with its peers, the forwarders will update quickly.

- CSCuh68961

  Symptom: In a DO-DO scenario, the CUBE is not able to send re-invite on other leg if the CUBE receives re-invite immediately followed by ACK.

  Conditions: SIP (PSTN) -- CUBE -- SIP -- CUCM -- IP phone transfers to another IP phone Message Sequence in CUBE CUCM --> reINVITE --> CUBE --> reINVITE --> Provider <-- 200OK 200OK <-- ACK --> reINVITE --> --> ACK

  reINVITE from CUCM is not forwarded to the provider

  Workaround: There is no specific workaround. This issue is only seen from the Cisco IOS release 15.1(4)M and newer.

- CSCuh72000

  Symptom: The TOS of one kind of PIM signaling packet is set to 6. When the packet is encapsulated into MPLS, the TOS value is copied to the EXP value. The packet will then be encapsulated into GRE/IP again, but the EXP value is not copied. PI just leaves the TOS in the IP/GRE header 0.

  Conditions: This symptom does not occur under specific conditions.

  Workaround: There is no workaround.

- CSCuh87195

  Symptom: A crash is seen on a Cisco router.

  Conditions: The device crashes with gw-accounting and call-history configured. The exact conditions are still being investigated.

  Workaround: Perform the following workaround:

  1. Completely remove gw-accounting
  2. Disable call-history using the following commands:

  ```
  gw-accounting file
  no acct-template callhistory-detail
  ```

- CSCui04860

  Symptom: HA sync is not happening from active to standby.

  Conditions: This symptom is observed when HA Sync-up is not happening for PKI Server on Cisco IOS Release 15.3(2.25)M0.1.

  Workaround: There is no workaround.

- CSCui29745

  Symptom: Member links under MLPPP go down as the LCP negotiation of those PPP links fails.

  Conditions: This symptom occurs after the router reloads and the traffic is flowing through the multilink.

  Workaround: Reload SPA/LC on the other end of the link.

- CSCui51363

  Symptom: The multilink does not pass traffic even though it is in an up/up state.

  Conditions: This symptom occurs when the auto DNR status is set and the sip400 ucode crashes.

  Workaround: Perform a shut/no shut in the multilink.

- CSCui54359

  Symptom: Switchover to T.38 fax-relay does not occur when configured for SG3 fax calls. Calls switchover to fax passthrough.

  Conditions: This is observed when fax machines support the SuperG3 standard on both end and the voice gateways are configured to use H323 and T38 v3 fax relay.

  ```
  example: dial-peer voice 1 voip
  destination-pattern <did>
  session target ipv4:<ip_address>
  fax protocol t38 version 3
  or
  voice service voip
  fax protocol t38 version 3
  ```

  Workaround: Use SIP as the VoIP protocol.

  Add “session protocol sipv2” to the voip dial-peer.

  If CUCM is involved, configure a SIP trunk for call handling from/to the voice gateway.

- CSCui59004

  Symptom: IOSd crashes while removing NTP server from the configuration.

  Conditions: This may occur rarely, when removing “ntp server <hosname>” from configuration. ntp servers configured with ip addresses will not cause the same.

Workaround: Timing the "no ntp" configuration such that it does not overlap with the 60 second DNS resolution timer.

- CSCui59927

  Symptom: A memory leak is observed on a Cisco device due to IPSec which causes free memory to deplete to an extent where the device becomes unreachable.

  Conditions: This symptom occurs when IPSec scaling is high.

  Workaround: Reduce scaling of IPSec sessions.

- CSCui64807

  Symptom: An active RP crashes during FIB sync because of memory overrun when the standby sup becomes unavailable.

  Conditions: This symptom occurs when redundant RPs are configured in SSO mode and the standby RP becomes unavailable (for instance because of crash or physical removal). The issue occurs only on Cisco 7600 RSP 720, Cisco 7600 Series Supervisor Engine 720, and Cisco 7600 platforms where the tableid "ISSU FOF LC" support is enabled. As of 03/17/2014, the tableid "ISSI FOF LC" feature is only supported on SY releases. This issue does not impact Cisco ASR 1000 Series platforms.

  Workaround: There is no workaround.

- CSCui85371

  Symptom: Ikev2 session is NOT coming UP.

  Conditions: This defect can be seen on an IKEv2 initiator only. The IKEv2 authentication mechanism is certificate based and a certificate map is configured under IKEv2 profile.

  Workaround: There is no workaround.

- CSCuj14595

  Symptom: A Cisco 3945 voice gateway running Cisco IOS Release 15.2(4)M3 or Cisco IOS Release 15.2(4)M4 may have a processor pool memory leak in the CCSIP_TCP_SOCKET process.

  Conditions: This symptom is seen on slow TCP connections, where the response is slow and frequent transmission errors are observed.

  Workaround: There is no workaround.

- CSCuj17818

  Symptom: PPPoE is configured on radio interfaces. When a shut and no shut are issued on remote interface Router2, nine packets get stuck in the Router1 input queue.

  Conditions: This problem is seen in Router1 when shut is issued on the Router2 interface to disconnect the PPPoE session between Router1 and Router2. In this case the Radio Emulator sends the PADQ packets to Router1 which gets stuck in input queue.

  Workaround: Reloading the box to clear the input queue.

- CSCuj19201

  Symptom: Re-registration time is recalculated on GM nodes upon receiving a TBAR rekey, based on the remaining TEK lifetime at the time of the TBAR rekey.

  This effectively causes a much-shorter re-registration window compared to the one obtained at the GM registration, even if the original TEK lifetime was configured with a long value.

  Conditions: This symptom is observed when TBAR is configured and long TEK lifetime used (more than 7200 seconds).

  Workaround: There is no workaround.

- CSCuj30572

  Symptom: With EIGRP and PFR configured, a Cisco router crashes after giving following EIGRP messages:

  ```
  000111: Sep 17 09:08:33.331: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.50.2.1
  (Tunnel502) is down: Peer Termination received 000112: Sep 17 09:08:33.347:
  %DUAL-3-INTERNAL: EIGRP-IPv4 1: Internal Error -Traceback= 319D4CB4z 319EC5E4z
  319EC7C8z 319E4950z 319EA760z 31A25008z 32C23084z 32C23068z
  ```

  Conditions: This symptom occurs when PFR, OER, and EIGRP are configured.

  Say RouterUnderTest has two EIGRP Peers HUB1 and HUB2. (Given metrics are only for illustration)

  When EIGRP has a Prefix with 3 different Paths installed in following order

  ```
  DRDB1 NH - HUB1, Metric 36571392 / 0 (Installed by PFR)
  DRDB2 NH - HUB2, Metric 58322432 / 409600 ( x Hops away learnt from RouterX)
  DRDB3 NH - HUB1, Metric 538004992/500409600 (y Hops away learnt from Router Y)
  ```

  With these initial conditions, if Neighbor ship with Router Y goes down, Both PFR and EIGRP try to delete DRDB3 Which results in inconsistent data structures with Memory corruption. Any further access to Memory will result in Crash.

  Workaround: No possible work arounds seen. Using other Load sharing methods instead of PFR looks only possible work around.

  More Info: Usually, the crash is seen during execution of EIGRP Route lookup function similar to below.

  ```
  0x33841E10:eigrp_pfr_get_drdb(0x33841ddc)+0x34
  0x33842014:eigrp_pfr_route_lookup(0x33841e88)+0x18c
  ```

- CSCuj62593

  Symptom: Gateway crashes with MALLOCFAIL during ASR/TTS load.

  Conditions: During longevity load for five days, crash is seen almost 61 hours into the load with Cisco IOS Release 15.3(3)M1 and almost 12 hours into load with Cisco IOS Release 15.2(4)M5, due to the non-optimal usage of memory.

  Workaround: There is no workaround.

- CSCuj72215

  Symptom:

  A vulnerability in handling of RTCP traffic of Cisco CUBE could allow an unauthenticated, remote attacker to cause traffic destined to an affected device as well as traffic that needs to be processed-switched to fail.

  The vulnerability is due to exhaustion of interface input queue by the RTCP traffic. An attacker could exploit this vulnerability by sending RTCP packet in a specific sequence. An exploit could allow the attacker to cause traffic destined to an affected device as well as traffic that needs to be processed- switched to fail.

  Conditions:

  RTCP packets have been found to be associated with SIP but any voice protocol may be involved.

  The default input queue size is 75 on ISR routers. When the input queue fills up, the size (76) will exceed the max. This may look like an input queue wedge on the surface but for this bug, the packets should be drained once the call is torn down and the socket is removed. The RTCP packets should only be punted to the CPU for processing (and thus hit the input queue) when the RTP session isn't yet established and we don't have a socket. Once this establishment is done, RTCP traffic should be processed in the fast-path.

Workaround: To alleviate the problems caused by filling up the input queue, the size can be increased with the following command at the interface level, **hold-queue <size> in**.

To stop the issue altogether, RTCP would be need to be disabled by the voice endpoints.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5/4.1: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:N/C:N/I:N/A:P/E:F/RL:OF/RC:C

CVE ID CVE-2014-3268 has been assigned to document this issue.

Additional details about the vulnerability described here can be found at: http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-3268

Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCuj82897

  Symptom: The "control-word" length is not set properly for small HDLC packets running over HDLC AToM VC with SIP-200. For example: SPA-8XCHT1/E1.

  Conditions: This symptom occurs when HDLC AToM VC with SIP-200 is deployed, for example, SPA-8XCHT1/E1, will result in a packet length mismatch issue or dropping by the remote PE router when HDLCoverMPLS runs over the Ethernet link adding an additional padding which cannot be classified at all.

  Workaround: Use SIP-400.

- CSCuj85382

  Symptom: ME3400 reload.

  Conditions: This symptom is observed under the following conditions:

  1. "ethernet cfm traceroute cache" configured.
  2. A Local only ethernet traceroute performed.

  Workaround: Disable CFM traceroute cache by removing "ethernet cfm traceroute cache" configuration.

- CSCuj87667

  Symptom: When value "xxx" of MPLS exp bits was copied to outer IP/GRE header TOS, the new TOS value should be "xxx00000" but now it is "00000xxx", so that the QoS information was broken.

  Conditions: This symptom is observed in MPLS over GRE case.

  Workaround: There is no workaround.

- CSCuj94571

  Symptom: To run the BERT test, remove "keepalive" from the interface. After completing the BERT test, adding "keepalive" causes the standby RSP to reset.

  Conditions: This symptom is consistent and affects Cisco IOS Release 15.1(3)S1.

  Workaround: After the completion of the BERT test, remove the BERT test with "no bert pattern qrss interval <interval>" and then add "keepalive". This will avoid standby RSP reset.

- CSCul27924

  Symptom: Customer experienced crash on ASR-1001 during normal operation.

  Conditions: This symptom is not observed under any specific condition.

  Workaround: There is no workaround.

- CSCul49375

  ```
  Symptom: The Cisco ASR 1000 router displays the following messages in the logs:
  %IDMGR-3-INVALID_ID: bad id in id_get (Out of IDs!) (id: 0x0) -Traceback=
  1#cb40dca901558e45a65b881a8695af4f :400000+8653B3 :400000+893696 :400000+DF330C
  :400000+DED89B :400000+DF8643 :400000+1F57F36 :400000+1F4BBFB :400000+1F33BA7
  :400000+1F336C1 :400000+1F34FF9 :400000+1F27763 :400000+1F29B16 :400000+2546FF3
  :400000+2546EDD :400000+1F2930B
  ```

  No new PPPoE sessions can be established anymore.

  Conditions: The conditions to this symptom are unknown.

  Workaround: Reload the device.

- CSCul54254

  Symptom: Invalid LSAs are not flushed by the router which has their Advertising Router ID. Specifically, Router LSAs which do not have LSID of 0 will not be flushed if the router does not re-originate them, and any LSA with a type that the router does not recognize.

  Lingering LSAs could lead to incorrect routing in some very obscure instances. For example, stale Router LSA fragments from two neighboring routers would need to remain in the network. There would not be a routing problem if only one router's stale Router LSA fragment was allowed to linger.

  Conditions: There are several possible scenarios that could lead to this symptom. One example is that a router is configured with many interfaces attached to an OSPFv3 instance such that it originates more than one Router LSA fragment. Then the router is reloaded before the configuration is saved, and after the reload it does not reoriginate some of the Router LSA fragments.

  Workaround: There is no workaround.

- CSCul75876

  Symptom: A router may crash in an OSPF process during reconfiguration.

  Conditions: This symptom occurs under the following conditions:

  1. Configure the router with "ipfrr" in area 0.
  2. Connect router to area 0 through two links. For some route one interface is the primary path, and the second is the repair path.
  3. Configure router as ABR, that is, have a non-zero area with a neighbor. Do not configure "ipfrr" in the non-zero area. Quickly remove the IP address from both the interfaces in area 0 and router the may crash.

  Workaround: Changes to the reconfiguration procedure will avoid the crash.

  – Shutdown the interface before removing the IP
  – Remove the IP from one interface in area 0, wait for a few seconds and remove the IP address from the second interface in area 0.

- CSCul94087

  Symptom: Output Packet drops is observed on the ATM IMA interface even when there is no live traffic and only signaling exchange between non-Cisco devices. Although output drops in most cases means low bandwidth issues but in this case, an entire site was down due to these drops.

Conditions: This symptom occurs under the following conditions:

1. Layer 2 cross connect is configured on Cisco device and Non-Cisco device at other end.
2. Only signalling traffic flows through the devices.
3. IMA group is created for the ATM connectivity.
4. SPA-24CHT1-CE-ATM card is to be used for the ATM connection.

Workaround: Reload the SPA.

- CSCul96778

  Symptom: A router may crash and reload with BGP related traceback in an extremely rare timing condition while running “show ip bgp vpnv4 vrf XXXX nei A.A.A.A”.

  Conditions: While making BGP related changes such as moving the same neighbor with quick operation of “no neighbor x.x.x.x “ and then “neighbor x.x.x.x” across VRFs. Immediately after this if we type a “show ip bgp vpnv4 vrf XXXX nei A.A.A.A” on a Cisco router running IOS and BGP, then in extremely rare timing condition the router may crash. The possibility of this to happen increases if their configuration and unconfiguration is done from one console and the show operation done from other console.

  Workaround: When doing configuration and un-configuration and then show, its better to serialize the operation rather than aggressively use multiple consoles to do all actions at the same time.

- CSCum00056

  Symptom: ASR IOSd crash occurs with the following error:

  ```
  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = ISG CMD HANDLER
  ```

  Conditions: This symptom occurs when changes are made through RADIUS.

  Workaround: There is no workaround.

- CSCum02221

  Symptom: A vulnerability in BGP processing code of Cisco IOS could allow an unauthenticated, remote attacker to cause a reload of the affected device..

  The vulnerability is due to improper parsing of malformed BGP packets. An attacker could exploit this vulnerability by sending malformed BGP packets to an affected device. An exploit could allow the attacker to cause a reload of the affected device.

  Conditions: This symptom occurs when the device configured for BGP.

  Workaround: There is no workaround.

- CSCum14830

  Symptom: Leaking IPv6 routes is observed from a VRF table into the global table using BGP. These routes consist of the following: 1. BGP routes learned from the VRF IPv6 BGP peer. 2. Redistributed static and connected routes.

  The BGP routes leak fine, but the redistributed static and connected routes have an issue. After the redistributed routes leak, the exit interface shows “null0”. Sometimes instead of showing the exit interface as “null0”, it shows a random interface which is a part of VRF and has IPv6 enabled on it.

  Conditions: This symptom occurs with IPv6 redistributed connected and static routes into BGP VRF (could also be redistributed from other protocols as well but have not been tested).

  Workaround: There is no workaround.

- CSCum16315

  Symptom: Upon reload of a Cisco 7600 router configured with a CoPP policy containing IPv6 ACLs and DSCP matching, the CoPP is only applied to the active RSP as shown below.

  After reload:

```
lab-7609-rsp-02#sh mod power Mod Card Type Admin Status Oper Status ---
-------------------------------------- ------------ ------------ 1 CEF720 48 port
10/100/1000mb Ethernet on on 5 Route Switch Processor 720 (Active) on on 6 Route
Switch Processor 720 (Hot) on on 7 CEF720 8 port 10GE with DFC on on 8 CEF720 8 port
10GE with DFC on on
```

  CoPP is applied to only the active RSP/SUP after reload:

```
lab-7609-rsp-02#sh mod power
Mod Card Type Admin Status Oper Status --- --------------------------------------
------------ ------------ 1 CEF720 48 port 10/100/1000mb Ethernet on on
5 Route Switch Processor 720 (Active) on on
6 Route Switch Processor 720 (Hot) on on
7 CEF720 8 port 10GE with DFC on on
8 CEF720 8 port 10GE with DFC on on
CoPP is applied to only the active RSP/SUP after reload:
lab-7609-rsp-02#sh policy-map control-plane in | inc class|Earl
class-map: COPPCLASS_MCAST (match-any)
Earl in slot 5 :
class-map: COPPCLASS_MGMT (match-any)
Earl in slot 5 :
class-map: COPPCLASS_ALLOW_ICMP (match-any)
Earl in slot 5 :
class-map: COPPCLASS_MONITORING (match-any)
Earl in slot 5 :
class-map: COPPCLASS_FILEXFER (match-any)
Earl in slot 5 :
class-map: COPPCLASS_REMOTEACCESS (match-any)
Earl in slot 5 :
class-map: COPPCLASS_OSPF (match-any)
class-map: COPPCLASS_LDP (match-any)
Earl in slot 5 :
class-map: COPPCLASS_BGP (match-any)
class-map: COPPCLASS_MISC (match-any)
class-map: COPPCLASS_UNDESIRABLE (match-any)
Earl in slot 5 :
class-map: COPPCLASS_IPV4_CATCHALL (match-any)
Earl in slot 5 :
class-map: COPPCLASS_IPV6_CATCHALL (match-any)
class-map: class-default (match-any)
Earl in slot 5 :
```

  When this issue is triggered, the following error will be seen in the logs:

```
*Dec 14 02:33:14.579: %QM-2-TCAM_BAD_LOU: Bad TCAM LOU operation in ACL
```

  This issue potentially exposes the device to a DoS vulnerability.

  Conditions: This symptom occurs under the following conditions:

  1. 7600 HA Environment.
  2. CoPP IPV6 ACL with DSCP match.
  3. Reload or Switchover.

  Workaround: There are two workarounds for this issue.

  1. Modify the CoPP Policy to remove IPV6 ACL/DSCP matching.

2. Remove and reapply the CoPP configuration as shown below:

```
lab-7609-rsp-02(config)#control-plane
lab-7609-rsp-02(config-cp)#no service-policy in COPP
lab-7609-rsp-02(config-cp)#service-policy in COPP
lab-7609-rsp-02(config-cp)#end
```

CoPP is applied to all modulues as required:

```
lab-7609-rsp-02#sh policy-map control-plane in | inc class|Earl
class-map: COPPCLASS_MCAST (match-any)
Earl in slot 1 :
Earl in slot 5 :
Earl in slot 7 :
Earl in slot 8 :
class-map: COPPCLASS_MGMT (match-any)
Earl in slot 1 :
Earl in slot 5 :
Earl in slot 7 :
Earl in slot 8 :
class-map: COPPCLASS_ALLOW_ICMP (match-any)
Earl in slot 1 :
Earl in slot 5 :
Earl in slot 7 :
Earl in slot 8 :
class-map: COPPCLASS_MONITORING (match-any)
Earl in slot 1 :
Earl in slot 5 :
Earl in slot 7 :
Earl in slot 8 :
class-map: COPPCLASS_FILEXFER (match-any)
Earl in slot 1 :
Earl in slot 5 :
Earl in slot 7 :
Earl in slot 8 :
class-map: COPPCLASS_REMOTEACCESS (match-any)
Earl in slot 1 :
Earl in slot 5 :
Earl in slot 7 :
Earl in slot 8 :
class-map: COPPCLASS_OSPF (match-any)
Earl in slot 1 :
Earl in slot 5 :
Earl in slot 7 :
Earl in slot 8 :
class-map: COPPCLASS_LDP (match-any)
Earl in slot 1 :
Earl in slot 5 :
Earl in slot 7 :
Earl in slot 8 :
class-map: COPPCLASS_BGP (match-any)
Earl in slot 1 :
Earl in slot 5 :
Earl in slot 7 :
Earl in slot 8 :
class-map: COPPCLASS_MISC (match-any)
Earl in slot 1 :
Earl in slot 5 :
Earl in slot 7 :
Earl in slot 8 :
class-map: COPPCLASS_UNDESIRABLE (match-any)
Earl in slot 1 :
Earl in slot 5 :
Earl in slot 7 :
```

```
Earl in slot 8 :
class-map: COPPCLASS_IPV4_CATCHALL (match-any)
Earl in slot 1 :
Earl in slot 5 :
Earl in slot 7 :
Earl in slot 8 :
class-map: COPPCLASS_IPV6_CATCHALL (match-any)
Earl in slot 1 :
Earl in slot 5 :
Earl in slot 7 :
Earl in slot 8 :
class-map: class-default (match-any)
Earl in slot 1 :
Earl in slot 5 :
Earl in slot 7 :
Earl in slot 8 :
```

PSIRT Evaluation: The Cisco PSIRT has evaluated this issue and does not meet the criteria for PSIRT ownership or involvement. This issue will be addressed via normal resolution channels.

If you believe that there is new information that would cause a change in the severity of this issue, please contact psirt@cisco.com for another evaluation.

Additional information on Cisco’s security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCum17958

  Symptom: An IOSd crash is observed during a configuration replace.

  Conditions: This symptom occurs on configuration with a port-channel interface.

  Workaround: There is no workaround.

- CSCum24565

  Symptom:

  - MPLS is being processed by the CPU instead of HW switching.
  - **rem com sw show mls vlan-ram** shows “0” value under vpn-num and netdr shows that mpls is being processed by the CPU:

  ```
  Example: 7600# rem comm sw sh mls vlan-ram 1906 1906
  TYCHO Vlan RAM Key: * => Set, - => Clear
  vlan eom nf-vpn mpls mc-base siteid stats rpf vpn-num bgp-grp l2-metro rpf-pbr-ovr
  ----+---+------+----+-------+------+-----+---+-------+-------+--------+-----------
  1906 * - * 0 0 - - 0 0 - * <<<=== vpn-num 0
  ```

  There is a possibility of a high CPU due to interrupts.

  Conditions: The symptom may occur on the Cisco 7600 Series Routers after an SSO is performed on PE with L2VPN in PFC VLAN mode.

  Workaround:

  1. Remove xconnect configuration from the subinterface and reconfigure it.
  2. Shut/no shut the xconnect source interface.

- CSCum61595

  Symptom: Alignment errors are observed after upgrading to Cisco IOS Release 15.2(4)M5.

  ```
  Jan 9 19:42:59.623 GMT: %ALIGN-3-CORRECT: Alignment correction made at 0x6477F81Cz
  reading 0x6BE87495 Jan 9 19:42:59.623 GMT: %ALIGN-3-TRACE: -Traceback= 0x6477F81Cz
  0x647805D0z 0x6478FE70z 0x64751088z 0x64B99F4Cz 0x64B99FD4z 0x64752 284z 0x647525ACz
  ```

Conditions: This symptom does not occur under specific conditions.

Workaround: There is no workaround.

- CSCum65604

  Symptom: A Cisco router gets crashed.

  Conditions: This symptom occurs when shut/no shut is performed on the access interface.

  Workaround: There is no workaround.

- CSCum85813

  Symptom: Shut primary static router and secondary static is not installed automatically.

  Conditions: This symptom is seen on the sites where the BFD state of the backup static route is marked as “U” in the output of “show ip static route bfd”.

  Workaround: Reinstall the default backup static route.

- CSCum95330

  Symptom: Removing an Ethernet service instance which is a member of a bridge domain may cause the router to reload.

  Conditions: This symptom is observed when the last service instance is removed from the bridge domain and there are still members of the bridge domain which are not service instances (such as VFIs).

  Workaround: Completely unconfigure the bridge domain and reconfigure it.

- CSCun10381

  Symptom: A traffic drop was observed because labels do not get programmed.

  Conditions: This symptom occurs when scalable EoMPLS with L3VPN is configured. When notifications on atom-imps arrive, they have to get programmed.

  Workaround: Clear ip route.

  More Info: Traffic was seen to be dropped as the atom-imps could not be programmed because label entry could not be found for the atom-imps.

- CSCun11782

  Symptom: Rtfilter prefixes are sent with incorrect next-hop equal to next-hop of the default static route in GRT instead of BGP router-id.

  Conditions: This symptom occurs with a default static route present in GRT pointing, for example, to the next-hop known behind the connected interface.

  Workaround: Replace the default static route with a more specific static route or remove static and clear BGP.

- CSCun13688

  Symptom: The Cisco Catalyst 6500 Supervisor Engine 2T with CLNS routing configured crashes after **show clnbs route**.

  Conditions: This symptom occurs when CLNS routing is configured.

  Workaround: There is no workaround.

- CSCun20187

  Symptom: HSRP communication fails between two PEs (Cisco 7600 Series router) right after removing a neighbor from VFI.

Conditions: Assume that a VPLS circuit is running between more than two PEs say A,B, and C and HSRP is running between A and B. Removing VPLS peer C on either A or B would cause HSRP communication failure between A and B. This failure is not expected as data path is still available between A and B.

Workaround: Perform shut/no shut on the SVI.

- CSCun24813

  Symptom: In an HA setup, on standby reload, an active crash occurs.

  Conditions: There are a few states maintained on active for the tunnel reserved and tunnel global VLANs depending on the status of their usage (the one trying to free the VLAN).

  When the standby frees the VLAN, the state of VLAN is set to 2 on active. But in this case when the state of VLAN is set to 2, and the standby is reloaded, the active crashes .

  Workaround: There is no workaround.

  More Info: In an HA setup there are states maintained for the VLAN on active, depending on the active or standby that has freed it . There are 4 states : State 1: When the active wants to free the VLAN and is waiting for a message from the standby to free the VLAN. In this case, VLAN is put in delay list for 4 minutes.

  State 0: When VLAN is freed by the active, the state is set to 1.

  State 2 : When VLAN is freed by the standby, the state is set to 2.

  State 3 : Same as State 1 for global rsvd VLAN.

  Cases :

  Case 1: The active wants to free the VLAN, waits for a message from the standby, set the state to 1, before 4 minutes standby frees the VLAN and sends the message to active, the state is set to 0 .

  Case 2 : The active wants to free the VLAN first, set the state to 1, within 4 minutes if a message from the standby does not arrive, the state is set to 0. After 4 minutes the standby frees the VLAN and sends the message to active, and the state is set to 2 .

  Case 3: The standby wants to free the VLAN first, sends a message to the active, the state is set to 2, the active also frees it, and sets the state to 0 finally.

  Now when a peer reload is done, all the VLANs which are in delay list waiting for the standby message are to be freed. Here we check if the state of the VLAN is not 0, it is set to 0 and freed. In case 2, the state of the VLAN after it is deleted from the active and the standby is 2, so on reload an attempt to again free these VLANs is made, hence the crash.

- CSCun31021

  Symptom: A vulnerability in IKE module of Cisco IOS and Cisco IOS XE could allow an unauthenticated, remote attacker to affect already established Security Associations (SA)..

  The vulnerability is due to a wrong handling of rogue IKE Main Mode packets. An attacker could exploit this vulnerability by sending a crafted Main Mode packet to an affected device. An exploit could allow the attacker to cause dropping of valid, established IKE Security Associations on an affected device.

  Conditions: Device configured to process IKE request that already has a number of established security associations.

  Workaround: There is no workaround.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4.3/3.6: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:N/A:P/E:F/RL:OF/RC:C

CVE ID CVE-2014-2143 has been assigned to document this issue.

Additional details about the vulnerability described here can be found at: http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-2143

Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCun35055

  Symptom: The RPF is not cleared when the internal VLAN is freed by shutting down an interface with RPF configuration. This affects the new interface assigned with this internal VLAN.

  Conditions: This symptom occurs when an interface with RPF configuration is shut down.

  Workaround: Flap the RPF configuration for the new interface.

- CSCun48344

  Symptom: A config-sync failure occurs due to the **address-family ipv6 unicast vrf** command during the immediate unconfiguration and reconfiguration of VRF definition.

  Conditions: This symptom occurs with attached running configurations.

  Workaround: There is no workaround.

- CSCun58072

  Symptom: ifOutOctets goes backwards when an output drop happens on the FR subinterface. The PVC output counter also goes backwards.

  Conditions: This symptom occurs when there is an output drop on the FR subinterface.

  Workaround: There is no workaround.

- CSCun62181

  Symptom: A Cisco ASR 1002 router running Cisco IOS XE Release 3.4S crashes when recalculating PMTU.

  Conditions: The symptom occurs when the outgoing tunnel interface flaps.

  Workaround: There is no workaround.

- CSCun68542

  Symptom: CSR1000V router running XE3.11 (15.4(1)S) working as Route Reflector.

  The route-reflector is advertising prefixes with incorrect subnet masks to ibgp peers and route-reflector clients. The incorrect prefixes are not present in the bgp table of the route-reflector itself, however they do get installed in the bgp table of the router receiving the update.

  Conditions: This symptom is observed when BGP route reflector uses the additional paths feature.

  Workaround: Disable additional path feature either globally under address-family or per neighbor.

- CSCun73515

  Symptom: A router crashes due to RMON.

  Conditions: This symptom occurs on activation of an RMON event.

  Workaround: There is no workaround.

- CSCun77010

  Symptom: A router may crash after or during the execution of the **show ipv6 ospf rib** command.

  Conditions: This symptom occurs when many routes or route paths are present in the OSPFv3 rib. The OSPFv3 rib is significantly recomputed during execution of commands.

  Workaround: Limit the use of the **show ipv6 ospf rib** command.

- CSCun86087

  Symptom: In a VPLS environment, packets of some VCs are blocked in an imposition direction.

  Conditions: This symptom occurs with port channels and LAG as MPLS core-facing interface on ES+.

  Workaround: There is no workaround.

- CSCun90108

  Symptom: On CUBE there is a port leak seen for each audio+video call negotiated to audio call.

  Conditions: This symptom is observed when audio + Video M line offer answered with only audio m line.

  Workaround: Send answer with both audio m line and video, if video not supported send port 0.

- CSCun91923

  Symptom: CUBE reloads intermittently while handling SIP call forking scenario.

  Conditions: In SIP Call forking scenario, an INVITE sent from CUBE is routed to multiple SIP endpoints and multiple SIP provisional responses such as 183 Session Progress with different To tags are received.

  Workaround: There is no workaround.

- CSCun92095

  Symptom: IOS-XE running router may reload when unconfiguring BGP along with other removal operations in a scaled setup.

  Conditions: BGP is configured with 1Million+ nets and 4000 VRFs. Then the bgp instance is removed using “no router bgp <>”

  Workaround: Shut down the bgp neighbor sending big scale nets to remove the nets first from BGP and RIB. Then remove the BGP using “no router bgp <>”.

- CSCuo08759

  Symptom: With IP-FRR, VPLS traffic is dropped on a core-facing port-channel after a link flap.

  Conditions: This symptom occurs when a core-facing interface is a port-channel configured on a Cisco 7600 ES+ card.

  Workaround: Perform shut and no shut on the port-channel interface.

- CSCuo13314

  Symptom: ES+ crashes while deleting the imposition table from LC.

  Conditions: This symptom occurs while flapping the scalable EoMPLS.

  Workaround: There is no workaround.

- CSCuo15967

  Symptom: Receiving TCP RST does not trigger a BGP session down.

Conditions: This symptom occurs when BGP NSR (ha-mode SSO) is enabled. It is observed on a Cisco ASR 1001 router running the following releases:

  - Cisco IOS XE Release 3.6.xS
  - Cisco IOS XE Release 3.7.xS

Workaround: Disable NSR on the router as “no neighbor x.x.x.x ha-mode sso”.

- CSCuo16717

  Symptom: PPPoX brings up sessions failure with IPv6 configurations.

  Conditions: This symptom occurs when “vpdn authen-before-forward” is configured.

  Workaround: Do not configure “vpdn authen-before-forward”.

- CSCuo22184

  Symptom: The VPLS bit is not set in the flood VLAN LTL index which causes a traffic drop.

  Conditions: This symptom occurs under the following conditions:

  - Have a port-channel with member links on different NP (say NP2 and NP1) and a physical interface on the same LC and NP (say NP2) to different neighbors, say PE1 and PE2 respectively.
  - Shut down the member link of NP1.
  - Remote shut the VLAN or access interface on PE2 (reached by physical interface).
  - The V-bit is not set and this affects the traffic towards PE1 (reached by port-channel interface).

  Workaround:

  - Either no-shut the remote VLAN or AC on PE2.
  - Perform shut and no-shut the port-channel.

- CSCuo46913

  Symptom: A crash is seen causing a system reload. The crash occurs in the crypto IKMP process:

```
Exception to IOS Thread: Frame pointer 0x3CEFFB58, PC = 0x164CC518
UNIX-EXT-SIGNAL: Segmentation fault(11), Process = Crypto IKMP
```

  Conditions: This symptom occurs after the following debug:

```
debug cry condition peer subnet XXX.XXX.XXX.XXX XXX.XXX.XXX.XXX
```

  The exact conditions are still being investigated.

  Workaround: There is no workaround.

- CSCuo47685

  Symptom: While evaluating the Cisco IOS Release 15.3(3)S3 early release image, the following error message was observed when using the CoPP configuration given below which matches based on precedence only as shown:

```
class-map match-any coppclass-protocol match precedence 6 7
```

  “Match precedence in IPv4/IPv6 packets is not supported for this interface error: failed to install policy map CoPP”

  Upon occurrence, the entire CoPP policy map is not loaded. There is a concern that some field devices on the current release (Cisco IOS Release 15.0(1)S6) may have the above configuration and as such is prone to this error (CoPP installation failure during upgrade).

Conditions: This symptom occurs while evaluating the Cisco IOS Release 15.3(3)S3 early release image.

Workaround: There is no workaround.

- CSCuo48507

  Symptom: While testing ISSU from XE310<->XE311 with ikev2_dvti and GRE features, packet drops is observed after a switchover.

  Conditions: This symptom is observed during upgrade to Cisco IOS Release 3.11 and downgrade to Cisco IOS Release XE 3.10.

  Workaround: There is no workaround.

- CSCuo49923

  Symptom: Performing an ISSU upgrade with the CEF table consistency checkers enabled may result in a crash on "issu runversion".

  Conditions: This symptom occurs with a Cisco Catalyst 6500 Series Switch running Cisco IOS Release 15.1(02)SY.

  Workaround: Turn off the CEF table consistency checkers before performing an ISSU upgrade.

- CSCuo53561

  Symptom: BGP fails to apply an inbound route map on prefixes after a switch over.

  Conditions: This symptom occurs when NSR is enabled and RP switchover is performed twice.

  Workaround: Enable the knob "bgp sso route-refresh-enable" or manually do a soft refresh to get the routes back from NSR peers on the new active RP.

- CSCuo56871

  Symptom: A Cisco ASR 1001 router running Cisco IOS Release 15.2(4)S4 acting as a route server crashes when **clear bgp ipv4 unicast *** is executed.

  Conditions: This symptom occurs when a router is configured as as route server and a command executed in an IPv4 table is reset via **clear bgp ipv4 unicast ***.

  Workaround: Do not execute command **clear bgp ipv4 unicast ***. Instead, one could use the **clear ip bgp *** to hard reset all the BGP tables.

- CSCuo60001

  Symptom: MFR links do not come up.

  Conditions: This symptom occurs when SPA reloads.

  Workaround: There is no workaround.

- CSCuo62753

  Symptom: SIP400 LC microcode goes into error state.

  Conditions: This symptom occurs when FRF12 is configured and a microcode reload is done.

  Workaround: Perform an LC reload.

- CSCuo70773

  Symptom: Confidence levels sent to an ASR server from VXML gateway in the MRCPv2 messages are not the expected values. The values may appear to have had their leading zero after decimal place removed or trimmed.

  Conditions: This symptom occurs under the following conditions:

  - MRCPv2

  - Incoming confidence level in VXML document is less than 0.10

  Workaround: Do not use a confidence level value smaller than 0.10 in VXML documents. Do not provide a confidence level that has a leading zero after the decimal point. Example: 0.05.

- CSCuo76187

  Symptom: BGP peer terminates session with NOTIFICATION 3/10 (illegal network).

  Conditions: This symptom occurs when a recursively known VPNv4 route is advertised from an IOS-based router to XR or JunOS based router. The issue is not observed when both peers are running IOS.

  Workaround: There is no workaround.

- CSCuo83510

  Symptom: A stack overflow and boot loop can occur when configuring OSPFv3 for IPv6 using a non-broadcast network type on IOS XE

  Conditions: SVI or Layer-3 Interface using the ospf non-broadcast network type.

  Workaround: Remove the non-broadcast network configuration.

  Further Problem Description:This issue was found during a security audit of the product.

  PSIRT Evaluation: The Cisco PSIRT has evaluated this issue and does not meet the criteria for PSIRT ownership or involvement. This issue will be addressed via normal resolution channels.

  If you believe that there is new information that would cause a change in the severity of this issue, please contact psirt@cisco.com for another evaluation.

  Additional information on Cisco's security vulnerability policy can be found at the following URL:

  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCup11582

  Symptom: A Cisco router randomly crashes.

  Conditions: This symptom occurs with normal SIP voice traffic with TLS signaling and SRTP for media flows.

  Workaround: There is no workaround.

- CSCup18062

  Symptom: A memory leak is observed.

  Conditions: This symptom occurs on a device running Cisco IOS XE Release 3.7.5S. The leak does not occur with all crypto map-related configuration. It occurs with RSA authentication and with specific configuration as shown below:

  ```
  crypto dynamic-map itcard_dynamic 600 set transform-set <name> set pfs group5 set
  identity IDENTITY600>*** match address IDENTITY600
  ```

  Workaround: There is no workaround.

- CSCup22590

  Symptom: Some Cisco Internetwork Operating System (IOS) releases may be affected by the following vulnerabilities:

  These products include a version of openssl that is affected by the vulnerabilities identified by the Common Vulnerability and Exposures (CVE) IDs:

  CVE-2014-0195 - DTLS invalid fragment vulnerability

  CVE-2014-0221 - DTLS recursion flaw

CVE-2014-0224 - SSL/TLS MITM vulnerability

This bug has been opened to address the potential impact on this product.

Conditions: Devices running an affected version of Cisco IOS and utilizing an affected configuration.

One of more of these vulnerabilities affect all versions of IOS prior to the versions listed in the Integrated In field of this defect.

Workaround: There is no workaround.

Further Problem Description: Customers may utilize the Cisco IOS Software Checker to see if their releases are impacted by these vulnerabilities.

The Cisco IOS Software Checker can be found here:
http://tools.cisco.com/security/center/selectIOSVersion.x

Customers will need to input the version(s) of IOS that are of interest in Step 1. At Step 2, customers should select "All previously published Cisco Security Advisories". If affected by the June 5th OpenSSL Cisco Security Advisory it will be listed in the results.

CVE-2014-0224: All Cisco IOS services that provide a form of TLS or SSL encryption are affected by this vulnerability. This includes features such as the HTTPS Web Management interface.

CVE-2014-0195: Cisco IOS devices that support SSLVPN (AnyConnect) and have the feature configured and enabled are affected by this vulnerability.

CVE-2014-0221: Cisco IOS devices that support SSLVPN (AnyConnect) and have the feature configured and enabled are affected by this vulnerability.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 10/9.5:

https://intellishield.cisco.com/security/alertmanager/cvss?target=new&version=2.0&vector=AV:N/AC:L/Au:N/C:C/I:C/A:C/E:F/RL:U/RC:C

The Cisco PSIRT has assigned this score based on information obtained from multiple sources. This includes the CVSS score assigned by the third-party vendor when available. The CVSS score assigned may not reflect the actual impact on the Cisco Product.

Additional information on Cisco's security vulnerability policy can be found at the following URL:

http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

- CSCup23792

  Symptom: A loss of service-group configuration under a subinterface is observed.

  Conditions: This symptom occurs only when the router is reloaded. It is not seen with a particular LC reload where the interface exists.

  Workaround: There is no workaround.

- CSCup53658

  Symptom: q-in-q subinterfaces on a Cisco ASR 1000 Series router do not show correct traffic statistics via SNMP ifTable/ifXTable or CLI (show vlans dot1q).

  Conditions: This symptom occurs when the subinterface is configured under a port channel. The issue is not seen when the subinterface is a part of the physical interface.

  Workaround: Traffic statistics via CLI can be obtained directly from the SPA by using the following command for each member interface of the port channel:

  Using Gi1/3/0 as an example:

  request platform software console attach 1/3

(Note: On Cisco ASR 1000 releases prior to XE 3.2 this command may fail. If so, use the hidden command: ipc-con <slot> <bay>)

```
show hw-module subslot 0 tcam all_entries vlan brief
```

Note the VLANs (denoted by V1 and V2) for which statistics are required.

```
Example: Slot-0-0>show hw-module subslot 0 tcam all_entries vlan brief ADDR PO V1 V2
C1 C2 ETYPE QVASN IPF IT IACL IRID EPF ET EACL ERID VVID PV PS DA SCTH FE RGN 2076 00
2005 1507 00 00 0000 18 2212 00 0004 0000 0002 00 0004 0000 0000 C0 00 00 0000 00 6
```

Use the following command to get VLAN TCAM statistics for the TCAM with address 2076 (that handles q-in-q for VLAN 2005 and 1507 as per V1 and V2 columns)

Output will be like the following:

```
show hw-module subslot 0 tcam counters vlan 2076 VLAN Rx Hit : Pkt: 1066 VLAN Rx
Unicast Send : Pkt: 1065 Byte: 126102 VLAN Rx Mcast Send : Pkt: 0 Byte: 0 VLAN Rx
Bcast Send : Pkt: 1 Byte: 64 VLAN Rx Osub Drop : Pkt: 0 Byte: 0 VLAN Tx Hit : Pkt:
1066 VLAN Tx Ucast Send : Pkt: 1064 Byte: 126038 VLAN Tx Mcast Send : Pkt: 0 Byte: 0
VLAN Tx Bcast Send : Pkt: 2 Byte: 128
```

Alternatively to avoid the need to look up the TCAM address beforehand, you can use the following syntax:

```
show hw-module subslot 0 tcam entry vlan 0 first-vlan-tag second-vlan-tag 0 8 8 | i
Pkt
```

The Hit counters represent overall TX/RX packet counters. The RX/TX send represent packet and byte counts for Unicast, Multicast and Broadcast Respectively

Note: The only way to clear the counters is to remove and readd the member interface from the port channel.

- CSCup66424

  Symptom: A Cisco router fails to send out any packet. The link status is up/up, but no packet is sent out the interface.

  Conditions: This symptom occurs when one interface is connected and the link status is up.

  Workaround: There is no workaround.

- CSCuq01057

  Symptom: An SP crash occurs at @tyfib_error_recovery or “%MLSCEF-SP-2-SANITY_FAIL: Sanity Check of MLS FIB s/w structures failed” is observed while performing a core interface shut/no shut with BGP PIC enabled on an L3VPN PE.

  Conditions: This symptom occurs on performing a core interface shut/no shut with BGP PIC enabled on an L3VPN PE.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.2(4)S5

- CSCeh69721

  Symptom: The box crashes with the following error message:

  ```
  %SCHED-3-CORRUPT,%SCHED-3-STILLWATCHING
  ```

Conditions: This symptom occurs when the box is stress tested with e-phone calls. This is a bug at socket layer so any application which needs to duplicate a socket will encounter this sort of a bug. For example, repeated attempts for a tftp copy also can cause this.

Workaround: There is no workaround.

- CSCej00344

  Symptom: A router may reload unexpectedly when opening a terminal session.

  Conditions: This symptom can be seen on any platform. It can be seen while starting any terminal session from the router, including a mistyped command which the router by default will try to resolve as an address to telnet to. This bug is not specific to X.25 configuration and is seen when initiating an outbound telnet/ssh/rlogin session from the device. It occurs when there are multiple outbound sessions from the same terminal (console,vty).

  Workaround: There is no workaround.

- CSCsm40779

  Symptom: A router may go into initial configuration dialog on bootup.

  Conditions: This symptom is observed on a router that is running Cisco IOS Release 12.4(11)T2 with the c7200p-adventerprisek9-mz image.

  Workaround: There is no workaround.

- CSCtb34814

  Symptom: The %DATACORRUPTION-1-DATAINCONSISTENCY: copy error is observed without any traceback just before the the system crashes.

  Conditions: This issue occurs under normal conditions.

  Workaround: There is no workaround.

- CSCtf31377

  Symptom: Cisco IOS crashes due to processor pool memory corruption.

  Conditions: This symptom occurs due to processor pool memory corruption. IOS generates one or more CLUE memory error messages similar to the following messages:

  ```
  %CLUE-DFC3-3-SOR_CORRUPT: CLUE record corruption in start of record field, record id
  3341, record starting address 0x5FFFFF90
  ```

  This issue could also be seen on LAN cards of a Cisco 7600 router.

  Workaround: There is no workaround.

- CSCtn04686

  Symptom: When MHSRP is configured and the hello packets are passing through Etherchannel, and the cables connected to the Etherchannel port are unlugged/plugged, the MHSRP hello packets are not received on the Etherchannel interface.

  Conditions: This symptom is observed on a Cisco 3845 router running Cisco IOS Release 15.0(1)M4.

  Workaround: Unplug/plug the cables.

- CSCtz13023

  Symptom: A crash occurs during registration in SRST mode.

  Conditions: This symptom occurs during registration in SRST mode.

  Workaround: This issue is fixed and committed.

- CSCtz19192

  Symptom: Router crashes with the following message:

  ```
  "Unexpected exception to CPU: vector 1200".
  ```

  Conditions: This symptom occurs due to a change in the bandwidth or policing rate of the dialer interface.

  Workaround: Downgrade to Cisco IOS Release 15.1(4)M4.

- CSCtz66347

  Symptom: Router crashes on executing **show tech-support** from the linux client to the IOS server over an SSH session with the rekey enabled.

  Conditions: This symptom occurs when the rekey value “ip ssh rekey volume 400” is configured.

  Workaround: Disable the rekey feature by configuring the **no ip ssh rekey** command.

- CSCtz73473

  Symptom: In a rare multipath import configuration on IOS router, the following traceback is seen:

  ```
  SW0: *May 4 12:08:40.175 PDT: %IPRT-3-INVALID_NEXTHOP: Duplicate ID 0x3 113.1.1.0/24
  from bgp decode: 0x6770760 ---> ip_route_update+37C 0x59F7B20 --->
  bgp_ipv4_rib_install+578 0x59F87C8 ---> bgp_ipv4_rib_update+108 0x5A8C524 --->
  bgp_vpnv4_update_iprib+2C 0x59F8C24 ---> bgp_v4class_update_fwdtable_walker+60
  ```

  Though there is no operational impact, it disturbs the console with the above traceback.

  Conditions: This symptom is observed when you configure the following in the VRF address family:

  ```
  router bgp 200000
  !
  address-family ipv4 vrf 5
  import path selection multipaths
  maximum-paths eibgp 8
  ```

  Workaround: Do not log output on console but make it buffered to keep console clean.

- CSCua18166

  Symptoms: When sub appid is triggered by end points, the network does not recognize it and displays it as “Unknown identifier”.

  Conditions: This symptom occurs when the limitation results in not supporting traffic classification based on sub appid.

  Workaround: There is no workaround.

- CSCua44483

  Symptoms: Mcast stops sending for all groups once all flows have ceased, due to timeout.

  Conditions: This symptom occurs during normal operation, after senders have stopped sending and/or flows have timed out as normal.

  Workaround: Disable and reenable mcast routing.

- CSCua60785

  Symptoms: Metadata class-map matches only the first of the following filter, if present, in a class map (the other media-type matches are skipped):

  ```
  match application attribute [category, sub-category, media-type, device-class]
  value-string match application application-group value-string
  ```

  Conditions: Seen in a case where the class map has the aforementioned filters.

Workaround: There is no workaround.

- CSCua86620

  Symptoms: The vmware-view application is not detected/classified.

  Conditions: This symptom is observed when vmware-view applications are used.

  Workaround: There is no workaround.

- CSCuc18606

  Symptoms: After BGP flap or device reload, the following error is displayed in the log:

  ```
  BGP-3-DELROUTE Unable to remove route for [XYZ] from radix trie
  ```

  There is also a reachability issue.

  Conditions: This symptom is observed during BGP flap, router reload, and when changing the NET statement under the ISIS process.

  Workaround: Reconfiguring NET under ISIS or reloading the device may help to resolve the issue.

- CSCuc28931

  Symptom: The router crashes due to high CPU and lack of memory.

  Conditions: This symptom occurs when using a local connect between an EFP with encap dot1q and an EFP with encap untagged.

  Workaround: There is no workaround.

- CSCuc41531

  Symptoms: Forwarding loop is observed for some PfR-controlled traffic.

  Conditions: This symptom is observed with the following conditions:

  - Traffic Classes (TCs) are controlled via PBR.
  - The parent route is withdrawn on selected BR/exit.

  Workaround: This issue does not affect configured or statically defined applications, but only affects learned applications so this can be used as one workaround. Another option is to issue shut/no shut on PfR master or clear the related TCs with the **clear pfr master traffic-class ...** command (this fixes the issue until the next occurrence).

- CSCuc99750

  Symptom: EIGRP routes, that are not Feasible Successor are getting into the routing table.

  Conditions: This symptom is observed when you increase variance and maximum paths.

  Workaround: There is no workaround.

- CSCud63146

  Symptoms: In a GETVPN scenario, the GM fails to install policies on reload. A crypto map is applied on ethernet 0/0 while the local address of the crypto map is configured with ethernet 0/1.1

  Conditions: This symptom occurs after a reload. The GM fails to install policies from the key server.

  Workaround: Remove the crypto map configuration on the interface and reapply.

- CSCue68714

  Symptom: Newer released IOS-XE BGP, post Cisco IOS Release 15.2(4)S/XE3.7 not forming BFD session with the older implementations. This happens when using eBGP multi-hop to peer between two loopback interfaces on directly connected routers.

Conditions: This ddts adds a couple of options “[single-hop | multi-hop]” to the existing BGP-BFD knob “neighbor x.x.x.x fall-over [bfd] [check-control-plane-failure]”.

So, after the change the knob would be: “neighbor x.x.x.x fall-over [bfd] [single-hop | multi-hop] [check-control-plane-failure]”

**Note: Existing: “neighbor x.x.x.x fall-over [bfd]” --- This behavior would not be disturbed; so that we do not change the behavior that has been released as part of all the releases for more than three years now.

Add-on in this ddts:

1) “neighbor x.x.x.x fall-over [bfd] [single-hop] -- NEW-option “single-hop”; would force BGP to open a single-hop bfd session. Even in case of back-to-back ebgp update-source loopback with 2 hop BGP peering.

2) “neighbor x.x.x.x fall-over [bfd] [multi-hop] -- NEW-option “multi-hop”"; would force BGP to open a multi-hop bfd session.

Workaround: There is no work around. ISR G2 should support BFD multi-hop feature.

More Info: ISR-G2 does not support multi-hop BFD, while ISR4400 supports multi-hop BFD. BFD multi-hop support for ISR-G2 needs to be provided, so that they can interop with ISR4400 and ASRs.

- CSCue69214

  Symptom: Memory leaks are seen in the metadata after removing a virtual interface.

  Conditions: This symptom occurs after removing a virtual interface, if metadata is enabled.

  Workaround: There is no workaround.

- CSCue95644

  Symptom: This is the Cisco response to research performed by Mr. Philipp Schmidt and Mr. Jens Steube from the Hashcat Project on the weakness of Type 4 passwords on Cisco IOS and Cisco IOS XE devices. Mr. Schmidt and Mr. Steube reported this issue to the Cisco PSIRT on March 12, 2013.

  Cisco would like to thank Mr. Schmidt and Mr. Steube for sharing their research with Cisco and working toward a coordinated disclosure of this issue.

  A limited number of Cisco IOS and Cisco IOS XE releases based on the Cisco IOS 15 code base include support for a new algorithm to hash user-provided plaintext passwords. This algorithm is called Type 4, and a password hashed using this algorithm is referred to as a Type 4 password. The Type 4 algorithm was designed to be a stronger alternative to the existing Type 5 and Type 7 algorithms to increase the resiliency of passwords used for the enable secret password and username username secret password commands against brute-force attacks.

  This Cisco Security Response is available at
  http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20130318-type4

  Conditions: See the published Cisco Security Response.

  Workaround: See the published Cisco Security Response.

  PSIRT Evaluation: The Cisco PSIRT has evaluated this issue and a Cisco Security Response is available at
  http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20130318-type4

  If you believe that there is new information that would cause a change in the severity of this issue, please contact psirt@cisco.com for another evaluation.

  Additional information on Cisco’s security vulnerability policy can be found at the following URL:

  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCuf53543

  Symptom: MPLS-TP L2 VCs are down after an SIP reload and RP switchover.

  Conditions: This symptom occurs when VCs are configured through an MPLS-TP tunnel in a hardware redundant platform.

  Workaround: There is no workaround.

- CSCuf56842

  Symptom: A reload may occur while using **show oer** and **show pfr** commands via SSH.

  Conditions: This symptom is observed when the **show pfr master application detail** command is used via SSH.

  Workaround: There is no workaround.

- CSCug22238

  Symptom: UUS/UUI fields from a refer are not sent out on the corresponding INVITE when this is a SIP GW.

  Conditions: This symptom is observed in Cisco IOS Release 15.1.4M6.

  Workaround: There is no workaround.

- CSCug43009

  Symptom: SYS-SP-2-MALLOCFAIL memory allocation fails due to I/O buffer memory leak in process_online_diag_pak.

  Conditions: This symptom occurs when some diag packets get en-queued to a queue which is not being watched. Hence, there is no dequeueing on that queue which leads to I/O memory leak.

  Workaround: Reload the box to clear the I/O pool when it is full.

- CSCug50606

  Symptom: Sometimes, IPCP assigns an different address for clients from wrong address pool.

  Conditions: This symptom is observed under the following conditions:

  - **peer default ip address** command is configured on dialers.
  - There are some dialers on the Cisco router.
  - The issue could happen on Cisco IOS Release 15.2(4)M3.

  Workaround: There is no workaround.

- CSCug71297

  Symptom: An SP crash is observed at the below RPC call block during an ISSU upgrade after commit version.

  ```
  SP: Frames of RPC pf_issu_sp2rp process (pid 579) on 16 (proc|slot) after blocking rpc
  call failed: 42342B84
  ```

  Conditions: This symptom occurs during ISSU commit version while saving the configuration.

  Workaround: There is no workaround.

- CSCug75194

  Symptom: A latency issue is observed. The order of packets changes.

  Conditions: This symptom occurs on EVC xconnect for MACsec packets and data packets.

  Workaround: Stop the control traffic from the peer side and send only data traffic.

- CSCug97383

  Symptom: Switch crashes with EOAM and IP SLA Ethernet-monitor configurations.

  Conditions: This issue occurs infrequently when EOAM configuration include VLANs. Does not occur if all EOAM configurations are configured with only Ethernet Virtual Circuits (EVC).

  Workaround: There is no workaround.

- CSCug99771

  Symptom: The OSPF N2 default route is missing from the spoke upon reloading the hub. The hub has a static default route configured and sends that route over the DMVPN tunnel running OSPF to spoke. When the hub is reloaded, the default route is missing on the spoke. NSSA-External LSA is present on the spoke after reload, but the routing bit is not set. Hence, it is not installed in RIB on the spoke.

  Conditions: Default originated using the **area X nssa default-information-originate** command.

  Workaround: Removing & readding **area X nssa default-information-originate** on the hub resolves the issue.

- CSCuh09324

  Symptom: UDP-based entries are not deleted from the flowmgr table resulting in a crash or poor system response with CPU hog messages being shown.

  Conditions: This symptom occurs in ct5760-ipservicesk9.bin cat3k_caa-universalk9.bin and cat4500e-universalk9.bin images

  The device is configured with UDP services that originate from the device. This includes but not limited to the following features:

  - TFTP
  - Energy Wise
  - DNS
  - Cisco TrustSec

  Workaround: Enter the following commands:

  ```
  Router#config terminal
  service internal
  end
  Router#show flowmgr
  ```

  The output of this command will show many lines entries holding with the same port numbers. Disabling the feature that is being held in the flows until an upgrade can be performed, is a workaround.

  A reload is required to clear the held flows.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5.4/4.5: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:H/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C

  CVE ID CVE-2013-6704 has been assigned to document this issue.

  Additional details about the vulnerability described here can be found at: http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2013-6704

  Additional information on Cisco’s security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCuh37664

  Symptom: Prefixes/TCs stay INPOLICY although some configured resolvers are above threshold.

  Conditions: This symptom is observed when the policy uses non-default resolvers.

  Workaround: Reload the MC.

- CSCuh41290

  Symptom: After the unavailability of the LDAP CRL, no new CRL fetches can be done because LDAP waits for a reply infinitely and never times out.

  Conditions: This symptom was first seen on Cisco IOS Release 15.1(4)M6 but is not exclusive to it.

  Workaround: Set "revocation-check none" under affected trustpoint. Reload router.

- CSCuh45042

  Symptom: Traffic on some GIG subinterfaces are seen to be dropped at the SPA. The SPA TCAM is seen to have two entries sharing the same logical address as a result of which one entry is seen to overwrite the other.

  Conditions: This symptom was observed after a router/LC/SPA reload. The exact condition that triggers this symptom is not known.

  Workaround: There is no workaround.

- CSCuh69292

  Symptom: LDAP moves in the stuck state.

  Conditions: This issue is seen if the LDAP server becomes unavailable during LDAP transactions.

  Workaround: There is no workaround.

- CSCuh91645

  Symptom: WS-SUP720-3B crashes while receiving DHCP packets.

  Conditions: This symptom occurs with the **ip dhcp relay information policy-action encapsulate** command.

  Workaround 1. Use the **ip dhcp relay information policy-action replace** command.

  Workaround 2. Use the **no ip dhcp relay information trusted** command.

- CSCuh94035

  Symptom: A watchdog timeout crash occurs.

  Conditions: This symptom occurs when IPv4 or IPv6 EIGRP are configured. A crash occurs while DUAL is updating the EIGRP topology table.

  Workaround: There is no workaround.

- CSCuh97129

  Symptom: Losing EIGRP Extended communities on BGP L3VPN route.

  Conditions: This symptom is observed when Remote PE-CE connection is brought down and only backup EIGRP path remains in the BGP table.

  Workaround: Clearing the problem route in the VRF will resolve the issue.

- CSCui04530

  Symptom: Upon FPD upgrade, you get this error on Cisco IOS c7600 switch:

```
! %FPD_MGMT-3-BUNDLE_EXTRACT_ERROR: Cannot extract the ssc-600-fpd.bndl bundle from
sup-bootdisk:c7600-fpd-pkg.151kg - The required bundle is not in the package file.
Please make sure that you have the right FPD image package file. % Cannot get the
required data from the indicated file, please verify that you have a valid file and
entered a valid URL. !
```

Conditions: This symptom is observed under the following conditions:

```
IOS: c7600s72033-advipservicesk9-mz.122-33.SRB3
CARDS: WS-SSC-600 WS-IPSEC-3
CLI: upgrade hw-module slot x fpd file sup-bootdisk:c7600-fpd-pkg.151-3.S2.pkg
```

Workaround: Upgrade to FPD image that includes corresponding *.bndl image.

- CSCui14692

  Symptom: Crash on C819G running 152-4.M1 due to memory corruption at vm_xif_malloc_bounded_stub.

  Conditions: This condition is seen due to recursive function call of fib code, NHRP, IP SLA etc. However, these might not be the only trigger.

  Workaround: There is no workaround.

- CSCui17064

  Symptom: A traffic drop is seen while sending traffic from CE to PE.

  Conditions: This symptom is observed if l2acl is configured in PE to permit broadcast and multicast traffic. While sending traffic from CE to PE, packets are dropped.

  Workaround: There is no workaround.

- CSCui21030

  Symptom: A vulnerability in OSPF implementation of Cisco IOS and Cisco IOS XE could allow an unauthenticated, adjacent attacker to cause a reload of the affected device.

  The vulnerability is due to improper parsing of certain options in OSPF LSA type 11 packets. An attacker could exploit this vulnerability by sending LSA type 11 OSPF packet with unusual options set. An exploit could allow the attacker to cause a reload of the affected device.

  Conditions: This symptom occurs on receiving a bad RI opaque LSA with some unusual options.

  Workaround: There is no workaround.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5.7/4.7: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:A/AC:M/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C

  CVE ID CVE-2013-5527 has been assigned to document this issue.

  Additional details about the vulnerability described here can be found at: http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2013-5527

  Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCui34165

  Symptom: Port-channel QoS features might fail to work after a router reload, followed by QoS configuration modification.

  Conditions: This symptom occurs when a vlan load-balanced port-channel is used with policy aggregation configuration where the QoS policy is configured on member links and the port-channel sub-interface, and after a system reload (configuration is from startup config).

Workaround: Reload the router without port-channel QoS configuration, and add port-channel QoS configuration to the running configuration after the router boots up.

- CSCui46593

  Symptom: CPU hog crash due to Mwheel Process.

  Conditions: This symptom is observed in a normal operation.

  Workaround: There is no workaround.

- CSCui59185

  Symptom: ASR901 crashes while booting up with memory lite disabled.

  Conditions: This symptom is observed when RFLA is enabled with memory lite disabled.

  Workaround: Enable memory lite.

- CSCui65083

  Symptom: CoS Markings are not being preserved on the dot1q interface after reload.

  Conditions: This symptom occurs under the following conditions:

  1. Policy Map (with “match cos”) applied on the main interface with the subinterface as dot1q.
  2. Reload the router.

  Workaround: Unconfigure the service-policy from interface and configure it again.

- CSCui65914

  Symptom: Minor or major temperature alarms are reported in the syslog along with the following DATACORRUPTION logs:

  ```
  Aug 5 15:54:30.972 Buc: DATACORRUPTION-SP-1-DATAINCONSISTENCY copy error, -PC=
  0x414DEED4z -Traceback= 4027C4F4 419551C0 414DEED4 414E5BC4 414E0CA0 414E0F00 Aug 5
  15:54:30.972 Buc: C6KENV-SP-4-MINORTEMPALARM interface 10/0 outlet temperature crossed
  threshold #1(=60C). It has exceeded normal operating temperature range.
  ```

  Conditions: This symptom is observed on ES+ series linecards of Cisco 7600 Series Routers.

  Workaround: There is no workaround.

- CSCui67919

  Symptom: QoS policy applied on AToM SVI does not get any matches until the user removes and reapplies the policy. Once the policy is reapplied, the policy works as expected. However, the QoS counters do not get updated and the policy statistics cannot be verified with “show policy-map interface x/x”.

  Conditions: This symptom is observed when the xconnect is applied under SVI and the core facing line card is ES20 running Cisco IOS Release 15.2(4)S3a.

  Workaround: Reapply the policy. Please note that QoS counters in “show policy-map interface xx” will not work but the policy comes in effect after re-applying it.

- CSCui74609

  Symptom: After a RSP switchover the backup pseudowire state is down and never recovers to standby state.

  Conditions: This symptom occurs on CEM circuits in an SAToP environment after an SSO switchover.

  Workaround: There is no workaround.

- CSCui76564

  Symptom: A roaming mobile customer (example: iPASS, Boingo etc.) logs on via a Web-Portal-Page and the ISG doesn't send in the radius accounting-request packet from the V-Cookie to the Radius Server.

  Conditions: This symptom occurs depending on the ISG setup. In this case L & V Cookie must be sent in accounting-request from the ISG to the AAA Server.

  Workaround: There is no workaround.

- CSCui82757

  Symptom: Session query responses in lite sessions have inconsistent calling-station-ID behavior.

  Conditions: This symptom occurs when:

  1. Walkby feature is enabled with L4R & PBHK features applied to lite session.
  2. Session query is sent to ISG.

  Workaround: Do not use calling-station-ID.

- CSCui82817

  Symptom: A tunnel with lower absolute metric is not advertised properly.

  Conditions: This symptom occurs under the following conditions:

  1. When there are multiple tunnels to a destination.
  2. The tunnel with a better metric comes up.
  3. When ISIS is used as IGP and both L1 and L2 are present and configured for TE.

  Workaround: Clear the ISIS sessions.

- CSCui83823

  Symptom: When CU executes show tech or any show commands which gives a long output using putty the SSH2 putty closes prematurely.

  Conditions: This symptom is observed when "term length 0" is enabled, the putty session closes prematurely while executing show tech show memory.

  Workaround: Redirect the output to a file.

- CSCui85019

  Symptom: When the command **show xconnect** is entered, it may result in a memory leak. This can be observed by entering the command **show memory debug leaks chunks** and seeing entries like this:

  ```
  router#show memory debug leaks chunks
  Adding blocks for GD...
  I/O memory
  Address Size Alloc_pc PID Alloc-Proc Name
  Chunk Elements:
  AllocPC Address Size Parent Name
  Processor memory
  Address Size Alloc_pc PID Alloc-Proc Name
  AA3F8B4 2348 6D0B528 97 Exec
  PW/UDP VC event trace
  ```

  Conditions: This symptom is observed when one or more xconnects are configured with UDP encapsulation.

  Workaround: There is no workaround.

- CSCui89069

  Symptom: An ISIS flap is observed on performing SSO.

  Conditions: This symptom occurs when **nsf ietf** is configured and one or more loopbacks are configured as passive interfaces.

  Workaround 1. Use **nsf cisco**.

  Workaround 2. Continue to use **nsf ietf** but configure **ip router isis <process_name>** on the loopback interfaces.

- CSCui90811

  Symptom: While running the Cisco IOS 15.3S release and Cisco IOS 15.4S release software for the L2VPN pseudowire redundancy feature on a Cisco router, the traffic is dropped when the primary pseudowire becomes active.

  Conditions: Initially the primary pseudowire is down due to either a local or a remote core-facing interface being shutdown. The backup pseudowire is active and traffic flows through the backup pseudowire. Later, when the backup pseudowire is down, the primary pseudowire is brought up and becomes active and traffic is not able to flow through primary pseudowire and is dropped.

  Workaround: There is no workaround.

- CSCui99031

  Symptom: In a pair of Cisco 7609-S routers running c7600rsp72043-advipservicesk9-mz.151-3.S5.bin IOS, phase 1 fails to establish due to a "signature invalid!" error when rsa-sig is used for phase 1 authentication.

  Conditions: This symptom occurs under the following conditions:

  - rsa-sig is used for phase 1 authentication
  - site to site tunnel

  Workaround: Use PSK instead of PKI.

- CSCuj00746

  Symptom: On performing an upgrade from 9.512 to 9.523, there is a label allocation failure in VPWS circuits as they are trying to utilize the labels that are already used by the VPLS circuits that are present in the database.

  Conditions: This symptom occurs when both VPWS and VPLS circuits are configured on the same node before upgrading.

  Workaround: Removing the VPLS circuit brings up the VPWS circuits. Reconfiguring the VPLS circuit is also successful with a different local label assigned.

- CSCuj11232

  Symptom: Changing the local label on an existing static (no signaling) Any Transport over MPLS (AToM) pseudowire, or changing the static pseudowire to a dynamic one (with LDP signaling) may cause traffic to fail to traverse the pseudowire.

  Conditions: This symptom is observed when either the configured value of the static local label is changed, or if the pseudowire is changed to a dynamic one.

  Workaround: Completely unconfigure the existing xconnect or pseudowire before entering the new configuration.

- CSCuj11576

  Symptom: A router experiences a crash when BFD is configured.

  Conditions: This symptom occurs when BFD is configured.

Workaround: There is no workaround.

- CSCuj16742

  Symptom: In a pseudowire redundancy configuration, packets may fail to flow even though the xconnect virtual circuit appears to be up.

  Conditions: This symptom has been observed when the xconnect is re-provisioned while the primary pseudowire is down and the backup pseudowire is up. The issue has only been observed on Circuit Emulation (CEM) attachment circuits, but it is possible other attachment circuit types may be affected as well.

  Workaround: Completely unconfigure the xconnect and then reconfigure it.

- CSCuj17482

  Symptom: On a device running low on memory, an EFP is attempted to be deleted, but fails due to lack of memory. The second attempt at removing that same EFP causes the router to restart.

  Conditions: This symptom occurs when the a lot of configuration has been applied to the device, causing high memory usage.

  Workaround: Do not overconfigure the device.

- CSCuj22189

  Symptom: On a Cisco ASR series router, a crash occurs when **mpls ip** is added under the interface.

  Conditions: This symptom occurs when the hidden command **snmp-server hc poll** is already configured.

  Workaround: Ensure that the hidden command **snmp-server hc poll** has not been configured.

- CSCuj26593

  Symptom: Simple IP Dual stack and IPv6 sessions failed to survive an RP switchover.

  Conditions: This symptom occurs when the dual stack session exists.

  Workaround: Do not use the dual stack session.

- CSCuj30702

  Symptom: This bug is specific to port channel sub interface configuration in ES+ card. This bug is not relevant to any other port channel configuration in ES+, that is, EVC/Bridge-Domain over PoCH sub-int etc, and other card types, such as ES20/ LAN cards are free from this bug. Any type of IP communication on port channel sub interfaces in ES+ cards fail. Such an issue is seen only with port channel sub interfaces on ES+ and not seen with port channel main interfaces.

  Conditions: This symptom will only be seen with images where the fix of CSCuh40617 is integrated.

  Workaround: The connections will work fine if it is moved to the main interface or by using EVC BD configurations.

- CSCuj31090

  Symptom: When L2TPv3-based pseudowire is configured between two PE routers and different VLAN ids are used on the ACs on both sides, ES+ on egress PE does not rewrite a dot1q VLAN tag when sending a frame toward CE.

  Conditions: This symptom occurs when:

  1. Both ACs are Ethernet VLAN type.
  2. Different dot1q tag is used on both ACs.

  Workaround: Configure the same dot1q tag for the ACs on both PEs.

- CSCuj39400

  Symptom: A Cisco 3945 series router running Cisco IOS Release 15.2(2)T2 may crash with a bus error. This relates to VOIP_RTCP.

  Conditions: This symprom has been observed to occur often while running SIP debugs. However, at least one identical crash happened after SIP debugs were disabled three days before.

  Workaround: There is no known workaround.

- CSCuj47554

  Symptom: PBHK bundles are not released even after the session is cleared.

  Conditions: This symptom occurs after the session is cleared and the port-bundle status is not shown correctly with **show ip portbundle status** command.

  Workaround: There is no workaround.

- CSCuj52396

  Symptom: In a VPLS Inter-Autonomous System Option B configuration, the virtual circuits between the Autonomous System Border Router (ASBR) and the PE may fail to come up.

  Conditions: This symptom is observed while initially establishing VCs after the ASBR has reloaded.

  Workaround: The **clear xconnect** exec command can be used to clear the VCs that are down.

- CSCuj57367

  Symptom: A 10 gig line card crashes on a Cisco 7600 platform with the following or similar errors:

  ```
  %SYS-DFC3-3-MGDTIMER: Uninitialized timer, timer stop, timer = 30CCCFB0. -Process= "RO
  Notify Timers", ipl= 0, pid= 7 -Traceback= 2060E1BCz 2060E8E4z %SYS-DFC3-3-MGDTIMER:
  Uninitialized timer, timer stop, timer = 30CCD154. -Process= "RO Notify Timers", ipl=
  0, pid= 7 -Traceback= 2060E1BCz 2060E8E4z %SYS-DFC3-3-MGDTIMER: Uninitialized timer,
  timer stop, timer = 30CCCFB0. -Process= "RO Notify Timers", ipl= 0, pid= 7 -Traceback=
  2060E1BCz 2060E8E4z
  08:54:43 Central Tue Oct 1 2013: Address Error (load or instruction fetch) exception,
  CPU signal 10, PC = 0x20642A08
  ```

  Conditions: This symptom occurs when a large number of IPC messages are used.

  Workaround: There is no workaround.

  More Info: On mac-scaling, the L2-DRV application sends more ICC messages(though not always). But periodically(approximately 2-3 minutes), some burst of around 150 ICC messages are sent by the SP towards the RP. This means that mac-scaling has a direct correlation with the number of IPC messages being sent.

- CSCuj58299

  Symptom: Interface input queue starts to become congested. The input queue can reach the input queue maximum which will cause problems for all control-plane and punted traffic (management, routing protocols, call control, etc).

  Example from the **show interface** output:

  ```
  Input queue: 76/75/0/5549 (size/max/drops/flushes); Total output drops: 0
  ```

  It may seem like the router becomes “unresponsive” and may require a reboot to restore service. Access from the console will still be possible. After some time, the input queue can clear on its own.

  Conditions: This symptom is observed under the following conditions:

  1. Router serves as a SIP-SIP CUBE

2. Packets that are congesting input queue are RTCP packets. Check "show buffers input-interface [interface] packet". (RTCP packets are most commonly odd source/destination UDP ports in the range 16384 - 32768)
3. CUBE receives a 180 without SDP followed by a 180 with SDP on one of the call legs (collect ’debug ccsip message’ for a period of time leading up to and including when you see the input queue begin to fill)

Workaround: Perform the following workaround:

1. Increase input hold-queue to a very large value.
2. Create an ACL to block RTCP traffic on interfaces (not possible if RTCP is used for inactivity detection).
3. Influence downstream call flows such that CUBE does not receive 180 without SDP followed by a 180 with SDP.

- CSCuj60533

  Symptom: Repeated CPUHOG messages may be seen along with a crash when “reload” is issued just after a bootup.

  Conditions: This symptom occurs when the line cards are still booting up and are in other states.

  Workaround: Issue “reload” after the line cards have booted.

- CSCuj65057

  Symptom: The **ip vrf forwarding** command under “aaa” is deleted after reloading the stack master.

  Conditions: This symptom occurs after reloading the stack master switch.

  ```
  aaa new-model
  !
  aaa group server tacacs+ TACACS+
  ip vrf forwarding VRF01
  !
  ip vrf VRF01
  rd x.x.x.x ---------
  ```

  Workaround: Use the **vrf definition** command instead of the **ip vrf command to define vrf**. (This command is supported on Cisco IOS Release 12.2(58)SE or later releases.)

- CSCuj66352

  Symptom: A system crash is observed in the SNMP engine.

  Conditions: This symptom occurs under the following conditions:

  – ?show subscriber session?
  – polling the ISG-MIB
  – clearing the subscriber

  Workaround: Do not use SNMP polling.

- CSCuj68932

  Symptom: L2TPv3 tunnel with digest fails to establish. Cisco IOS device gives the following messages when “debug l2tp all” and “debug l2tp packet detail” are enabled:

  ```
  L2TP _____:________: ERROR: SCCRQ AVP 59, vendor 0: unknown L2TP _____:________:
  Unknown IETF AVP 59 in CM SCCRQ
  ```

Conditions: This issue is observed when IOS device peers with non-IOS device that sends IETF L2TPv3 digest AVP (IETF AVP 59) in L2TP control message. This issue is present in S images starting from Cisco IOS Release 12.2(33)XNC and in T train from Cisco IOS Release 15.3(2)T.

Workaround: There is no workaround.

- CSCuj75952

  Symptom: The Cisco ASR 1000 route processor reloads.

  Conditions: This symptom occurs during PPPoA session establishment if CAC determines that resources are low and HW-assisted CAC needs to be enabled. The router is used to terminate PPPoA sessions and Call Admission Control (CAC) is enabled.

  Workaround: Disable Call Admission Control.

- CSCuj78636

  Symptom: A memory leak is observed in the IP Switching segment.

  Conditions: This symptom occurs if a subscriber roams with the same MAC address but a different IP address . This happens only for L2 roaming and not for L3 roaming.

  Workaround: There is no workaround.

- CSCuj88523

  Symptom: In a pseudowire redundancy configuration, traffic may fail to flow after a switchover to a backup pseudowire.

  Conditions: This symptom occurs on the Cisco 7600 series routers.

  Workaround: Execute the following commands on the attachment circuit interface:

  - **shutdown**
  - **no shutdown**

- CSCuj96893

  Symptom: Cisco router hangs and it stopped passing the traffic. Customer needs to reload the router to make it work until it hangs next time. It hangs sometimes once in month.

  Conditions: This issue is seen with more than one router.

  Workaround: There is no workaround.

- CSCuj99537

  Symptom: Not all LI streams that are properly configured via SNMPv3 and appropriate ACLs and are programmed in TCAM, are intercepted and forwarded towards MD.

  Conditions: This symptom occurs in an SIP-400 based LI.

  Workaround: Remove and reapply the problematic tap but it doesn’t prevent the problem from reoccurring if new LI taps are applied via SNMPv3

- CSCuj99819

  Symptom: MVPN GRE tunnels are not established.

  Conditions: BGP has a VPN peer configured using an update-source that does not have PIM enabled.

  Workaround: There is no workaround.

- CSCul11995

  Symptom: An L2TPv3 session fails to establish and Cisco IOS receives a StopCCN message from the peer with the following message in response to its ICRP message:

  ```
  "No handler for attr 68 (68)"
  ```

Conditions: This symptom occurs when IOS device peers with non-IOS devices send IETF L2TPv3 Pseudowire Type AVP (IETF AVP 68) in an ICRP message.

Workaround: There is no workaround.

- CSCul14571

  Symptom: A Cisco router can crash after OSPFv3 is unconfigured from an interface.

  Conditions: This symptom is observed when NSR is enabled.

  Workaround: Unconfigure NSR before unconfiguring OSPFv3 from an interface.

  More Info: This is extremely rare issue; the OSPFv3 should be in a process of checkpointing LSA from primary RP to standby while an interface from which the LSA was received is unconfigured.

- CSCul24682

  Symptom: L2TP LNS puts a non-negotiated magic number to LCP packets. The PPPoE client may terminate the session prematurely due to the unknown magic number.

  Conditions: This symptom occurs when L2TP LAC does not negotiate the magic number with the PPPoE client and L2TP LNS does not renegotiate options with the PPPoE client.

  Workaround: Configure "lcp renegotiation always" on L2TP LNS.

- CSCul27327

  Symptom: On the Cisco c7600 router, if PIM is configured on the port-channel and on the port members, any failure on one of the port members will disable the FE CAM.

  Conditions: This symptom occurs when PIM is configured on the port members.

  Workaround:

  1. Do not configure PIM sparse-mode on the port members even though the CLI is accepted.
  2. In case the PIM sparse-mode is configured on the port members, remove it from the port members and the port-channel and then reapply the PIM configuration on the port-channel only.

  Further Problem Description: A similar issue (CSCtf75608) is seen on the Cisco Catalyst 6500 Series Switches, but the workaround is to configure PIM on the port-channel and the port members to avert the FE CAM to be disabled in the event of one of the port members failing.

- CSCul40898

  Symptom: After reloading the router or fresh service-instance configuration, traffic received from the access is sent to the core without a dummy VLAN header. This traffic is received by a remote PE2 and sent to switch with a missing VLAN header. Therefore CE2 drops received packets. When the issue is removed, captured traffic in the core contains a dummy VLAN header.

  Conditions: This symptom is occasionally observed when the router is reloaded and is consistently observed when a new service instance is configured as an xconnect member.

  Workaround: Perform **shutdown** followed by **no shutdown** on the service instance.

- CSCul47135

  Symptom: On Cisco ASR 1000 routers, services are not removed or applied from the active subscriber sessions when CoA is sent from the radius server. The router sends wrong values in response to the CoA request packet.

  Conditions: This symptom occurs when 15.2(20130918:081157) is run.

  Workaround: There is no workaround.

- CSCul54254

  Symptom: Invalid LSAs are not flushed by the router which has their Advertising Router ID. Specifically, Router LSAs which do not have LSID of 0 will not be flushed if the router does not re-originate them, and any LSA with a type that the router does not recognize.

  Lingering LSAs could lead to incorrect routing in some very obscure instances. For example, stale Router LSA fragments from two neighboring routers would need to remain in the network. There would not be a routing problem if only one router's stale Router LSA fragment was allowed to linger.

  Conditions: There are several possible scenarios that could lead to this symptom. One example is that a router is configured with many interfaces attached to an OSPFv3 instance such that it originates more than one Router LSA fragment. Then the router is reloaded before the configuration is saved, and after the reload it does not reoriginate some of the Router LSA fragments.

  Workaround: There is no workaround.

- CSCul65614

  Symptom: The FAN-MOD-6SHS module consumes more power than expected(should be around 180W).

```
#sh power
<SNIP>
Fan Type Watts A @42V State
---- ------------------ ------- ------ -----
1 FAN-MOD-6SHS 427.14 10.17 OK
```

  Conditions: This symptom occurs when the ES+ Combo card is placed in slot-1 of 7600 chassis.

  Workaround: Place ES+ Combo cards in any other slot other than slot-1 of 7600 chassis.

- CSCul86211

  Symptom: When LNS switches off while the sessions keep on establishing at LAC, LAC finds the l2tp db memory exhausted after sometime. Due to this, it fails to update the session in the database and during this period a crash is observed.

  Conditions: This symptom occurs when LAC tries to add l2tp session in the database and fails to do so. In order to handle this error condition, LAC frees the l2tp and l2x session twice. This double free is the reason for crash.

  Workaround: There is no workaround.

- CSCul87037

  Symptom: An "sg subrte conte" chunk leak occurs while roaming.

  Conditions: This symptom occurs after an account-logoff and if service permit is configured in control policy. In case of a service permit, the subscriber remains unauth and is redirected to the portal once again. Post successful second account logon and the subscriber session is cleared by timeout or cli, the leak is seen and the same client will not be able to create the session once again. The leak is seen after simulating for the second time account-logon. And if service permit is configured.

  In case of service disconnect configured under account-logoff, account-logon is not a practical scenario as the portal is not reachable for the client.

  Workaround: Use **service disconnect** for **event account-logoff**.

```
class type control always event account-logoff
1 service disconnect delay 10
!
```

- CSCul92497

  Symptom: The Cisco 7600 router providing layer2 EoMPLS services may stop forwarding ingress and egress traffic for an xconnect for which a backup peer config has been applied.

  Conditions: This symptom occurs in Cisco 7600 routers running Cisco IOS Release 15.2(4)S4a with ES+ cards (access/core facing) and xconnect configured under a service instance.

  Workaround: Clear the xconnect on the Cisco 7600 router side. Clearing on the remote size does not have an effect.

- CSCum65501

  Symptom: IPv6 CoPP ACL in PI matches traffic incorrectly for sw-switched paks. Packets are not hit against IPv6 ACE matching on L4 protocol. This causes traffic to be classified incorrectly.

  Conditions: This symptom occurs with recent Cisco IOS images. Results are as expected on Cisco IOS Release 12.2(33)SRE9a. However, it is broken in Cisco IOS Release 15.2(4)S4a onwards.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.2(4)S4a

Cisco IOS Release 15.2(4)S4a is a rebuild release that addresses a critical issue impacting 7600 platform for Cisco IOS Release 15.2(4)S.

- CSCuj30702

  Symptom: This bug is specific to port channel sub interface configuration in ES+ card. This bug is not relevant to any other port channel configuration in ES+, that is, EVC/Bridge-Domain over PoCH sub-int etc, and other card types, such as ES20/ LAN cards are free from this bug. Any type of IP communication on port channel sub interfaces in ES+ cards fail. Such an issue is seen only with port channel sub interfaces on ES+ and not seen with port channel main interfaces.

  Conditions: This symptom will only be seen with images where the fix of CSCuh40617 is integrated.

  Workaround: The connections will work fine if it is moved to the main interface or by using EVC BD configurations.

Resolved Caveats—Cisco IOS Release 15.2(4)S4

Cisco IOS Release 15.2(4)S4 is a rebuild release for Cisco IOS Release 15.2(4)S. The caveats in this section are resolved in Cisco IOS Release 15.2(4)S4 but may be open in previous Cisco IOS releases.

- CSCsv74508

  Symptom: If a linecard is reset (either due to an error or a command such as hw-module slot reload) at the precise time an SNMP query is trying to communicate with that linecard, the RP could reset due to a CPU vector 400 error.

  Conditions: This symptom occurs when the linecard is reset(either due to error or a command such as hw-module slot reload) at the precise time an SNMP query is received.

  Workaround: There is no workaround.

- CSCtd45679

  Symptom: The standby supervisor reloads after removing an IPSLA probe via CLI:

  ```
  R7600(config)#no ip sla 1 R7600(config)# 06:53:31: Config Sync: Line-by-Line sync
  verifying failure on command: no ip sla 1 due to parser return error
  ```

```
06:53:31: rf_reload_peer_stub: RP sending reload request to Standby. User:
Config-Sync, Reason: Configuration mismatch R7600(config)# 06:53:31:
%RF-SP-5-RF_RELOAD: Peer reload. Reason: Proxy request to reload peer R7600(config)#
06:53:31: %OIR-SP-3-PWRCYCLE: Card in module 6, is being power-cycled (RF request)
R7600(config)# 06:53:32: %PFREDUN-SP-6-ACTIVE: Standby processor removed or reloaded,
changing to Simplex mode R7600(config)#
```

Conditions: This issue only occurs if the probe is configured via SNMP.

Workaround: Remove the probe via SNMP.

More Info: This issue is applicable to a Cisco Catalyst 6500 platform running Cisco IOS 12.2SX releases. It may also affect other high availability (HA) platforms running Cisco IOS 12.2 or 15.X releases.

- CSCtj61284

  Symptoms: NAT overload does not work for non-directly connected destinations in MPLS-VPN configurations.

  Conditions: The symptom is observed with NAT overload configured to NAT traffic coming over an MPLS VPN to internet (via a VRF-enabled interface).

  Workaround: There is no workaround.

- CSCtr88785

  Symptoms: Following an upgrade from Cisco IOS Release 12.4(24)T2 to Cisco IOS Release 15.1(4)M1, crashes were experienced in PKI functions.

  Conditions: This symptom is observed on a Cisco 3845 running the c3845-advipservicesk9-mz.151-4.M1 image with a PKI certificate server configuration.

  Workaround: Disable Auto-enroll on the CA/RA. Manually enroll when needed.

- CSCts63581

  Symptoms: The standby PRE4 resets after write memory command at “Failed to sync private-config to standby RP”.

  Conditions: The symptom is observed with a scaled configuration that is more than NVRAM can store.

  This may occur when the standby NVRAM is locked by some other process and when config sync tries to access the standby NVRAM it fails. It then restarts the standby.

  Workaround: Significantly decrease configuration size, if possible.

- CSCtx99353

  Symptom: %SYS-3-INVMEMINT: Invalid memory action (malloc) at interrupt level.

  Conditions: The symptom is observed when music on hold (MOH) is enabled.

  Workaround:

  1. Remove the route list from the multicast MOH CLI, so that you can still have music on hold and can continue the feature.
  2. Disable the MOH (but no music comes on hold).

- CSCty26035

  Symptom:

  1. There is a discrepancy in the inbound and the outbound SA lifetime in the standby router.
  2. The KB lifetime in a standby router is greater than that of the active router, when a KB lifetime rekey occurs.

3. The ping will not go through after applying a dynamic crypto map.

Conditions: The issues are seen after establishing the session between the HA routers and various test conditions.

Workaround: There is no workaround.

- CSCty59423

Symptoms: Memory leak seen with following messages:

```
Alternate Pool: None Free: 0 Cause: No Alternate pool -Process= "VOIP_RTCP", ipl= 0,
pid= 299 -Traceback= 0x25B1F0Cz 0x25AB6CBz 0x25B1029z 0x46C02Ez 0x46C89Bz 0x46BCC2z
0x471D12z 0x43EF59Ez 0x43DD559z 0x43DCF90z %SYS-2-MALLOCFAIL: Memory allocation of 780
bytes failed from 0x46C02E, alignment 32
```

Conditions: The conditions are unknown.

Workaround: There is no workaround.

- CSCty77441

Symptom: Memory leaks are observed after unconfiguring BFD sessions.

Conditions: This symptom occurs after BFD sessions are unconfigured.

Workaround: There is no workaround.

- CSCtz90697

Symptoms: EIGRP authentication is not working.

Conditions: The symptom is observed when authentication is configured with key-id 0.

Workaround: Use any other key-id for authentication.

- CSCua21049

Symptom: User configures a recursive multicast-only IPv6 static route. Although the static route next-hop apparently resolves in the context of the ipv6 multicast-unicast routing table, the route is not inserted in the routing table.

Conditions: This symptom occurs when a user has configured IPv6 multicast. User has configured a recursive multicast-only ipv6 static route.

For example:

A user has configured recursive multicast-only static:

```
ipv6 route 2001:DB8:11::1/128 2001:DB8:16::1 multicast
```

Next-hop apparently resolves in context of the multicast-unicast routing table:

```
rtr> show ipv6 routing multicast IPv6 Multicast Routing Table - default - 8 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route B - BGP, R -
RIP, H - NHRP, I1 - ISIS L1 I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D -
EIGRP EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination NDr -
Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1 OE2 - OSPF ext 2, ON1 -
OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2 ls - LISP site, ld - LISP dyn-EID C
2001:DB8:16::/112 [0/0] via Ethernet0/1, directly connected
```

However, the static route is not present in routing table and “show ipv6 static multicast detail” shows the route resolves outside the table:

```
rtr> show ipv6 static multicast detail IPv6 Static routes Table - default Codes: * -
installed in RIB, u/m - Unicast/Multicast only U - Per-user Static route N - ND Static
route M - MIP Static route P - DHCP-PD Static route R - RHI Static route m
2001:DB8:11::1/128 via 16::1, multicast distance 1 Route resolves outside the table
```

Workaround: There is no workaround.

- CSCua35161

  Symptom: On the DMVPN HUB, some crypto maps still exist after removing Tunnel protection from the Tunnel interface.

  Conditions: This symptom occurs with scaling test.

  Workaround: There is no workaround.

- CSCua55797

  Symptoms: The **privilege exec level 0 show glbp brief** command causes the memory to be depleted when the **show running** or **copy running-config startup-config** commands are used. The configurations will then show this:

  ```
  privilege exec level 0 show glbp GigabitEthernet0/0 brief brief brief brief brief
  brief brief privilege exec level 0 show glbp GigabitEthernet0/0 brief brief brief
  brief brief brief privilege exec level 0 show glbp GigabitEthernet0/0 brief brief
  brief brief brief privilege exec level 0 show glbp GigabitEthernet0/0 brief brief
  brief brief privilege exec level 0 show glbp GigabitEthernet0/0 brief brief brief
  privilege exec level 0 show glbp GigabitEthernet0/0 brief brief privilege exec level 0
  show glbp GigabitEthernet0/0 brief privilege exec level 0 show glbp privilege exec
  level 0 show
  ```

  Removing the configurations causes this to happen over and over until the telnet session is terminated:

  ```
  priv_push : no memory available priv_push : no memory available priv_push : no memory
  available priv_push : no memory available priv_push : no memory available
  ```

  If the configurations are saved and device is reloaded, the device will not fully boot until the configurations are bypassed.

  Conditions: This issue happens after the **privilege exec level 0 show glbp brief** command is entered and saved.

  Workaround: Reload the router before saving the configurations.

- CSCua75781

  Symptoms: CME reloads for E911 call ELIN translation for incoming FXS/FXO trunk.

  Conditions: The symptom is observed from Cisco IOS interim Release 15.3(0.2)T.

  Workaround: There is no workaround.

- CSCub04965

  Symptom: Multiple symptoms may occur including:

  - Multiple sessions established to TACACS+ server which never clear are seen in the output of **show tcp brief**.
  - Pings to the loopback address from directly connected equipment suffers packet loss.
  - Traffic and pings through the switch suffers packet loss.
  - CPU utilization remained stable and below 10% when the issue was occurring, the interface counters were not reporting any errors or drops.
  - TACACS+ authentication errors, authorization errors, or accounting errors.
  - SSH/TELNET via VTY not accessible.
  - If condition exists for a period of time the switch may stop passing traffic.

Conditions: The symptom is observed when the device is configured with TACACS+. It is seen mostly on Cisco 3750/3760 switches, but has been observed on Cisco 6500 switches.

Workaround:

- Remove the AAA and TACACS+ server configuration.
- Clear the existing TCP connections with **clear tcp tcb**.
- Reconfigure the TACACS+ server configuration to use "single-connection" mode.
- Reconfigure the AAA configuration.

Mitigation using EEM: A Cisco IOS Embedded Event Manager (EEM) policy that is based on Tool Command Language (Tcl) can be used on vulnerable Cisco IOS devices to identify and detect a hung, extended, or indefinite TCP connection that causes the symptoms to be observed. The policy allows administrators to monitor TCP connections on a Cisco IOS device. When Cisco IOS EEM detects hung or stale TCP connections, the policy can trigger a response by sending a syslog message or a Simple Network Management Protocol (SNMP) trap to clear the TCP connection. The example policy provided in this document is based on a Tcl script that monitors and parses the output from two commands at defined intervals, produces a syslog message when the monitor threshold reaches its configured value, and can reset the TCP connection. The EEM script is available at:

https://supportforums.cisco.com/docs/DOC-19344

- CSCub18622

  Symptom: Dynamic ACL does not get applied to the interface ACL, but the user shows up in the **show ip auth-proxy cache** command output.

  Conditions: This symptom occurs when auth proxy is configured on a tunnel interface.

  Workaround: Move the auth-proxy rules onto a physical interface.

- CSCub34534

  Symptom: A basic call between 2 SIP phones over SIP trunk (KPML-enabled) fails.

  Conditions: This symptom is observed with Cisco ISR G2 platforms.

  Workaround: There is no workaround.

- CSCub40547

  Symptoms: ES+ module crashes with the followoing error message:

  ```
  %NP_DEV-DFC1-2-WATCHDOG: Watchdog detected on NP 0
  ```

  Conditions: The issue is specific to the type of packet and its content which is unique when vidmon is configured.

  Workaround: Remove vidmon configuration.

- CSCub46423

  Symptoms: Connecting from Windows 7 L2TP/IPSec client to the VPN fails when using HSRP virtual IP as a gateway IP and Error 788 is displayed.

  Conditions: This symptom is observed with Cisco IOS Release 15.2(3)T or later releases, and the Windows 7 L2TP/IPsec VPN client.

  Workaround: Downgrade to Cisco IOS Release 15.1(3)T.

- CSCub52278

  Symptom: The DVTI Virtual Access interface may flap during rekey with a large number of IKEv2/IPSec tunnels.

Conditions: This symptom occurs when IKEv2 is used in large scale deployment.

Workaround: There is no workaround.

- CSCub68199

  Symptom: A Cisco Router configured for IPv6/IPv4 Native IP Routes or l2-connected ISG sessions may reload with following errors in crashinfo:

  ```
  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = IP Inband Session Initiator
  ```

  Conditions: This symptom occurs due to high or extended duration of setup and tear-down rate of sessions. Time to potential reload can vary depending on call volume and duration of session cycling.

  Workaround: There is no workaround.

- CSCub93641

  Symptom: The load balancing feature of the Flex-VPN solution of Cisco IOS does not provide authentication facilities to avoid a non authorized member to join the load balancing cluster. Thus, an attacker may impact the integrity of the Flex-VPN system by inserting a rogue cluster member and having the load balance master to forward a VPN session to it. A number of secondary effects, including black-holing of some of the VPN traffic may be triggered by this issue.

  Conditions: This symptom occurs in Flex-VPN with the Load Balancing feature active.

  Workaround: Using CoPP and interface access-list may be used to allow only trusted router to join the load balancer cluster

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4.3/3.9: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:P/A:N/E:F/RL:W/RC:C

  CVE ID CVE-2012-5032 has been assigned to document this issue. Additional information on Cisco’s security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCub95285

  Symptoms: No logging messages are seen when configuring the syslog server in CLI mode until configuration mode is exited. However when unconfiguring the syslog server, syslog messages will appear within configuration mode.

  Conditions: The symptom is observed when, in CLI configuration mode, you enter the following command:

  ```
  Router(config)#logging host 1.2.3.4 transport tcp
  ```

  Workaround: There is no workaround.

- CSCuc08477

  Symptom: All EOS and non EOS entries are missing for mLDP labels in the mid/bud node.

  Conditions: This symptom may occur due to random path flap mLDP tree changes.

  Workaround: Removing and adding the mLPD tree will trigger re-programming.

- CSCuc11958

  Symptom: 7600-SIP-400 linecard crash seen with SPA reload.

  Conditions: The symptom is observed with a SPA reload.

  Workaround: There is no workaround.

- CSCuc22651

  Symptom: A router may experience a crash in the “BGP Task” process during best path selection.

  Conditions: In a rare corner case, when the last remaining paths are deleted around the same time by two different threads of execution, a null pointer exception can be raised in the “BGP Task” process.

  Workaround: There is no workaround.

- CSCuc25995

  Symptoms: A router unexpectedly reboots and a crashinfo file is generated. The crashinfo file contains an error similar to the following:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address 04:52:23 UTC Wed Sep 19 2012 addr=0x4,
  pc=0x26309630z , ra=0x26309614z , sp=0x3121BC58
  ```

  Conditions: This occurs when IPsec is used. More precise conditions are not known at this time.

  Workaround: There is no workaround.

- CSCuc34973

  Symptom: There is a CPU hog with G8302.

  Conditions: This symptom occurs when the router is reloaded.

  Workaround: There is no workaround.

- CSCuc47356

  Symptoms: Static routes are not getting removed.

  Conditions: This symptom is observed with Smap - Smap. Removal of CLI does not remove the static route.

  Workaround: Remove the ACL before removing the SA.

- CSCuc51879

  Symptom: Traffic loss occurs on the Cisco ASR 1000 Series Routers during an RP SSO switchover.

  Conditions: This symptom occurs during an RP SSO switchover on the Cisco ASR 1000 Series Routers.

  Workaround: There is no workaround.

- CSCuc59858

  Symptoms: Valid dynamic authorization requests which are not retransmissions are marked as retransmission.

  Conditions: This may occur when valid dynamic authorization requests with the same RADIUS packet identifier is sent from different source ports.

  Workaround: There is no workaround.

- CSCuc61302

  Symptoms: The symptoms for XE38, XE37 and mcp_dev are different for this DDTS. On mcp_dev, VPLS PW is not coming up, but on XE37 and XE38, static mac commands are missing after a reload.

  Conditions: This occurs only on reload. The configured static mac commands are missing after a reload.

  Workaround: There is no workaround other than re-entering the static mac commands.

- CSCud02391

  Symptoms: The EIGRP routes are not coming up after removing and reenabling the tunnel interface.

  Conditions: This symptom is observed when EIGRP routes do not populate properly.

  Workaround: There is no workaround.

- CSCud11078

  Symptoms: Removal of the service instance on the target device causes a crash.

  Conditions: This symptom is not consistently reproducible on all configurations as the underlying cause is a race condition.

  Workaround: De-schedule the probe before removing the service instance.

- CSCud13768

  Symptom: RP crashes while trying to verify UDP-JITTER in IP SLAs VRF-lite.

  Conditions: This symptom occurs while trying to verify IP SLAs UDP Jitter operation.

  Workaround: There is no workaround.

- CSCud24806

  Symptom: Compared to V1 ATM SPA, V2 SPAs have more latency and bad bandwidth partition.

  Conditions: The symptom is observed under the following conditions:

  1. V2 SPA configured in L3 QoS mode.
  2. Policy map contains “no priority queue”.
  3. Policy map has more than one QoS class.
  4. Each class has a WRED profile configured.

  Workaround: While using a policy-map with a WRED profile, use the drop-probability value as 8. This improves the partition.

- CSCud45339

  Symptom: The **ping mpls tp tunnel-tp lsp act** indicates that the LSP is unreachable even though it is functioning correctly.

  Conditions: This symptom occurs during MPLS Transport Profile (TP) and OAM GAL handling.

  Workaround: There is no workaround.

  More Info: The MPLS Generic Associated Channel (GAL) may not be processed in the exception handling path, which impacts OAM ping mpls for tunnel-tp.

- CSCud55286

  Symptoms: Traffic drops for sometime after doing a switchover.

  Conditions: The symptom is observed when a switchover is performed on a Cisco ASR 903.

  Workaround: Put a neighbor command where the neighbor has no meaning and will never be up. This will solve the timing issue.

- CSCud58457

  Symptom: Standby interface stays UP/UP after a reload:

  ```
  BGL.S.15-ASR1004-1#sh int des Interface Status Protocol Description Te0/0/0 down down
  Te0/1/0 up up Te0/2/0 down down Te0/3/0 up up Gi0 admin down down
  ```

  It should be like this :

```
BGL.S.15-ASR1004-1#sh int des Interface Status Protocol Description Te0/0/0 down down
Te0/1/0 up up Te0/2/0 down down Te0/3/0 standby mode down Gi0 admin down down
```

Conditions: The symptom is observed when “backup interface” and “carrier-delay” are configured under the interface:

```
interface TenGigabitEthernet0/1/0 backup interface TenGigabitEthernet0/3/0 ip address
10.163.137.29 255.255.255.224 logging event link-status carrier-delay up 1
carrier-delay down msec 0 cdp enable hold-queue 4096 in hold-queue 4096 out !
interface TenGigabitEthernet0/3/0 mac-address d867.d9dd.ff10 no ip address logging
event link-status carrier-delay up 1 carrier-delay down msec 0 cdp enable hold-queue
4096 in hold-queue 4096 out !
```

Workaround: Flap the standby interface.

- CSCud83835

  Symptoms: An IPsec VPN tunnel fails to be established. The **debug crypto ipsec** command shows no output when attempting to bring up the tunnel.

  Conditions: This symptom occurs when all of the following conditions are met:

  1. The crypto map is configured on a Virtual-Template interface.
  2. This Virtual-Template interface is configured with “ip address negotiated”.
  3. The tunnel is initiated locally (in other words, if the tunnel is initiated by the peer, it comes up correctly).

  Workaround: Downgrade to Cisco IOS Release 15.2(2)T3 or earlier releases or always initiate the VPN tunnel from the peer.

- CSCud86954

  Symptom: Some flows are not added to the Flexible Netflow cache, as indicated by the “Flows not added” counter increasing in the **show flow monitor statistics** command output. “Debug flow monitor packets” shows “FNF_BUILD: Lost cache entry” messages, and after some time, all cache entries are lost. At that moment, debug starts showing “FLOW MON: ip input feature builder failed on interface couldn’t get free cache entry”, and no new entries are created and exported (“Current entries” counter remains at 0).

  The following is sample output when all cache entries are lost:

```
Router#sh flow monitor FNF-MON stat Cache type: Normal Cache size: 4096 Current
entries: 0 High Watermark: 882
Flows added: 15969 Flows not added: 32668 Flows aged: 15969 - Active timeout ( 1800
secs) 0 - Inactive timeout ( 15 secs) 15969 - Event aged 0 - Watermark aged 0 -
Emergency aged 0
```

  Conditions: This symptom occurs when all of the following are true:

  - Flexible Netflow is enabled on a DMVPN tunnel interface.
  - Local policy-based routing is also enabled on the router.
  - Local PBR references an ACL that does not exist or an ACL that matches IPsec packets.

  Workaround:

  1. Make sure that the ACL used in the local PBR route-map exists and does not match IPsec packets sent over the DMVPN tunnel interface.
  2. Disabling encryption on the tunnel interface, or changing tunnel mode from mGRE to GRE also removes this bug.
  3. The issue will not be seen if FNF is not configured, or if FNF is configured but is not monitoring VPN traffic.

- CSCud88483

  Symptom: In a GETVPN and IPsec redundant configuration combination, if you reload a secondary group member in the topology it will cause TEK registration of the group member to be lost once the router comes back up and the HSRP does a state transition to standby.

  Conditions: The symptom is observed with a GETVPN with IPsec redundancy configuration.

  Workaround: Wait for the next rekey or issue **clear crypto gdoi**.

- CSCue01146

  Symptom: SNMP GET fails for VPDN-related MIB.

  Conditions: This symptom occurs while receiving an SNMP GET for the MIB before all VPDN configurations are applied.

  Workaround: Reload the router.

- CSCue09385

  Symptom: Active RP crash during sessions bring up after clearing PDP.

  Conditions: The symptom is observed after clearing PDP.

  Workaround: There is no workaround.

  More Info: This is a negative test where DHCP IP under APN on IWAG is the access interface IP. In real world, we do not configure access interface IP as a DHCP IP for an APN.

- CSCue25526

  Symptom: Router crashes when configuring FNF interface bind.

  Conditions: This symptom occurs when an interface bind is removed in a session before the first session bind is complete.

  Workaround: Do not remove the bind in the second session until the first session bind is complete.

- CSCue28318

  Symptoms: A Cisco router doing authentication proxy may unexpectedly reload when running the **test aaa command** command.

  Conditions: This symptom occurs when the router is using LDAP authentication and has a misconfigured LDAP authentication configuration.

  Workaround: Correct the misconfiguration.

- CSCue32707

  Symptom: crypto pki export <> causes crash.

  Conditions: This symptom is observed in when a SUB CA trustpoint is configured and a trustpoint is configured and enrolled to that SUB CA.

  Workaround: If possible, have the trustpoint on a separate box.

- CSCue39518

  Symptom: A Cisco 7200 with VSA fails to encrypt traffic under specific conditions.

  Conditions: The symptom is observed under the following conditions:

  - Cisco 7200 has IPsec SSO configured with HSRP. Dynamic crypto map is configured. Remote sides have static crypto map to this device.
  - All the 15.x codes to the latest Cisco IOS 15.2(4)M2 are affected.
  - Issue is not seen in the Cisco IOS 12.4 codes.

  - Issue not seen when IPsec SSO and HSRP are removed.

  Workaround: There is no workaround.

- CSCue47586

  Symptom: For an MGRE tunnel, internal VLANs are not allocated in the standby supervisor.

  Conditions: The symptom is observed when an HA router boots up with MGRE tunnel configurations. Internal VLANs are not allocated in the standby supervisor due to a sync issue during bootup.

  Workaround: There is no workaround.

- CSCue57495

  Symptom: Traceback is observed with the following error message:

```
standby cannot allocate VLAN for Tunnel Rsvd Vlan
```

  Conditions: The issue seen while configuring L2VPN and L3VPN with scaled tunnel configurations.

  Workaround: There is no workaround.

- CSCue59592

  Symptom: Multiple crashes observed with the following tracebacks after upgrading the Cisco IOS Release from 12.2(33)SRC1 to 12.2(33)SRE6:

```
*Jul 27 01:39:33 SUM: %SCHED-3-SEMLOCKED: CMFI RP process attempted to lock a
semaphore, already locked by itself -Traceback= 87807BC 999A314 9E1684C 9E17E4C
9E18074 AA9B25C AA9B2C8 AAAA270 A1D33B4 A1D3474 A1D61A4 A1D14B0 AAC8A28 9E1909C
9E19F1C 9E1D4FC *Jul 27 01:39:33 SUM: %SCHED-3-SEMLOCKED: CMFI RP process attempted to
lock a semaphore, already locked by itself -Traceback= 87807BC 999A314 9E1684C 9E17E4C
9E18074 AA9B25C AA9B2C8 AAAA270 A1D33B4 A1D3474 A1D61A4 A1D14B0 AAC8A28 9E1909C
9E19F1C 9E1D4FC *Jul 27 01:39:33 SUM: %SCHED-3-SEMLOCKED: CMFI RP process attempted to
lock a semaphore, already locked by itself -Traceback= 87807BC 999A314 9E1684C 9E17E4C
9E18074 AA9B25C AA9B2C8 AAAA270 A1D33B4 A1D3474 A1D61A4 A1D14B0 AAC8A28 9E1909C
9E19F1C 9E1D4FC
```

  Conditions: The symptom is observed with a combination of BGP VPNv4 prefixes + PBR enabled on the interface for the VRF and during upgrade of image or reload of the device. If "mls mpls recirc agg" is enabled in global mode, then this crash will not be observed.

  Workaround: Enable "mls mpls recirc agg" in global mode.

- CSCue65405

  Symptom: SAs do not get installed in GETVPN GM.

  Conditions: The symptom is observed when the key server is configured with "receive-only" SAs.

  Workaround: Remove receive-only configuration at the key server.

- CSCue65498

  Symptoms: Wrong CIR is getting cloned to the VA interface.

```
Dialer1 Service-policy output: OPT3-DIALER-4b-TR25 Class-map: CRI-OUT (match-any)
police: cir 8 % cir 819000 bps, bc 25593 bytes <<<<<
Virtual-Access3 Service-policy output: OPT3-DIALER-4b-TR25 Class-map: CRI-OUT
(match-any) police: cir 8 % cir 8000000 bps, bc 250000 bytes <<<<<
```

  Conditions: This symptom is observed with the PPPoE dialer/client configuration.

  Workaround: Remove and reapply the service-policy under the Dialer interface.

- CSCue68761

  Symptom: A leak in small buffer is seen at ip_mforward in Cisco IOS Release 15.1(4)M3.

  ```
  Device: Cisco 2911 Cisco IOS: c2900-universalk9-mz .SPA.151-4.M3.bin
  ------------------ show buffers ------------------
  Buffer elements: 156 in free list (500 max allowed) 11839912 hits, 0 misses, 617
  created
  Public buffer pools: Small buffers, 104 bytes (total 45187, permanent 50, peak 45187 @
  10:04:00): 0 in free list (20 min, 150 max allowed) 7968057 hits, 202704 misses, 2128
  trims, 47265 created 71869 failures (680277 no memory)
  ------------------ show buffers usage ------------------
  Statistics for the Small pool Input IDB : Mu1 count: 45180 Caller pc : 0x22CF95C4
  count: 45180 Resource User: IP Input count: 45180 Caller pc : 0x22381654 count: 2
  Resource User: Init count: 2 Output IDB : Mu1 count: 4 Caller pc : 0x2380114C count: 4
  Resource User: PIM regist count: 4 Number of Buffers used by packets generated by
  system: 45187 Number of Buffers used by incoming packets:
  ++++++++++++++++++++++++++++small buffer packet+++++++++++++++++++++++++++++++
  <snip>
  Buffer information for Small buffer at 0x2A815220 data_area 0xD9DEB04, refcount 1,
  next 0x0, flags 0x2080 linktype 7 (IP), enctype 16 (PPP), encsize 2, rxtype 1 if_input
  0x30F21520 (Multilink1), if_output 0x0 (None) inputtime 00:02:46.212 (elapsed
  05:55:11.464) outputtime 00:01:22.632 (elapsed 05:56:35.044), oqnumber 65535
  datagramstart 0xD9DEB56, datagramsize 38, maximum size 260 mac_start 0xD9DEB56,
  addr_start 0x0, info_start 0xD9DEB58 network_start 0xD9DEB58, transport_start
  0xD9DEB6C, caller_pc 0x22CF0044
  source: 10.131.124.33, destination: 224.0.1.40, id: 0x55F0, ttl: 11, TOS: 192 prot:
  17, source port 496, destination port 496
  Enter hex value: 0x22CF95C4 0x22CF95C4:ip_mforward(0x22ce9448)+0x51c Enter hex value:
  0x22CF0044 0x22CF0044:ip_mforward(0x22ce9448)+0x51c
  ```

  Conditions: This symptom is observed with the Cisco 2911 running Cisco IOS Release 15.1(4)M3. When IP Multicast is used with NAT, in certain scenarios when NAT functionality returns error, multicast code does not free duplicate packet buffers eventually leading to exhaustion of packet buffer pool in the router.

  Workaround: There is no real workaround except to disable NAT.

- CSCue74612

  Symptom: FTP download fails in FTS client.

  Conditions: The symptom is observed with FTS transfer over FTP via VRF.

  Workaround: There is no workaround.

- CSCue75986

  Symptom: The active route processor crashes because of a segmentation fault in the PIM IPv6 process after de-configuring a VRF.

  Conditions: This symptom is observed when BGP, multicast-routing, or a VRF is de-configured while VRF-forwarding for the affected VRF is still configured on some interfaces and IPv6 multicast state entries exist within the affected VRF.

  Workaround: Before removing a VRF using **no vrf definition xxx**, de-configuring “router bgp ...” or de-configuring multicast-routing for any VRF or for the global routing table, de-configure the IPv6 and the IPv4 MDT tunnels for affected VRFs as follows:

  1. Under the “vrf definition ...”/ “address-family ipv6” configuration sub-mode, execute **no mdt default ...**.
  2. Under the “vrf definition ...”/ “address-family ipv4” configuration sub-mode, execute **no mdt default ...**.

- CSCue76057

  Symptom: On a SIP 400 with gigeV2 SPA, when EVC is configured with “encap default”, it is seen that sometimes the FUGU TCAM is not programmed with correct VVID for the EVC. This results in incoming traffic reaching the linecard with wrong VVID. This can impact traffic incoming on the EVC.

  Conditions: The symptom is observed with an “encap default” configuration under EVC, or removal and re-application of “encap default” under EVC.

  Workaround: There is no workaround.

- CSCue76102

  Symptoms: Redistributed internal IPv6 routes from v6 IGP into BGP are not learned by the BGP neighboring routers.

  Conditions: This symptom occurs because of a software issue, due to which the internal IPv6 redistributed routes from IGPs into BGP are not advertised correctly to the neighboring routers, resulting in the neighbors dropping these IPv6 BGP updates in inbound update processing. The result is that the peering routers do not have any such IPv6 routes in BGP tables from their neighbors.

  Workaround: There is no workaround.

- CSCue81327

  Symptoms: Standby RP crashes during bulk sync with:

  ```
  Unexpected exception to CPU: vector 1400
  ```

  Conditions: The crash occurs while syncing a shutdown TE tunnel interface configuration.

  Workaround: Delete the shutdown TE tunnel configuration, if not required.

- CSCue89779

  Symptom: A FlexVPN spoke configured with an inside VRF and front-door VRF may have problems with spoke-to-spoke tunnels if they are not the same. During tunnel negotiation, two Virtual-access interfaces are created (while only one is needed), the one in excess may fail to cleanup correctly. As a result, the routes created by NHRP process may lead to loss of traffic, or traffic may continue to flow through the Hub.

  Conditions: This symptom occurs when the VRF used on the overlay (IVRF) and the VRF used on the transport (FVRF) are not the same.

  Workaround: There is no workaround.

- CSCue94653

  Symptom: When the port-security configured interface goes to blocking state (MST), the VLANs configured on the port go to not-forwarding state temporarily. The secure mac-addresses are not added back resulting in loss of traffic.

  Conditions: The symptom is observed when the port-security configured interface goes to blocking state.

  Workaround: Shut and no shut the port-security interface to re-add the mac-addresses.

- CSCuf03079

  Symptom: A Cisco IOS router running with ISIS remote-LFA configured can crash.

  Conditions: This symptom occurs when shut/no shut is performed on an interface multiple times.

  Workaround: Disable the ISIS remote-LFA configuration.

- CSCuf09006

  Symptoms: Upon doing a **clear ip bgp * soft out** or **graceful shutdown** on a PE, all VPNv4/v6 routes on an RR from this PE are purged at the expiry of enhanced refresh stale-path timer.

  Conditions: The symptom is observed with the following conditions:

  1. 1. PE must have BGP peering with at least one CE (VRF neighbor) and at least one RR (VPN neighbor).
  2. PE must have a rtfilter unicast BGP peering with the RR.
  3. IOS version must have “Enhanced Refresh” feature enabled.
  4. A **clear ip bgp * soft out** or **graceful shutdown** is executed on the PE.

  Workaround: Instead of doing **clear ip bgp * soft out**, do a route refresh individually towards all neighbors.

- CSCuf09198

  Symptom: After deleting a VRF, you are unable to reconfigure the VRF.

  Conditions: The symptom is observed when BGP SAFI 129 address-family is not configured, but unicast routes are installed into multicast RIB to serve as upstream multicast hop, as described in RFC 6513. This applies to VRFs configured before BGP is configured.

  Workaround: Beyond unconfiguring BGP, there is no workaround once the issue occurs. Configuring a dummy VRF multicast address-family under BGP before the issue occurs can prevent the problem from occurring.

- CSCuf30798

  Symptom: SIP 600 crashes.

  Conditions: The symptom is observed with VPLS VC going over GRE tunnel and chassis having both ES+ and SIP 600 card.

  Workaround: Remove VPLS over GRE. This configuration is not supported.

- CSCuf56776

  Symptom: After a linecard is removed and reinserted (OIR), traffic may fail to pass through some virtual circuits which have been configured for pseudowire redundancy.

  Conditions: This symptom is observed when the first segment ID in the redundancy group is numerically greater than the second segment.

  ```
  PE1#show ssm id | inc 1st 1stMem: 16394 2ndMem: 12301 ActMem: 12301 1stMem: 16394
  2ndMem: 12301 ActMem: 12301
  ```

  After the OIR is performed, it can be seen that the segments are reversed on the linecard.

  ```
  ESM-20G-12#sh ssm id | inc 1st 1stMem: 12301 2ndMem: 16394 ActMem: 12301 1stMem: 12301
  2ndMem: 16394 ActMem: 12301
  ```

  Workaround: There is no workaround.

- CSCuf60830

  Symptom: Standby-RP occasionally crashes on process SSS Manager after an RP failover when the new Standby-RP attempts to sync.

  Conditions: This symptom occurs during an RP Failover, at high scale, with a high churn of sessions and ISG services.

  Workaround: There is no workaround.

- CSCuf61640

  Symptom: Tracebacks as follows seen during router bootup:

  ```
  %SYS-2-INTSCHED: 'suspend' at level 2 -Process= "Init", ipl= 2, pid= 3
  -Traceback= 4F6966C 6A708EC 890127C 6B4F924 6B4F7F8 6B4EAAC 6B4F43C 6B4F514 6DD6D4C
  6DDB3A8 6A23E50 6A23F18 6A24100 57D3F94 57D42D8 4F701E4
  0x4F6966C ---> process_ok_to_reschedule+288 0x6A708EC ---> process_suspend+4C
  0x890127C ---> random_fill+248 0x6B4F924 ---> default_entropy_routine+9C 0x6B4F7F8
  ---> hardware_entropy_source+CC 0x6B4EAAC ---> nist_instantiate+78 0x6B4F43C --->
  try_create_rng+1B4 0x6B4F514 ---> nist_rng+34 0x6DD6D4C --->
  cts_sap_get_key_counter+54 0x6DDB3A8 ---> cts_sap_init+C4 0x6A23E50 --->
  subsys_init_routine+60 0x6A23F18 ---> subsys_init_class_internal+A8 0x6A24100 --->
  subsys_init_class+8C 0x57D3F94 ---> system_init+250 0x57D42D8 ---> init_process+94
  0x4F701E4 ---> ppc_process_dispatch+
  ```

  Conditions: The symptom is observed during router bootup.

  Workaround: There is no workaround.

- CSCuf62756

  Symptom: If **bandwidth qos-reference** *value* is configured on an interface which bandwidth can change, then the actual interface bandwidth will be used for QoS service-policy validation when the interface bandwidth changes. This can result in a service-policy being removed if the interface bandwidth is insufficient to meet the requirements of the service-policy, such as bandwidth guarantees.

  Conditions: This symptom occurs in variable-bandwidth interfaces such as EFM interfaces or PPP multilink bundles.

  Workaround:

  1. Use proportional actions in the QoS service-policy, such as “police rate percent....”, “bandwidth remaining ratio...”, “bandwidth remaining percent...”, and “priority percent”
  2. You can configure **bandwidth qos-reference** with maximum bandwidth of the interface:

  interface Ethernet0 bandwidth qos-reference <*max bandwidth of interface*>

  This can prevent policy-map detached due to interface bandwidth change.

- CSCuf64313

  Symptoms: Linecard crash is seen with machine-check exception.

  Conditions: There is no trigger. The crash is random.

  Workaround: There is no workaround.

- CSCuf65371

  Symptom: On LAC, with “l2tp hidden” configured under VPDN template, L2TP sessions are failing to establish on existing L2TP tunnels after RP failover.

  Conditions: The symptom is observed with “l2tp hidden” configured under VPDN template.

  Workaround: Tear down L2TP tunnels after RP failover, or unconfigure “l2tp hidden”. Disabling L2TP redundancy with “no l2tp sso enable” will fix issue as well.

- CSCuf68995

  Symptom: Ping failures. Traffic gets dropped.

  Conditions: The symptom is observed when you configure MPLSoMGRE tunnel on PE1 and PE2. Initiate ping from CE1 to CE2. Packets reach the CE2 and replay is coming back but these packets are getting dropped on PE2. After PE2 switchover, ping fails from CE1 to CE2. PE2 is configured with MPLSoMGRE on an HA system. Topology:

```
CE1---- PE1 ----PE2----CE2
```

Workaround: There is no workaround.

- CSCuf81275

  Symptom: Some ISG sessions do not pass traffic.

  Conditions: This symptom is observed when you have more than one Line Card for the ISG sessions.

  Workaround: There is no workaround.

- CSCuf82179

  Symptom: BGP routes remain installed in multicast RIB even after “address-family” configuration has been removed from “vrf definition”.

  Conditions: This symptom is observed in MVPN topology, where the stale routes are installed as an upstream multicast hop, as described in RFC: http://tools.ietf.org/html/rfc6513

  Workaround: There is no workaround.

- CSCuf93376

  Symptom: CUBE reloads while testing SDP passthrough with v6.

  Conditions: The symptom is observed while testing SDP passthrough with v6.

  Workaround: There is no workaround.

- CSCuf93606

  Symptoms: A Cisco 3945E router crashes.

  Conditions: The symptom is observed with the following conditions:

  – Extension mobility is configured for the phone. The logout profile should not be configured with any number.

  – In the logged out state, user has to press the “NewCall” softkey followed by dialing any digit between 1-9 (excluding 0).

  – Instead of pressing “dial” softkey, press “AbbrDial” softkey.

  Workaround: Have a proper number configured under the logout profile.

- CSCug04187

  Symptom: Build breakage.

  Conditions: This symptom occurs due to CSCuf62756.

  Workaround: There is no workaround.

- CSCug08561

  Symptom: After a web-logon, users do not get the web-logon response page sent by the portal. If the web-logon is successful, users are not redirected to the web address which they have entered initially but are redirected to the portal for authentication.

  Conditions: This symptom occurs under the following conditions:

  1. Walkby feature is enabled with L4R & PBHK features applied to the lite session.
  2. User initiated the web-logon request.

  Workaround: There is no workaround.

  More Info: When a user does a web-logon, an account-logon coa request is triggered from the portal to ISG. In ISG, the account-logon request triggers a lite session conversion to a dedicated session. During the conversion, lite session and its associated resources (L4R and PBHK mappings) are removed from PD and a dedicated session gets provisioned. Once the conversion is done, ISG replies back with COA ACK/NACK to the portal. Based on the response from ISG, the portal generates a weblogon response (SUCCESS/FAILURE) page and sends it back to the client. But when it reaches ISG, the response packet does not get classified to session in the downstream direction and gets dropped in ISG because PBHK & L4R maping are deleted.

- CSCug10922

  Symptom: A traceback is seen in the standby RP after a headend SSO.

  Conditions: This symptom occurs when SSO tracebacks are seen.

  Workaround: There is no workaround.

- CSCug15952

  Symptom: %QOS-3-INDEX_EXISTS error message is shown and router crashes.

  Conditions: The symptom is observed when sessions are bought up and the collision IDs with dynamic policy names are synced to standby from active. When the sessions time out and restart, the same dynamic policy names are synced to HA tree on standby again without cleaning up the tree earlier and the crash will happen.

  Workaround: Avoid the same session reestablishment before rebooting the router.

- CSCug17724

  Symptom: When using session protection and graceful restart for LDP, LDP neighbor goes down immediately after filtering LDP hello between routers. The LDP neighbor should go down after 10 minutes (default value of forwarding state holding time for GR).

  Conditions: The symptom is observed when you enable session protection and graceful restart for LDP

  Workaround: There is no workaround.

- CSCug17808

  Symptom: Redistributed default route not advertised to EIGRP peer.

  Conditions: This symptom is observed when Cisco ASR router is rebooted or the route is cleared via the **clear ip route** command, the route disappears form the spokes.

  Workaround: Clearing the EIGRP Neighborship restores the route on the spokes.

- CSCug18797

  Symptom: Router crashes when it checks whether the interface is configured as DHCP SIP session initiator.

  Conditions: The symptom is observed DHCP and ISG are configured.

  Workaround: There is no workaround.

- CSCug20048

  Symptom: MPLS traffic engineering BC MAM model does not take effect when configured.

  Conditions: The symptom is observed when you configure the BC MAM model.

  Workaround: There is no workaround.

- CSCug20705

  Symptom: A 7600-SIP-400 LC crash is seen with an SPA reload.

  Conditions: This symptom occurs after an SPA reload with FRF12 and service policy on the interface.

Workaround: There is no workaround.

- CSCug23348

  Symptom: The "mod" value in the SSRAM may be inconsistent to the number of ECMP paths.

  Conditions: This occurs with ECMP TE tunnels with **tunnel mpls traffic-eng load-share** *value* commands configured.

  Workaround: Remove the **tunnel mpls traffic-eng load-share** *value* commands from the TE tunnels.

- CSCug24114

  Symptom: CTS environment-data download fails from ISE.

  Conditions: The symptom is observed if there is less PAC and environment-data refresh timer is configured in ISE. After multiple refreshes of PAC and environment data and the switch is reloaded, sometimes a CTS environment-data download fails from ISE on the switch.

  Workaround: Unconfigure **pac key CLI** and configure it again as below:

  ```
  no pac key pac key <key-id>
  ```

- CSCug25258

  Symptom: Router crashes while running the **show interface rate-limit** command. When entries down the list of the output disappear for reasons such as interfaces going down or PPPoE clients disconnecting, the router may crash when you hit the space bar to get to these invalid entries.

  Conditions: This symptom occurs when rate limiting is configured.

  Workaround: Configure **term length 0** before running the show output.

- CSCug28904

  Symptoms: Router drops ESP packets with CRYPTO-4-RECVD_PKT_MAC_ERR.

  Conditions: The symptom is observed when the peer router sends nonce with length 256 bytes.

  Workaround: There is no workaround.

- CSCug31561

  A vulnerability in the DHCP implementation of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

  The vulnerability occurs during the parsing of crafted DHCP packets. An attacker could exploit this vulnerability by sending crafted DHCP packets to an affected device that has the DHCP server or DHCP relay feature enabled. An exploit could allow the attacker to cause a reload of an affected device.

  Cisco has released free software updates that address this vulnerability. There are no workarounds to this vulnerability.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130925-dhcp

  Note: The September 25, 2013, Cisco IOS Software Security Advisory bundled publication includes eight Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the September 2013 bundled publication.

  Individual publication links are in "'Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep13.html

- CSCug33084

  Symptom: SP/DFC crash is seen when churn on multicast is done, either through provisioning/unprovisioning or other network event.

  Conditions: The issue occurs when a pointer to an already freed hal_context is still present in a replicate queue. Later during churn the same pointer is accessed which leads to the crash.

  Workaround: There is no workaround.

- CSCug34404

  Symptom: RP crash seen at be_interface_action_remove_old_sadb.

  Conditions: The symptom is observed while unconfiguring the 4K SVTI sessions after an HA test.

  Workaround: There is no workaround.

- CSCug34503

  Symptom: LLDP packets with destination MAC: 01:80:C2:00:00:0E are dropped.

  Conditions: This symptom occurs with the fix of CSCue41216.

  Workaround: There is no workaround.

  More Info: Regression because of CSCue41216 causes LLDP packets which have a MAC address of 01.80.c2.00.00.0e to get dropped according to MEF standard. But the packets should get dropped for SUNI and NNI port, while for CUNI they should get passed.

- CSCug34507

  Symptom: Traffic decrypted on a Cisco ISR G2 series is process switched instead of staying in the CEF path.

  Conditions: The symptom is observed when the hub and/or the spoke are located behind NAT or PAT.

  Workaround: Disable NAT/PAT.

- CSCug34877

  Symptom: A switch crashes with following message:

  ```
  %SYS-2-LINKED: Bad enqueue of 901E0D40 in queue 1AABE690 -Process= "SSH Process", ipl=
  0, pid= 392
  ```

  Conditions: This symptom occurs while making an SSH connection to a remote device from the switch while having multiple SSH connections to the same switch

  Workaround: There is no workaround.

- CSCug37242

  Symptoms: Router crash due to memory leak.

  Conditions: The symptom is observed with a CME shared line feature configuration.

  Workaround: Disabling shared line feature will avoid memory leak.

- CSCug38011

  Symptom: Device crashes with CPU hog messages.

  Conditions: The symptom is observed when the device is reloaded after configuring NTP peer:

  ntp server pool.ntp.org source cell0

  Workaround: There is no workaround.

- CSCug39278

  Symptom: L3 QoS policy not working in EVC L3 VPN.

  Conditions: The symptom is observed when CFM is enabled globally.

  Workaround: Disable CFM.

- CSCug44667

  Symptom: SG3 fax call failures observed for STCAPP audio calls.

  Conditions: Fax CM tone detection is turned ON even when all fax and modem related configurations have been disabled on the STCAPP gateway.

  Workaround: STCAPP modem pass-through feature can be enabled, but you may run into issues with some answering SG3 fax machines which have stringent requirements for fax CM signal.

- CSCug50208

  Symptom: A crash is seen due to double free of memory.

  Conditions: The symptom is seen when the accept interface VLAN goes down.

  Workaround: There is no workaround.

- CSCug50340

  Symptom: PW traffic is not flowing after SSO/card reset the active PTF card.

  Conditions: The symptom is observed with the following conditions:

  1. Create a unprotected tunnel between the active PTF card and create a PW.
  2. Apply the table map. Bi-directional traffic is flowing fine.
  3. SSO/reset the active PTF card in node 106 (4/1).
  4. Now tunnel core port is in standby card.
  5. Observed bi-directional traffic is not flowing once the card becomes up.
  6. Again reset the active PTF card (5/4).
  7. Observe uni-directional traffic only is flowing.

  Workaround: Delete the PW and recreate it again. However, note that if you do an SSO/card reset, the issue reappears.

- CSCug52119

  Symptom: A RIB route is present for a prefix, but the router continues to LISP encapsulate.

  Conditions: The symptom is observed when a LISP map-cache existed for a prefix and then the RIB route was added later.

  Workaround: Use the following command:

  ```
  clear ip/ipv6 lisp map-cache <prefix>
  ```

- CSCug58617

  Symptom: Usernames do not show up in CCP Express. Username shows up on a router with default configuration.

  Conditions: The symptom is observed on routers with configurations that break show runn | format.

  Workaround: Use default configuration.

- CSCug58977

  Symptom: 2.6Gbp/s traffic is observed on both of the VPN SPA interfaces. Traffic direction: Rx on outside interface, Tx on inside interface.

  Conditions: This symptom occurs when fragmented IPSec packet arrives on clear side. The issue is observed only in VRF mode.

  Workaround: Reload the IPSec card.

- CSCug59746

  Symptom: A crash is seen on the RP in the SS manager process:

  ```
  Exception to IOS Thread: Frame pointer 0x7F58BB22FE80, PC = 0x7C505FB
  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = SSS Manager -Traceback=
  1#980611ad3b9665cd80fe5178bcd6036a :400000+78505FB :400000+7C68774 :400000+7C6871A
  :400000+1C13522 :400000+7852194 :400000+78512C8 :400000+7C68774 :400000+7C6871A
  :400000+33A8AC1 :400000+77DD92F :400000+33C3E4C :400000+33AFE89 :400000+33B2564
  :400000+7824301 :400000+7823F37 :400000+77FA27F
  ```

  Conditions: The issue appears to be related to NAS port. It looks like a key is being set when the issue occurred. The exact conditions are still being investigated.

  Workaround: Possibly remove radius or more specifically, NAS port configurations. This still needs to be verified.

- CSCug61485

  Symptom: The Cisco ASR 1000 RP crashes in RSVP.

  Conditions: This symptom occurs when "mpls traffic-eng tunnels" is configured on an interface and "ip rsvp bandwidth" is not configured and the bandwidth on the physical interface is changed.

  Workaround: There is no workaround.

- CSCug62154

  Symptom: CPU shoots to 100% with TACACS configuration. VTY to the device does not work due to this.

  Conditions: This symptom is observed when the router or switch is booted up with TACACS configurations and the CPU shoots up to 100%. Telnet to the router is not possible. Any command issued on the console would take lot of time.

  Workaround: Remove the TACACS configurations and then reboot the router.

- CSCug63013

  Symptom: A DMVPN spoke router running Cisco IOS Release 15.2(4)M3 and configured with "if-state nhrp" might not re-form eigrp neighbourship if the line protocol on the interface goes down and comes back automatically.

  Conditions: This symptom occurs in a DMVPN spoke router running 15.2(4)M3 with "if-state nhrp" configured and interface line protocol going down. It must also be using the new multicast code (15.1(4)M onwards).

  Workaround:

  - Removing "ip nhrp map multicast x.x.x.x y.y.y.y" and readding it resolves the problem.
  - Shut/no shut on the tunnel interface

- CSCug63839

  Symptom: The Cisco 7301 router running c7301-advipservicesk9-mz.152-4.M3 experiences a memory leak in the Crypto IKMP process particularly on the crypto_ikmp_config_send_ack_addr function.

Conditions: This symptom occurs when running the Cisco 7301 router and connecting EasyVPN through it.

Workaround: Reload the router over a period of time.

- CSCug68193

  Symptom: Multicast traffic across ES+ cards stop flowing across subinterfaces.

  Conditions: The symptom is observed after a linecard OIR. After the linecard comes up, multicast traffic stops flowing across subinterfaces.

  Workaround: Shut/no shut the subinterface.

- CSCug69253

  Symptom: Users will see the following error message on unconfiguring a port-map of a protocol:

  ```
  % NBAR Error: Specified port(s) are associated with <protocol-name>
  ```

  Conditions: This symptom occurs when users have port-mapped a protocol on which other protocols are dependant, and this port-map configuration includes the well-known port as well. On unconfiguring this port-map configuration, the error message will be shown.

  For example, a lot of protocols are dependant on http (share-point, youtube, skype, etc.) because they run over http. If the user port-maps http and includes its well-known port (80) in the configuration, then the following error message will be shown during unconfiguration:

  ```
  Router(config)#no ip nbar port-map http tcp 80 94 8080 3128 8092
  % NBAR Error: Specified port(s) are associated with share-point
  ```

  Workaround: Users will not be able to remove this port-map configuration. To revert back, reconfigure http to its original configuration (tcp 80), save the configuration, and reload the router

  The following is the CLI to reconfigure http to its well-known configuration:

  ```
  Router(config)#ip nbar port-map http tcp 80
  ```

- CSCug72891

  Symptom: EIGRP neighbor flaps due to EIGRP SIA. Troubleshooting shows that a race condition causes EIGRP successor loop first and it leads to EIGRP QUERY loop resulting in the neighbor flaps.

  Conditions: The issue is observed when a worse metric update is received from the successor, once the route is already in active state, in a partially peered multiaccess network.

  Workaround: There is no workaround.

- CSCug78098

  Symptom: Supervisor engine crashes and the Cisco IOS software is forced to reload due to PIM process.

  Conditions: This symptom is observed when using the command, **show ip pim rp-hash** right after the BSR RP times out, causes the crash.

  Workaround: Perform these steps in the following order:

  1. Wait for a minute after BSR RP times out before using this command.
  2. Configuring **no ip domain lookup** will make the time taken to execute **show ip pim rp-hash** to a few milliseconds. This will prevent the crash from being reproduced manually.

- CSCug78929

  Symptom: Packets of a certain protocol are dropped due to v6 PACL applied on a switch port.

Conditions: This symptom occurs when v6 PACL contains explicit protocol entries such as “permit 89 any any”.

Workaround: There is no workaround.

- CSCug85947

  Symptom: OSPFv3 routes go missing after an NSR switchover.

  Conditions: This symptom occurs after an SSO.

  Workaround: Clear the IPv6 OSPF process.

- CSCug94275

  Symptom: ES+ card crashes with an unexpected exception to CPU: vector 200, PC = 0x0.

  Conditions: The symptom is observed on the ES+ series linecards on a Cisco 7600 series router. Symptom is reported on the ES+ console and in the crashinfo file on the ES+ flash disk. It is not reported in the syslog.

  Workaround: There is no workaround.

- CSCuh07349

  Symptom: A Cisco 7600 Sup may crash due to SP memory corruption.

  Conditions: This issue is observed on an REP enabled router, which is part of an REP segment. The exact trigger for this issue is not clear.

  Workaround: There is no workaround.

- CSCuh07657

  Symptom: VRF Aggregate label is not re-originated after a directly connected CE facing interface (in VRF) is shut down.

  Conditions: This symptom occurs in an MPLS VPN set-up with Cisco 7600(PE) Router running on Cisco IOS Release 12.2(33)SRE4 with per VRF aggregation.

  For example:

  ```
  mpls label mode vrf TEST protocol all-afs per-vrf
  ```

  Workaround: Downgrade to Cisco IOS Release 12.2(33)SRE3 or earlier.

- CSCuh16115

  Symptom: With VPLS configuration with IP-FRR, on doing multiple churns SP/LC may crash.

  Conditions: The issue occurs when xconnect internal data structre is to be freed up and IP FRR is still pointing to it.

  Workaround: Remove IP-FRR configuration before unprovisioning xconnect.

- CSCuh16927

  Symptom: Mac entries learned on a trunk link are flushed after removing VLANs.

  Conditions: The symptom is observed when some allowed VLANs are removed on a trunk link, all mac address entries learned on this link are flushed. This is issue is specific to extended VLAN IDs.

  Workaround: Executing ping to destination IP after removing VLANs will recover this condition.

- CSCuh21740

  Symptom: There is a deletion and addition of VRFs with MVPNV6 configurations.

  Conditions: This symptom occurs when PIM VRF neighbors are not up.

  Workaround: Reload the router.

- CSCuh24040

  Symptom: BGP routes are not marked Stale and considered best routes even though the BGP session with the peer is torn down. A hard or soft reset of the BGP peering session does not help.

  For BFD-related triggering, the following messages are normally produced with the BGP-5-ADJCHANGE message first, and the BGP_SESSION-5-ADJCHANGE message second. Under normal conditions, the two messages will have identical timestamps. When this problem is seen, the order of the messages will be reversed, with the BGP_SESSION-5-ADJCHANGE message appearing first, and with a slightly different timestamp from the BGP-5-ADJCHANGE message. In the problem case, the BGP_SESSION-5-ADJCHANGE message will also include the string “NSF peer closed the session”

  For example when encountering this bug, you would see:

  ```
  May 29 18:16:24.414: %BGP_SESSION-5-ADJCHANGE: neighbor x.x.x.x IPv4 Unicast vpn vrf
  VRFNAME topology base removed from session NSF peer closed the session May 29
  18:16:24.526: %BGP-5-ADJCHANGE: neighbor x.x.x.x vpn vrf VRFNAME Down BFD adjacency
  down
  ```

  Instead of:

  ```
  May 29 18:16:24.354: %BGP-5-ADJCHANGE: neighbor x.x.x.x vpn vrf VRFNAME Down BFD
  adjacency down May 29 18:16:24.354: %BGP_SESSION-5-ADJCHANGE: neighbor x.x.x.x IPv4
  Unicast vpn vrf VRFNAME topology base removed from session BFD adjacency down
  ```

  Log messages associated for non-BFD triggers are not documented.

  Conditions: This symptom is observed when BGP graceful restart is used in conjunction with BFD, but it is possible (but very low probability) for it to happen when BGP graceful restart processing happens when any other type of BGP reset (eg: clear command) is in progress.

  Affected configurations all include: router bgp ASN ... bgp graceful-restart ...

  The trigger is that BGP exceeds its CPU quantum during the processing of a reset, and gives up the CPU, and then BGP Graceful Restart processing runs before BGP can complete its reset processing. This is a very low probability event, and triggering it is going to be highly dependent on the configuration of the router, and on BGP’s CPU requirements.

  It is not possible to trigger this bug unless BGP graceful-restart is configured.

  Workaround: If you are engaged in active monitoring of router logs, and the bug is being triggered by a BFD-induced reset, you can detect this situation by watching for the reversal of log message order described in the Symptoms section, and then take manual steps to remedy this problem when it occurs.

  On the problematic router, issue **no neighbor <xxx> activate** command under the proper address-family will clear the stale routes.

  The other option is to manually shutdown the outgoing interface which marks the routes as “inaccessible” and hence not been used anymore. This prevents the traffic blackhole but the routes will stay in the BGP table.

  More Info: This bug affects all releases where CSCsk79641 or CSCtn58128 is integrated. Releases where neither of those fixes is integrated are not affected.

- CSCuh27770

  Symptom: On a dual-RP system which is configured for stateful switchover (SSO), some VPLS virtual circuits may fail to be provisioned on the standby route processor.

  Conditions: This symptom is observed when the VFI consists of VLAN interfaces that are also configured for IP.

  Workaround: Reload the standby RP.

- CSCuh29716

  Symptom: When a call is transferred from IVR to PSTN, the codec negotiation with Verizon fails only if the original invite received includes fax capabilities, dropping the call with reason code 47 and hanging the UDP port used.

  Call flow:

  ```
  Verizon -- CUBE -- CUSP -- Genesys/IVR, transferred with SIP Refer back to PSTN
  hair-pinning the call on CUBE.
  ```

  All subsequent calls that try to re-use the same UDP port for RTP stream are dropped with reason code 47 and provisn RSP fail is logged on show voip fpi stats.

  Conditions: This symptom occurs in hair-pinned calls that receive FAX capabilities on the original SIP invite from Verizon.

  Workaround: There is no workaround. Reload the router to clear UDP ports.

- CSCuh32177

  Symptom: The **no passive-interface** <*if-name*> command will be added automatically after configuring the **ipv6 enable** command on the interface even though the **passive-interface default** command is configured for OSPFv3.

  ```
  --- (config)#interface FastEthernet0/2/0 (config-if)#ipv6 enable (config-if)#end
  #sh run | sec ipv6 router ospf ipv6 router ospf 100 router-id 10.1.1.1
  passive-interface default no passive-interface FastEthernet0/2/0 <<< Added
  automatically. ---
  ```

  Conditions: This symptom occurs when the **passive-interface default** command is configured for OSPFv3.

  Workaround: Adjust the configuration manually. In this example it would be “passive-interface FastEthernet0/2/0”.

- CSCuh40275

  Symptom: SNMP occupies more than 90% of the CPU.

  Conditions: This symptom is observed when polling the cefFESelectionTable MIB.

  Workaround:Execute the following commands:

  ```
  snmp-server view cutdown iso included
  snmp-server view cutdown cefFESelectionEntry excluded
  snmp-server community public view cutdown ro
  snmp-server community private view cutdown rw
  ```

- CSCuh40329

  Symptom: OSPFV3 runs as PE-CE, but used to learn IPv4 prefixes. Core facing interface is GRE tunnel where OSPF and LDP runs. OSPV3 based Shamlinks are created between PEs. When tunnel flaps , OSPF and LDP recovers, but in a few seconds tunnel locks up. In locked up condition, all traffic fails on the tunnel, even directly connected pings. The only way to recover is to reconfigure the tunnel from scratch. It happens fairly consistently after every re-convergence, not every time though.

  Conditions: This symptom is seen only on ISRG2s that are configured as PEs. They are so far seen with 3925 running Cisco IOS Release 15.3(2)T and 2911 running Cisco IOS Release 15.2(4)M3.

  Workaround: Use OSPF V2 based shamlinks.

- CSCuh40617

  Symptom: Ping fails when “encap dot1q” is configured on an FE SPA inserted in bay 1 of flexwan.

Conditions: This symptom is observed when FE SPA is inserted in bay 1 of flexwan.

Workaround: Move the SPA to bay 0 of flexwan.

- CSCuh43027

  Symptom: Prefixes withdrawn from BGP are not removed from the RIB, although they are removed from the BGP table.

  Conditions: A withdraw message contains more than one NLRI, one of which is for a route that is not chosen as best. If deterministic med is enabled, then the other NLRI in the withdraw message might not eventually be removed from the RIB.

  Workaround: Forcibly clear the RIB.

- CSCuh43252

  Symptom: After upgrading to Cisco IOS Release 15.0(2)SE3, you can no longer authenticate using TACACS. The TPLUS process on the switch will be pushing the CPU up to 99%.

  Conditions: The symptom is observed when you use TACACS for authentication.

  Workaround: Downgrade the switch to a version prior to Cisco IOS Release 15.0(2)SE3.

- CSCuh43255

  Symptom: The BGP task update-generation process may cause the router to reload, in a rare timing condition when there is prefix flap and there is high scale of prefixes going through update-generation, including the flapping prefix.

  Conditions: The symptom is observed when the Cisco ASR router is acting as a route server for BGP along with having various route-server contexts. The router does not do any forwarding. It merely processes control plane traffic.

  Workaround: There is no workaround.

  More Info: The setup is the same as mentioned in this doc: http://www.cisco.com/en/US/docs/ios/ios_xe/iproute_bgp/configuration/guide/irg_route_server_xe.html.

- CSCuh46031

  Symptom: The Cisco ASR 1000 router sends a different Acct-Session-Id in the Access-Request and Accounting-Request for the same user.

  Conditions: This symptom occurs when Flex VPN IPsec remote access is configured.

  Workaround: There is no workaround.

- CSCuh46849

  Symptom: A Cisco ASR 1000 router may display the following log with a traceback:

  ```
  SCHED-3-UNEXPECTEDEVENT Process received unknown event (maj 80, min 0).
  ```

  Conditions: The conditions are unknown.

  Workaround: Reload the router.

- CSCuh48840

  Symptom: Cisco Router crashes.

  Conditions: This symptom is observed under the following conditions:

  - sup-bootdisk formatted and copied with big size file, like copy 7600 image file around 180M size

- reload box, and during bootup try to write file to sup-bootdisk (SEA write sea_log.dat 32M bytes)
- then the issue appear
- When the issue seen, check the sea_log.dat always with 0 byte
- No matter where (disk0 or bootdisk) to load image.
- No matter sea log disk to sup-bootdisk or disk0:. I reproduced the issue with “logg sys disk disk0:” config.

```
SEA is calling IFS API to create sea_log.dat, looks like IFS creating file hungs SP.
sea_log.c : sea_log_init_file() -> ifs_open() -> sea_zero_log() -> ifs_lseek() ->
ifs_write()
```

Workaround: There is no workaround.

- CSCuh53544

  Symptom: OSPF ABR router does not flush type-4 ASBR summary LSA after NSR swithover if the connection to ASBR is lost during NSR switchover.

  Conditions: This symptom is occurs when the VSS system acts as ABR and loses connection to an ASBR during NSR switchover. This configuration is not recommended and Layer 3 topology should not change during the switchover.

  Workaround: Clear ip ospf proc.

- CSCuh56327

  Symptom: IP SLA responder crash occurs on Cisco ASR 1002 router in Cisco IOS Release 15.2(4)S, Cisco IOS Release 15.2(4)S1, and Cisco IOS Release 15.2(4)S2.

  Conditions:This symptom occurs when ip sla udp jitter with precision microseconds, udp jitter with milliseconds and udp echo are configured on the sender device with the same destination port on Cisco ASR 1002 router.

  Workaround:Use different destination ports for udp-echo and udp jitter with millisecond precision than udp jitter with microsecond and optimize timestamp.

- CSCuh62266

  Symptom: During normal operation, the Cisco ASR 1000 router may crash after repeated SNMP related watchdog errors.

```
Jun 15 2013 10:43:30.325: %SCHED-0-WATCHDOG: Scheduler running for a long time, more
than the maximum configured (120) secs. -Traceback= 1#6d024ee43b83b4f5539a076aa2e8d467
:10000000+56A5348 :10000000+20F7D54 :10000000+2513910 :10000000+20F807C
:10000000+20EBE84 :10000000+2119BA8 :10000000+20EBE84 :10000000+2106C24
:10000000+20EBE84 :10000000+213C9E8 :10000000+213CC34 :10000000+225B748
:10000000+222941C :10000000+2214314 :10000000+224812C -Traceback=
1#6d024ee43b83b4f5539a076aa2e8d467 :10000000+21416F0 :10000000+2513910
:10000000+20F807C :10000000+20EBE84 :10000000+2119BA8 :10000000+20EBE84
:10000000+2106C24 :10000000+20EBE84 :10000000+213C9E8 :10000000+213CC34
:10000000+225B748 :10000000+222941C :10000000+2214314 :10000000+224812C
```

  Conditions: This symptom occurs while trying to obtain data from IP SLAs Path-Echo (rttMonStatsCollectTable) by SNMP polling operation.

  Workaround: There is no workaround other than to disable SNMP configuration from the router.

  More Info: This crash occurred in a customer environment and device with a particular version of the software (Cisco IOS Release 15.1(2)S2). No other similar issue has been identified so far.

- CSCuh78146

  Symptom: ES+ LC crashes while sending L2 traffic from Ixia.

  Conditions: This symptom occurs while sending continuous traffic from Ixia. The ES+ interface has the configurations of EVC and BD.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.2(4)S3a

Cisco IOS Release 15.2(4)S3a is a rebuild release for Cisco IOS Release 15.2(4)S. The caveats in this section are resolved in Cisco IOS Release 15.2(4)S3a and Cisco IOS Release 15.2(4)S3 but may be open in previous Cisco IOS releases.

- CSCuf64313

  Symptoms: Linecard crash is seen with machine-check exception.

  Conditions: There is no trigger. The crash is random.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.2(4)S3

Cisco IOS Release 15.2(4)S3 is a rebuild release for Cisco IOS Release 15.2(4)S. The caveats in this section are resolved in Cisco IOS Release 15.2(4)S3 but may be open in previous Cisco IOS releases.

- CSCsr06399

  Symptoms: A Cisco 5400XM may reload unexpectedly.

  Conditions: This symptom is intermittent and is seen only when the DSPs available are insufficient to support the number of calls.

  Workaround: Ensure that sufficient DSPs are available for transcoding.

- CSCtx50235

  Symptoms: During a crash on the Cisco Catalyst 6500, the normal crash information from the crashinfo files may be missing due to the crashes showing the Routing processor (RP) being reset by the Switching Processor (SP) and the RP crashinfo also showing the RP being reset by the SP. This bug addresses this serviceability issue and it has nothing to do with the root cause of the crash itself.

  In a majority of cases, the crash has been a single-event crash and has not repeated.

  Conditions: Conditions of this symptom are not known currently. At this point, it is believed that the real fault of the crash belongs to the SP.

  Workaround: There is no workaround.

- CSCty07538

  Symptoms: TCP sessions get reset intermittently when NAT is configured with more than 1500 translations.

  Conditions: This symptom occurs in the Cisco Catalyst 6500-Sup720/Sup32 when NAT is configured with more than 1500 translations.

  Workaround 1: Remove NAT.

Workaround 2: Force packets coming to RP on the NAT interfaces to be process switched by configuring **no ip route-cache** on the NAT interfaces.

- CSCtz26779

  Symptoms: A 7600 ES line card and/or SUP/RSP may crash displaying DATACORRUPTION-1-DATAINCONSISTENCY messages.

  Conditions: This symptom is observed when a policy-map is configured where the name exceeds 80 characters. This will trigger DATACORRUPTION messages on ES line cards and might cause the SUP/RSP to crash as well.

  Workaround: Configure policy-map names that are less then or equal to 80 characters.

- CSCtz53214

  Symptoms: The “clear counter pseudowire <#>” commands do not clear the pseudowire specific counters.

  Conditions: This symptom is reported to be present in all Cisco IOS Release 15.X(S) versions.

  Workaround: Issuing global clear count (“clear counters”) will clear counters including pseudowire specific counters.

- CSCtz60398

  Symptoms: Continuous “platform assert failure” trace backs with CFM over Xconnect on the box occurs.

  Conditions: This symptom occurs with CFMoXconnect and MPLS TE in the core. Flap the core-facing link.

  Workaround: There is no workaround.

- CSCtz97197

  Symptoms: SIP SPAs go in the out of service state in a scaled subinterface configuration (more than 2000 subinterfaces on a single Gigabit Ethernet port).

  Conditions: This symptom occurs while performing ISSU between the iso1-rp2 and iso2-rp2 Cisco IOS XE Release 3.6S throttle image. After ISSU runversion, the SIP SPAs go in the out of service state. This issue is seen in a heavily scaled configuration. The issue is observed when there are 2000 to 3000 subinterfaces on a single SPA and the following limits are exceeded:

  ```
  Overall Dual stack VRFs per box: 2800 Dual stack limit on interface: 1000
  ```

  Workaround: This issue is not seen in the following scenario:

  1. Before doing a load version from RP0(initial active), enter the following command:

     ```
     asr1000# show ipv6 route table | inc IPv6
     ```

  2. Note down the number of IPv6 route tables in the system.
  3. Do a load version.
  4. Wait for standby to come up to Standby hot.
  5. Enable the standby console from RP0 (active).

     ```
     asr1000#configure terminal
     Enter configuration commands, one per line. End with CNTL/Z.
     asr1000(config)#
     asr1000(config)#redundancy
     asr1000(config-red)#main-cpu
     asr1000(config-r-mc)#standby console enable
     ```

  6. Log in to the standby console and enter the following command:

```
asr1000-stby# show ipv6 route table | inc IPv6
```

7. Then, note down the number of IPv6 route tables in standby. If the number is lesser than the number noted in step 2, wait for some time and reverify till it reaches the number noted in step 2.
8. Issue ISSU runversion from RPO(active).

- CSCua43781

  Symptoms: WCCP redirection does not work. The mls netflow table does not get installed in the Cisco Catalyst 6500 switches for packets to get redirected to the WAAS hardware.

  Conditions: This symptom occurs when the current configuration, MASK/GRE/GRE, is changed to HASH/L2/L2.

  Workaround: Perform shut/no shut once or twice on the interface connected to the WAE hardware.

- CSCub10950

  Symptoms: The router crashes when an MR-APS switch is made. The crashes occur randomly.

  Conditions: This symptom occurs when the MLP is configured with 12 links.

  Workaround: There is no workaround.

- CSCub12911

  Symptoms: The Cisco ASR Series routers crash if the AAA profile is not defined and a DHCP discover message is sent from MN to MAG/ISG.

  Conditions: This symptom occurs when the AAA profile is not defined.

  Workaround: Define the AAA profile in ISG.

- CSCub28997

  Symptoms: Overlord crashes with 2000 crypto sessions (4000 IPSec SAs) upon repeatedly clearing and reestablishing the SAs.

  Conditions: This symptom is observed when the box is configured with 1K VRFs and 1K Virtual templates, and the crypto sessions are repeatedly cleared or reestablished.

  Workaround: There is no workaround.

- CSCub45763

  Symptoms: The device crashes due to SYS-2-FREEFREE and SYS-6-MTRACE messages while a CDP frame is being processed.

  Conditions: This symptom occurs when CDP is in use.

  Workaround: Disable CDP using the **no cdp run** command.

  Note: If the device in question relies on or supports a phone or voice network, this is not a valid workaround.

- CSCub56064

  Symptoms: Ping fails after doing EZVPN client connect if CEF is enabled.

  Conditions: This symptom is observed with the Cisco IOS Release 15.3(0.8)T image. This issue is seen only for a specific topology, where the in/out interface is the same.

  Workaround: There is no workaround.

- CSCub56842

  Symptoms: The router stops passing IPsec traffic after some time.

Conditions: This symptom is observed when the **show crypto eli** command output shows that during every IPsec P2 rekey, the active IPsec-Session count increases, which does not correlate to the max IPsec counters displayed in SW.

Workaround: Reload the router before active sessions reach the max value.

To verify, do as follows:

```
router#sh cry eli
CryptoEngine Onboard VPN details: state = Active
Capability: IPPCP, DES, 3DES, AES, GCM, GMAC, IPv6, GDOI, FAILCLOSE, HA
IPSec-Session: 7855 active, 8000 max, 0 failed <<<
```

- CSCub58119

  Symptoms: VRF-aware GRE tunnel traffic drops while performing SSO(VRF-GRE tunnel adjacency is wrong after performing SSO).

  Conditions: This symptom occurs because of incorrect programming of the adjacency interface.The adjacency information on the standby is incorrect as it does not get synced from “active”. Configure VRF-aware GRE tunnels and send traffic to all the tunnels. Perform SSO and traffic drops on all the tunnels.

  Workaround: Reload the router or perform shut/no shut on the tunnels.

- CSCub60422

  Symptoms: The ME-3600X-24CX-M box crashes on executing the **diagnostic start test all** command.

  Conditions: This symptom occurs on executing the **diagnostic start test all** command.

  Workaround: There is no workaround.

- CSCub72198

  Symptoms: Executed CLI fails to sync to standby and results in standby reload.

  Conditions: This occurs when the following conditions are met:

  1. Active and standby are running different version of IOS image.
  2. The CLI being applied is not PRC compliant, meaning that this CLI does not return a valid parser return code.

  Workaround: Avoid applying CLIs that are not PRC compliant during image upgrade or downgrade.

- CSCub85416

  Symptoms: The router crashes after the ISSU RUN VERSION in the latest mcp_dev image with G8302 configurations.

  Conditions: This symptom occurs with 11k EoMPLS VC and G8302 configurations.

  Workaround: There is no workaround.

- CSCub93442

  Symptoms: FlexVPN client does not get assigned with IPv6 address when IPv6 address is assigned using radius attribute “addrv6”.

  Conditions: This symptom is observed on assigning IPv6 using the radius attribute “addrv6”.

  Workaround: Assign IPv6 address statically or use radius IPv6 pool attribute “ipv6-addr-pool”.

  Further Problem Description:

  1. Radius Server is used for assigning IPv6 address to the FlexVPN clients.

2. Using radius attribute “ipv6-addr-pool” for assigning IPv6 address from a Ipv6 pool defined works fine.
3. If Radius attribute “addrv6” is used to assign IPv6 address then the IPv6 address assignment fails and client sends notification with internal address failure.

- CSCuc05929

  Symptoms: After a reload, sometimes the MPLS forwarding function on some interfaces is not enabled. Some interfaces that were configured with “mpls ip” and link-state-up do not show with the **show mpls interface** command. This issue depends on a timing of the interface up.

  Conditions: Sometimes the issue occurs after a router reload or SIP/SPA reload. It is not affected when you configure “mpls ip” on an interface, admin-shutdown/no shutdown, and link-flap.

  Workaround: There is no workaround. When the issue occurs, do an admin-shutdown/no shutdown on the affected interface or disable/re-enble MPLS on the interface.

- CSCuc21610

  Symptoms: The console displays a message indicating that offloading is not supported for the BFD echo mode.

  Conditions: This symptom occurs when a BFD session is configured in the echo mode.

  Workaround: There is no workaround. The issue has no functionality impact.

- CSCuc23542

  Symptoms: The PXE client network boot fails when an ME3600-running 152-4.S is the DHCP relay agent.

  Conditions: This symptom occurs when the ME3600 changes the option 54 “DHCP Server Identifier” address to its own IP address in the DHCP Offer received from the PXE DHCP server. This causes the client to send the PXE boot request (port 4011) to the ME3600 instead of the PXE server.

  Workaround: Downgrade ME3600 to Cisco IOS Release 15.1(2)EY.

- CSCuc31761

  Symptoms: The router crashes when GDOI groups are removed.

  Conditions: This symptom occurs when the “crypto isakmp diagnose error <no>” CLI is enabled. This CLI is now enabled by default.

  Workaround: Remove or disable the **crypto isakmp diagnose error** command.

- CSCuc43719

  Symptoms: The Cisco ASR 903 router with dual RSP may crash.

  Conditions: This symptom occurs with configurations related to NBAR. There is no specific trigger for this symptom.

  Workaround: Do not have any NBAR configurations on the box as these are not supported on the Cisco ASR 903 router.

- CSCuc54300

  Symptoms: During an SSO or an initial bootup, standby fails and reboots again.

  Conditions: This symptom occurs when a reload or SSO is performed.

  Workaround: There is no workaround.

- CSCuc54604

  Symptoms: CUBE SP does not respond to any SIP messages sent across using TCP. Call Flow:

```
Multiple CUCM's ---> SIP --->CUBE SP--->Provider
```

Conditions: This symptom occurs in the Cisco IOS Release 15.2(01)S01 and is only active when there are calls running SIP TCP. During create/close transaction on TCP, the control buffer will be on hold. So if closing of the existing TCP connection is needed while the control buffers are all being held, the connection will be marked as dead and will not be able to notify the corresponding peer. Therefore, the peer might still send data through that connection which CUBE-SP would think as invalid and get dropped internally.

Workaround: Send the SIP call as UDP instead of TCP.

- CSCuc59386

  Symptoms: Continuous IOMD crashes occur on OC-3 IM. Interfaces on OC-3 IM are not configurable and the following error message is seen:

  ```
  stand-by does not support this command
  ```

  Conditions: This symptom is seen on an HA Cisco ASR 903 router setup with OC-3 IM. It is observed when an IOMD crash happens on an active RSP and the standby IOMD session handle is not cleared.

  Workaround: Reload the standby RSP.

- CSCuc78328

  Symptoms: SP crashes followed by an RP reset.

  Conditions: This symptom occurs when multicast-enabled (PIM) tunnels are protected with IPSec.

  Workaround: There is no workaround.

- CSCuc85319

  Symptoms: RP crashes during the TFTP ATM interface configuration.

  Conditions: This symptom occurs after flapping the ATM subinterface configured with the ATM bundle 8192 times.

  Workaround: There is no workaround.

- CSCuc93082

  Symptoms: A Bulk Sync failure occurs.

  Conditions: This symptom occurs when the standby is brought up from ROMmon and the **service-policy** command is configured on the CEM circuit as active.

  Workaround: There is no workaround.

- CSCuc96345

  Symptoms: ARP exchange between the Cisco 7600 and the client device fails. The Cisco 7600 has an incomplete ARP entry in its ARP table for the client. This issue is likely to be seen between the Cisco 7600 and other Cisco platforms with MAC address 6073.5Cxx.xxxx. The incoming ARP reply is parsed by the platform CEF as an IP packet and dropped.

  The following OUIs (as of October 30, 2012) are affected: (first 3 bytes from MAC address/MAC starts with)

  ```
  14-73-73 20-73-55 4C-73-67 4C-73-A5 54-73-98 60-73-5C (One of Cisco's OUI ranges)
  64-73-E2 70-73-CB 8C-73-6E 98-73-C4 A0-73-32 C4-73-1E D0-73-8E F0-73-AE F4-73-CA
  ```

  Conditions: This symptom is observed with the EVC pseudowire and 802.1q subinterface on the same physical interface, and connectivity via the subinterface is affected.

  Sample configuration:

```
interface TenGigabitEthernet3/1 service instance 2013 ethernet encapsulation dot1q 411
second-dot1q 200 rewrite ingress tag pop 2 symmetric xconnect 10.254.10.10 3350075
encapsulation mpls interface TenGigabitEthernet3/1.906 encapsulation dot1Q 906 ip
address 10.10.10.1 255.255.255.0
```

Workaround: - There should be a static ARP entry on the Cisco 7600 for the client's MAC and IP. - Change the MAC address of client to a nonaffected OUI.

NOTE: This DDTS is caused or exposed due to fix of CSCtc22745.

- CSCuc96631

  Symptoms: Incoming calls through e1 r2 stop working in Cisco IOS Release 15.2(4)M1.

  Conditions: This symptom is observed with incoming calls through e1 r2 in Cisco IOS Release 15.2(4)M1. Outgoing calls work fine.

  Workaround: Use Cisco IOS Release 15.2(2)T.

- CSCud01502

  Symptoms: A crash occurs in CME while accessing a stream in sipSPIDtmfRelaySipNotifyConfigd.

  Conditions: This symptom occurs in CME.

  Workaround: There is no workaround.

- CSCud03250

  Symptoms: Large TCP data transfers take longer than expected (about a 40% increase in time). In particular, initial BGP convergence for a full internet routing table after reload is known to increase by several minutes. Performance degradation was seen starting the XE37 throttle build 09/18 (BLD_V152_4_S_XE37_THROTTLE_LATEST_20120918_070025).

  A comparison of sniffer traces of affected and unaffected traffic will show that in impacted versions of Cisco IOS, TCP more frequently probes the path MTU, and that when the larger packets are dropped, it treats these drops as indicating the presence of network congestion, and slows down the rate of data transmission.

  Conditions: This symptom is observed when the user tries with the BLD_V152_4_S_XE37_THROTTLE_LATEST_20120917_070015 label and the performance number is still good, but the BLD_V152_4_S_XE37_THROTTLE_LATEST_20120918_070025 label image shows much higher performance numbers in the order of 400 seconds. This issue is seen when the user also tries with the BLD_V152_4_S_XE37_THROTTLE_LATEST_20120917_070015 label.

  Workaround: The underlying problem is caused by changes in the TCP path MTU discovery algorithm. Disable TCP path MTU discovery for affected BGP neighbors. Depending on the release, this is done by configuring the following:

  ```
  neighbor x.x.x.x transport path-mtu-discovery disable or no neighbor x.x.x.x transport
  path-mtu-discovery
  ```

  Note that the use of this workaround may have other negative performance consequences caused by packet fragmentation, and there may be a need to tune interface MSS.

- CSCud05368

  Symptoms: Traffic will be redirected to the WCCP client even when it is denied in the WCCP redirect ACL.

  Conditions: This symptom occurs with WCCP on the Cisco ASR 1000 router, when there are port(s) defined in service definition, for example, 80 for web-cache, while different port(s) defined in permit entries of redirect-ACL.

  ```
  For example: permit tcp any eq 81
  ```

Workaround 1: Move the deny entries before the permits when possible (especially for deny... host ...). But it still may not work in some situations.

Workaround 2: Use different redirect ACLs for each service, and remove the unnecessary ones for specific services (that is, the permit entries with ports not matching service definition).

- CSCud07642

  Symptoms: AAL0 encapsulation fails.

  Conditions: This symptom occurs when “control” is disabled.

  Workaround: There is no workaround.

- CSCud09870

  Symptoms: The device crashes when you enable ?debug cmd-cfm? over xconnect with PC.

  Conditions: This symptom is observed when you configure the CFM over xconnect with PC downmep. After enabling the **debug** command, the device crashes.

  ```
  debug ethernet cfm pm session db 0.
  ```

  Workaround: Issue the **undebug all** command.

- CSCud11627

  Symptoms: SUP720 supervisor module may hang in ROMMON after the module reset triggered by TM_DATA_PARITY_ERROR.

  Conditions: The issue is observed after a module reset triggered by TM_DATA_PARITY_ERROR.

  Workaround: Power off or power on the router.

- CSCud19149

  Symptom: Traffic drops for a few VPLS VCs with ECMP links.

  Conditions: This symptom occurs when one of the ECMP paths is shut and when more than 200 VPLS VCs are configured.

  Workaround: There is no workaround.

- CSCud22038

  Symptoms: When a PC is moved between two VLAN ports (on one port, ISG is enabled and the other port is non-ISG) several times by its LAN cable connection on the L2SW that is connected to the Cisco ASR 1000 router, the PC is unable to receive DHCP OFFER due to the wrong VLAN ID from the DHCP server on the Cisco ASR 1000 router.

  Conditions: This symptom is observed with Cisco IOS Release 15.2(4)S1.

  Workaround: There is no workaround.

- CSCud24601

  Symptoms: After performing an SSO on a Quad-SUP setup, the previous standby displays the following error message on the console:

  ```
  *Nov 16 15:50:28.455: SW1-7_STBY: ics_cs_nego_open_active_port: ERROR: (no such port):
  Failed to locate active port *Nov 16 15:50:29.591: SW1-7_STBY: Bring up standby
  supervisor as a DFC *Nov 16 15:50:32.331: %PFREDUN-SW1-7_STBY-6-STANDBY: Initializing
  for SSO mode in In-chassis Domain
  ```

  Conditions: This symptom occurs occasionally after performing an SSO on a Quad- SUP setup. This error message is harmless. The system will still reach SSO successfully.

  Workaround: There is no workaround.

- CSCud28541

  Symptoms: SP crashes on doing **no mpls ip** followed by **shut** on port-channel acting as core link for scaled VPLS and EoMPLS setup.

  Conditions: In case of VPLS going over port-channel protected by IP-FRR, when the port-channel is shut the AToM VC is going down and getting created again. Also the PPO object is getting created afresh. The VC going down is not handled for VPLS case and AToM VC's pointer are still stored in IP-FRR's EoMPLS list which is getting access and hence crashing.

  Workaround: There is no workaround.

- CSCud30806

  Symptoms: Policy with class map match-all with prec 1 and prec 2 is accepted for WRED.

  Conditions: Conditions to this symptom are not known currently.

  Workaround: There is no workaround.

  Further Problem Description: match-all should not accept two prec values.

  ```
  class-map match-all prec1_2 match precedence 1 match precedence 2
  ```

- CSCud41058

  Symptoms: There is a route-map which matches tags and set a new value. This route-map is used in an EIGRP outbound distribute list. One in 10 times based on the received route tag, the correct route tag value is not set while advertising out.

  Conditions: The symptom is observed when you use a route map which matches tags and sets a new tag. Used in **distribute-list route-map** *name* **out**.

  Workaround: Clear the EIGRP process or readvertise the route.

- CSCud46309

  Symptoms: When an SSO is configured and a GR full mode is not configured, TE tunnels may stay down after a switchover.

  Conditions: This symptom is observed under the following conditions:

  - When SSO is configured.
  - When GR full mode not configured.
  - When a switchover is performed.

  Workaround: There is no workaround.

- CSCud51791

  Symptoms: Memory leak is seen on the router related to CCSIP_SPI_CONTRO.

  Conditions: This symptom is observed in CME SIP phones with Presence in running-configuration.

  Workaround: There is no workaround. You may try to remove Presence from running-configuration.

- CSCud56281

  Symptoms: There is a memory corruption issue while loading an NBAR protocol pack.

  Conditions: This symptom occurs when an NBAR protocol pack is loaded onto the router using the **ip nbar protocol-pack** command.

  Workaround: There is no workaround.

- CSCud63381

  Symptoms: Switching from periodic to on-demand DPDs may cause the DPDs to fail intermittently and thus IPSEC Failover may not work correctly.

  Conditions: This symptom is observed under the following conditions:

  1. If you are using Cisco 7200-VSA.
  2. For Cisco IOS Release 15.1(4)M2.
  3. When on-demand DPDs are configured for IPSEC Failover.

  Workaround: Disable the SCTP session:

  ```
  ipc zone default association 1 shutdown
  ```

- CSCud64870

  Symptom: DMVPN hub ASR1004 may crash after fetching the CRL from MS CRL server.

  Conditions: The crash occurs when there are 5 CDPs for the hub router to fetch the CRL. Since there are multiple CDPs, the hub router fetches the CRL in a parallel way, which leads to a crash under a timing issue.

  Workaround: Setting up one CDP instead of multiple CDPs will avoid the timing condition that leads to the crash.

- CSCud66955

  Symptoms: SPA-2CHT3-CE-ATM is flapping with Nortel Passport due to the fast bouncing of up or down 10s, after the interface is brought up.

  Conditions: This symptom is observed in E3 and DS3 mode.

  Workaround: There is no workaround.

- CSCud67105

  Symptoms: Virtual-Access is not removed when “clear ip nhrp” or “clear crypto session” are issued or when spoke-spoke FlexVPN session is gone. This is seen only in case of FlexVPN.

  Conditions: This symptom is seen only when CSCuc45115 is already in image.

  Workaround: There is no workaround.

- CSCud68830

  Symptoms: End to end L3 traffic is affected if the host queue (cpu queue 2) increments continuously at high rates (2000 packets and above).

  Conditions: This symptom occurs when the host queue (cpu queue 2) increments continuously at high rates (2000 packets and above).

  Workaround: There is no workaround.

- CSCud69421

  Symptoms: The router crashes continuously after downgrade with mode 3.

  Conditions: This symptom is observed when you set the SDM preferred template to mode 3 and reload with the XE37 image.

  Workaround: After the router crashes, boot with any XE38/mcp_dev image and set the SDM preferred template to mode 4 (mode 2) and boot with the XE37 image.

- CSCud71606

  Symptoms: The LSMPI Tracebacks errors are seen while clearing IP routes multiple times.

Conditions: This symptom is observed under the following conditions:

- Configuring OSPF
- Has more than 1000 OSPF neighbor, which will make OSPF LSU packet get fragmented
- Clear IP OSPF process * and OSPF will send LSU packet, which triggers this error message

>Workaround: There is no workaround.

- CSCud78649

  Symptoms: The following error message occurs when activating SBC:

  ```
  SBC: SBC ^T^U^V not configured
  ```

  Conditions: This symptom is observed when you run the **activate** command just after the **media-address ipv4 ...** command, as shown below:

  ```
  ASR-1001-CCN-7(config)#sbc test ASR-1001-CCN-7(config-sbc)#sbe
  ASR-1001-CCN-7(config-sbc-sbe)#media-address ipv4 1.20.0.2 vrf vrfa
  ASR-1001-CCN-7(config-sbc-media-address)#activate SBC: SBC ^A^T not configured
  ```

  Workaround: Exit SBC first, then enter SBC again and then run the **activate** command.

- CSCud84695

  Symptoms: Serial interface with FRF.12 feature is not coming up.

  Conditions: This symptom is observed when the flags related to FRF.12 feature are not properly updated in Elocal UCODE table.

  Workaround: There is no work around.

- CSCud86240

  Symptoms: The Cisco ASR 1000 ESP crashes (ucode core file created) when compressed packets are sent on a Multilink PPP interface using the Cisco IOS XE 3.5 Release and earlier Cisco ASR 1000 software images. On Cisco IOS XE 3.6 Release and later on Cisco ASR 1000 software images a crash does not occur, but routed traffic on configured interfaces are not forwarded.

  However, local traffic between the peer routers may still be forwarded. In all releases, routed traffic will be dropped on any other interfaces (for example, PPP, Multilink PPP, HDLC, and so on.) configured for this mode of compression.

  Conditions: This symptom is observed if the legacy IOS compression feature compress **[mppc | stac | predictor]** is configured on any interface (for example, PPP, Multilink PPP, HDLC, and so on.).

  If this feature is configured on a Multilink PPP interface then the ESP crash can be encountered if using an Cisco IOS XE 3.5 Release and an earlier Cisco ASR 1000 software image.

  Workaround: Remove the compress **[mppc | stac | predictor]** feature configuration from all interfaces as this functionality is not supported on the Cisco ASR 1000 router. The software fix associated with this bug report will be removing this configuration option from the Cisco ASR 1000 router.

- CSCud90457

  Symptoms: The serial interface of CE interfaces connected to the CEM interfaces on PE remain down on router reload with scaled configuration.

  Conditions: This symptom is observed when you have CESoP and SAToP scaled circuits and perform a router reload.

  Workaround: Perform IM OIR to resolve the issue.

- CSCud96075

  Symptoms: A router running Cisco IOS Release 15.2(4)M2 will reload with a bus error soon after the DSP reloads when there is a live transcoding session.

  Conditions: This symptom is observed with Cisco IOS Release 15.2(4)M2.

  Workaround: There is no workaround.

- CSCud99911

  Symptoms: There may be a delay of 15 seconds or more before switching over to a backup pseudowire in a pseudowire redundancy configuration.

  Conditions: This symptom is observed on the Cisco ME 3600 platform when the attachment circuit is a VLAN.

  Workaround: There is no workaround.

- CSCue00726

  Symptom: There is no functional impact to the system performance, warning messages will be seen only during initialization of the router and there are no security concerns on these units:

  ```
  *Dec 16 17:58:02.432: IOSXE_PLATFORM-3-WDC_INVALID_LENGTH WDC length can not be
  determined: 65535
  *Dec 16 17:58:10.703: PLATFORM_SCC-1-AUTHENTICATION_FAIL Chassis authentication failed
  *Dec 16 17:58:10.703: IOSXE_AUTHENTICATE-2-AUTHENTICATE_FAILED. The platform
  authentication failed
  ```

  Conditions: Programming of Quack & WDC (Watch Dog Certificate) was accidentally disabled in manufacturing during the regression testing. This caused units to ship without Quack & WDC programming. These messages show up at boot up for those specific units that had the quack disabled.

  Workaround: There is no workaround.

  Field Action: Strategy for Field Units:

  - Update Cisco IOS to remove authentication error messages for impacted serial numbers only. This action is In progress.
  - Target code releases with the update include Cisco XE 3.7.3 and Cisco XE3.8.1 and later.
  - TAC teams have the effective serial number list. Customers will be given a choice to upgrade to new Cisco IOS image (availability to be confirmed) or RMA the unit.
  - Customer also have the option to take no action if they want to ignore this message.

- CSCue03316

  Symptoms: The box crashed during scale testing.

  Conditions: During scale testing, the box runs out of memory resulting in MALLOCFAIL. Memory malled is not checked for failure resulting in crash.

  Workaround: There is no workaround.

- CSCue03418

  Symptoms: The OSPF protocol flaps may be noticed on executing the "redundancy force switchover" or on switchover. These are seen very intermittently and can cause about 20 to 30 seconds of traffic loss.

  Conditions: This symptom is observed on SSO or executing the **redundancy force-switchover** command and on a HA system with 6 seconds as OSPF "dead-interval".

  Workaround: Increase the dead-interval value.

- CSCue05358

  Symptoms: "Collect Identifier mac-address" -- for routed session is not working for the client who roams to a new interface.

  Conditions: This symptom is observed if the subscriber already has a session available in Interface 1.

  Workaround: There is no workaround.

- CSCue05492

  Symptoms: The DHCP snooping client ignores the IPC flow control events from CF.

  Conditions: This symptom is observed when CF gives flow control off event and the DHCP snooping client does not handle it.

  Workaround: There is no workaround.

- CSCue15619

  Symptoms: The SBC CLI hangs after configuring signaling-peer-port.

  Conditions: This symptom is observed after you re-configure the signaling-peer-port when the adj is already attached, the new vty terminal would be hung.

  Workaround: Perform "no attach" adjacency first.

- CSCue17116

  Symptoms: The following error message is logged during churning of EoGRE GTP sessions.

  ```
  Traceback %IDMGR-3-INVALID_ID: bad id in id_get (Out of IDs!)
  ```

  Conditions: This traceback is logged while churning 18,000 EoGRE GTP sessions.

  Workaround: There is no workaround.

- CSCue17123

  Symptoms: The ATM/IMA ping fails from 2nd interface post SSO in Cisco IOS XE 3.9 Release.

  Conditions: This symptom is observed when you have multiple ATM interfaces and issue switchover. Traffic does not flow from 2nd interface after switchover.

  Workaround: There is no workaround.

- CSCue18133

  Symptoms: The Cisco 7600 Router crashes at show_li_users.

  Conditions: This symptom is observed under the following conditions:

  1. In li-view, create an username: lawful-intercept and li_user password: lab1.
  2. Then, attempt its delete by "no username li_user".
  3. Later, show users of LI.

  Workaround: There is no workaround.

- CSCue25575

  Symptoms: The crash is observed for SDP pass through or call forward or antitrombone cases.

  Conditions: The crash is observed for a basic call involving SDP pass through or call forward or antitrombone cases.

  Workaround: There no workaround.

- CSCue27652

  Symptoms: The ATM interfaces are getting deleted on SSO.

Conditions: This symptom is observed when the ATM Interfaces are deleted on standby after IM OIR.

Workaround: There is no workaround.

- CSCue27698

  Symptoms: Configuring long list of REP block port preferred VLAN will result in losing part of this configuration after the reload.

  Example: Configuration like this

```
rep block port preferred vlan
76-86,94,98,200-201,400,592-593,606-607,611,633,635-636,638,640,643,901-902,1026,
1539,2007-2064
```

  will result in two lines in running configuration:

```
rep block port preferred vlan 76-86,94,98,200-201,400,592-593,606-607,611,633
rep block port preferred vlan 635-636,638,640,643,901-902,1026,1539,2007-2064
```

  after the reload second line will overwrite the first and only one line will remain:

```
rep block port preferred vlan 635-636,638,640,643,901-902,1026,1539,2007-2064
```

  Conditions: This symptom is observed after the reload.

  Workaround: Reconfigure the REP block list after the reload.

- CSCue30237

  Symptoms: The CFM trace route fails.

  Conditions: This symptom occurs in CFM with VPLS in the core. Configure the Up MEP on BD which has the VFI terminated.

  Workaround: There is no workaround. The issue is specific to VPLS in the core and Up MEP on the same BD.

- CSCue30590

  Symptoms: Packet loss are seen over pseudowire and high CPU.

  Conditions: This symptom is observed when IPv6 site-local multicast MAC traffic is sent over SVI EoMPLS, the traffic is looped between the PE of the EoMPLS.

  Workaround: There is no workaround.

- CSCue31321

  Symptoms: A Cisco router or switch may unexpectedly reload due to bus error or SegV when running the **how ip cef ... detail** command.

  Conditions: This symptom is observed when the output becomes paginated (---More---) and the state of the CEF adjacency changes while the prompt is waiting on the more prompt.

  Workaround: Set “term len 0” before running the **how ip cef ... detail** command.

- CSCue38489

  Symptoms: Multicast packets (both data and control) get duplicated when they egress out of the port channel with ten gigabit interface members.

  Conditions: This symptom occurs when we create the below configurations. Duplicate packets with Service Instance/ EFPs for multicast packets arise when the below conditions are true:

  - The port channel has only ten gigabit interfaces as members.
  - Multicast, unlearnt unicast, or broadcast packets egress out on the port channel interface.

But after reloading the box with the given configurations, the problem is seen only when admin shut/no shut is performed at least once on the port channel interface.

Workaround: There is no workaround.

- CSCue40354

  Symptoms: CPUHOG error message is seen at nile_mgr_bdomain_get_efp_count and then followed by a crash.

  Conditions: This symptom is observed on booting the router with scaled mVPN configurations.

  Workaround: There is no workaround.

- CSCue43250

  Symptoms: IMA configuration will not be parsed correctly after the router reload, when the A903-IM40S is inserted in Bay4/Bay5 of the ASR903 router.

  Conditions: This symptom is observed when the IMA and ATM interfaces are adjacent. This happens only for IM inserted on Bay 4 or above.

  Workaround: Insert the IM in bay 0 bay 3 if you want the IMA and ATM parsing to work, or reconfigure the ATM and IMA interfaces, for it to work.

- CSCue43776

  Symptoms: Cisco IOS memory leak at com.cisco.cxsc-cxsc-5651.

  Conditions: This symptom is observed when K2 firewall and kWAAS are configured.

  Workaround: There is no workaround.

- CSCue45934

  Symptoms: This problem is specific to the Catalyst 6000 platform. With IPv4 crypto map, ICMP echo reply is not triggered from the remote end.

  Conditions: This symptom is observed in IPv4 crypto map configuration and Catalyst 6000 platform.

  Workaround: There is no workaround.

- CSCue46685

  Symptoms: Client MAC/framed IP missing in the coa:session query response from ISG.

  Conditions: The symptom is observed when you do a COA account-query for lite-session.

  Workaround: There is no workaround.

- CSCue52708

  Symptoms: The router crashes upon defaulting the backup switch interface configuration immediately after doing shut/no shut on it.

  Conditions: This symptom is observed after the admin shut/no shut wait for some time (till the port comes up) before defaulting the interface configuration.

  Workaround: There is no workaround.

- CSCue55739

  Symptoms: PfR MC/BR session may be flapped, if PfR learn is configured with scale configuration.

  Conditions: This symptom may be observed, if PfR traffic-classes are learned by PfR global **learn** configuration.

  Workaround: Disable PfR global **learn** by configuring **traffic-class filter access-list** pointing to the **deny ip ip any** ACL, and configure PfR learn “list”.

- CSCue59773

  Symptoms: ARP for default gateway will not be resolved

  Conditions: This symptom is observed when client has a lite session in ISG and he clears his ARP table and then tries to query for the ARP second time

  Workaround: Do not clear the ARP entry in the client.

- CSCue65523

  Symptoms: The **archive download** command fails in mcp_dev/xe39 nightly image which is being used for software up-gradation.

  Conditions: This symptom is observed only on the whales 2 box.

  Workaround: There is no workaround.

- CSCue67751

  Symptoms: The classification based on QoS group egress policy is not working correctly.

  Conditions: With L3VPN configuration, the core interface packets should be classified based on EXP and marked with QoS-group. On the egress interface packets should be classified based on QoS group on the service instance.

  Workaround: There is no workaround.

- CSCue69527

  Symptoms: More than 95 SCCP controlled FXS ports cannot be configured on the Cisco VG350.

  The debug output for “debug ccm-manager config-download errors” is as follows:

  ```
  cmapp_sccp_gw_start_element_handler: warning - max number of interfaces reached.
  ```

  Conditions: This symptom occurs when configuring more than 95 SCCP FXS ports on the Cisco VG350 using CUCM.

  Workaround: There is no workaround.

- CSCue76251

  Symptoms: A BFD session is created for tunnel-tp without any BFD configuration underneath it.

  Conditions: This symptom occurs only on bootup and when there is no BFD configuration underneath tunnel-tp.

  Workaround: There is no workaround.

- CSCue77909

  Symptoms: The interface link shows UP, without fiber IN.

  Conditions: This symptom is observed with OCP vendor 100FX SFP on whales2.

  Workaround: There is no workaround.

- CSCue85737

  Symptoms: ASR with PKI certificate may crash when issuing **show crypto pki certificate** command.

  Conditions: This symptom is observed when the **show crypto pki certificate** command is issued on ASR with PKI certificate.

  Workaround: There is no workaround.

- CSCue86147

  *Policy with class map match-all with prec 1 and 2 is accepted for WRED.

- CSCue86845

  Symptoms: An unexpected behavior caused with Ingress QoS, caused by commit CSCuc01040.

  Conditions: This symptom is observed with Ingress QoS, caused by commit CSCuc01040.

  Workaround: There is no workaround.

- CSCue89385

  Symptoms: Traffic from routed VPLS does not trigger ARP.

  Conditions: This symptom is observed in a routed VPLS network that has multiple CE routers connected to the PE router. The issue occurs when a local CE router is connected to the PE router via an EVC and when a ping is sent from a local CE router to the remote CE router.

  Workaround: Ping the first interface VLAN of the EVC to resolve the ARP.

- CSCue92705

  Symptoms: The "DHCPD Receive", "CDP Protocol", and "Net Background" processes leaks could be seen after disabling "macro auto monitor".

  Conditions: This symptom is observed in Cisco IOS 15.0(2)SE1 Release, 2960S, dhcp, cdp traffic, and link flapping.

  Workaround: Configure "no service dhcp" if the switch is not a DHCP server.

  ```
  Configure device-sensor filter-spec cdp exclude all device-sensor filter-spec dhcp
  exclude all device-sensor filter-spec lldp exclude all
  ```

- CSCue97986

  Symptoms: Calls hang at SIP, CCAPI and VOIP RTP components (but are cleared in the dataplane of the Cisco ASR 1000 series platform).

  Conditions: This symptom occurs when a video call is setup as an audio call. The call then gets transferred with REFER but the caller hangs up the call before the call gets transferred. This is an intermittent problem.

  Workaround: If there is an SIP call dangling (sh sip call sum), then use the **clear cal voice causecode 16** command to clear the dangling call.

- CSCuf16504

  Symptoms: Classification based on the QoS group along with prec/dscp at the egress policy does not function as expected.

  Conditions: This symptom occurs with L2VPN/L3VPN configuration. On the core interface, packets should be classified based on exp and marked with the QoS group. On the egress interface, packets should be classified based on the QoS group and prec/dscp/cos inner.

  Workaround: There is no workaround.

- CSCuf17009

  Symptoms: With PIM enabled on a P2P GRE tunnel or IPSec tunnel, the SP of the Cisco 7600 series router might crash.

  Conditions: This symptom occurs when there are more number of tunnels going via the same physical interface. This issue is seen in Cisco IOS SREx and Cisco IOS 15.S based releases only.

  Workaround: There is no workaround.

- CSCuf20407

  Symptoms: Tracebacks are seen on Whales2 bootup.

Conditions: This symptom occurs when Whales2 boots with Cisco IOS Release 15.2(4)S0.2, Cisco IOS Release 15.3(1)S0.1 or prior releases on the new Rev 2 HW.

Workaround: There is no workaround.

- CSCuf20537

  Symptoms: The router crashes due to null pointer dereference.

  Conditions: This symptom occurs with the C4 VSS system (2 sup vss) with dual-homed fex stack (This has not been seen on other platforms, but the fix is ported as a precautionary measure). During the first SSO, no crash is observed [Active and Standby (Hot-Standby)]. During the second SSO, a is crash observed.

  Workaround: There is no workaround.

- CSCuf25555

  Symptoms: Policy-based routing stops working after the router reloads.

  Conditions: This symptom occurs when multiple next-hops configured on the same route map are reachable through the same interface.

  Workaround: Remove and reconfigure the route-map.

  Further Problem Description: This is a specific scenario where multiple next-hops configured on the same route map are reachable through the same physical interface on different VLANs.

  After reload, when the physical interface comes up, adjacency for all configured next-hops on different sequence numbers of the same route map were notified to the PD client simultaneously.

- CSCuf30554

  Symptoms: A traffic drop is seen with scalable EoMPLS VCs going over TE tunnels. The issue is reproduced if a large or small number of tunnels are present and they undergo a lot of flap events.

  Conditions: This symptom occurs when the MPLS label for a TE internal label gets allocated with a value having more than 20 bit.

  Workaround: There is no workaround.

- CSCuf43548

  Symptoms: When the POS Rx fiber at the tail end of the MPLS TE FRR is pulled, the FRR takes longer than 200ms to cut over to the other tunnel.

  Conditions: This symptom occurs with POS MPLS TE FRR when the head end receives a remote defect due to the Rx fiber pull at the tail end. Remote defects do not trigger FRR quickly.

  Workaround: There is no workaround.

- CSCuf65255

  Symptoms: CPU hog is caused by unnecessary calling of avl_get_next to calculate the dynamic MPLS label range for each of the service instances configured (especially for L3VPN services).

  Conditions: This symptom occurs under the following conditions:

  1. When running configuration is accessed using the “show running-config” CLI.
  2. While copying running configuration to either the startup configuration or the local disk or the tftp server.

  This results in the copy operation taking more than 300 seconds (for an average configuration size of 1000kB).

  Workaround: Reducing the number of BGP routes injected for L3VPN sessions causes the CPU hog to last for a smaller duration.

- CSCug31561

  A vulnerability in the DHCP implementation of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

  The vulnerability occurs during the parsing of crafted DHCP packets. An attacker could exploit this vulnerability by sending crafted DHCP packets to an affected device that has the DHCP server or DHCP relay feature enabled. An exploit could allow the attacker to cause a reload of an affected device.

  Cisco has released free software updates that address this vulnerability. There are no workarounds to this vulnerability.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130925-dhcp

  Note: The September 25, 2013, Cisco IOS Software Security Advisory bundled publication includes eight Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the September 2013 bundled publication.

  Individual publication links are in "'Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep13.html

Open Caveats—Cisco IOS Release 15.2(4)S2

Cisco IOS Release 15.2(4)S2 is a rebuild release for Cisco IOS Release 15.2(4)S. The caveat in this section is open in Cisco IOS Release 15.2(4)S2. This section describes only select open caveats.

- CSCud36113

  Symptoms: Ping fails between CE routers.

  Conditions: This symptom is observed when you configure MPLS VPN Inter-AS IPv4 BGP Label Distribution and flaps "mpls bgp forwarding" in the interface between ASBRs.

  Workaround: Removing and adding (flapping) the static routes between ASBRs resolves the issue.

Resolved Caveats—Cisco IOS Release 15.2(4)S2

Cisco IOS Release 15.2(4)S2 is a rebuild release for Cisco IOS Release 15.2(4)S. The caveats in this section are resolved in Cisco IOS Release 15.2(4)S2 but may be open in previous Cisco IOS releases.

- CSCtg39957

  The Resource Reservation Protocol (RSVP) feature in Cisco IOS Software and Cisco IOS XE Software contains a DoS vulnerability.

  Cisco has released free software updates that address this vulnerability. There are no workarounds available to mitigate this vulnerability.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-rsvp

Note: The March 27, 2013, Cisco IOS Software Security Advisory bundled publication includes seven Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the March 2013 bundled publication.

Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar13.html

- CSCtg47129

  The Cisco IOS Software implementation of the virtual routing and forwarding (VRF) aware network address translation (NAT) feature contains a vulnerability when translating IP packets that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are not available.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-nat

  Note: The March 27, 2013, Cisco IOS Software Security Advisory bundled publication includes seven Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the March 2013 bundled publication.

  Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar13.html

- CSCtk15666

  Symptoms: The Cisco IOS password length is limited to 25 characters.

  Conditions: This symptom is observed on Cisco NG3K products.

  Workaround: There is no workaround.

  PSIRT Evaluation: The Cisco PSIRT has evaluated this issue and does not meet the criteria for PSIRT ownership or involvement. This issue will be addressed via normal resolution channels.

  If you believe that there is new information that would cause a change in the severity of this issue, please contact psirt@cisco.com for another evaluation.

  Additional information on Cisco's security vulnerability policy can be found at the following URL:

  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCts52120

  Symptoms: Tracebacks are seen for PLATFORM_INFRA-5-IOS_INTR_OVER_LIMIT.

  Conditions: This symptom is observed with RPSO.

  Workaround: There is no workaround.

- CSCts75737

  Symptoms: Tracebacks are seen at swidb_if_index_link_identity on the standby RP.

  Conditions: This symptom is observed when unconfiguring and reconfiguring "ipv4 proxy-etr" under the router LISP.

Workaround: There is no workaround.

- CSCtu28696

  Symptoms: A Cisco ASR 1000 crashes with **clear ip route ***.

  Conditions: This symptom is observed when you configure 500 6RD tunnels and RIP, start traffic and then stop, and then clear the configuration.

  Workaround: There is no workaround.

- CSCtw65575

  Symptoms: The router may unexpectedly reload when OSPFv3 MIB is polled via SNMP.

  Conditions: This symptom occurs when OSPFv3 is configured with area ranges whose prefix length is /128. A router with no area ranges is not vulnerable.

  Workaround: Configure area ranges to have a smaller prefix length (that is, in the range of /0 to /127).

- CSCtw80678

  Symptoms: Multilink PPP ping fails when the serial interfaces experience QMOVESTUCK error.

  Conditions: This symptom may be observed if multilink PPP member links and serial interfaces on which the QMOVESTUCK error is reported are on the same SPA.

  Workaround: “no shut” the interface with the QMOVESTUCK error message, remove QoS policies on the interface and subinterfaces, and remove the interface from the T1/T3 controller. Then, rebuild the configuration.

- CSCtx31177

  Symptoms: RP crash is observed on avl_search in a high scaled scenario.

  Conditions: This symptom is observed in a high scaled scenario with continuous traffic flow.

  Workaround: There is no workaround.

- CSCtx34823

  Symptoms: OSPF keeps on bringing up the dialer interface after idle-timeout expiry.

  Conditions: This symptom occurs when OSPF on-demand is configured under the dialer interface.

  Workaround: There is no workaround.

- CSCty44654

  Symptoms: The router crashes when trying to test the MVPN6 functionality.

  Conditions: This symptom is observed with the following conditions:

  - Configure the router to test the MVPN6 functionality.
  - Delete the VRF associated with the interface in the MVPN6 test configuration.

  Workaround: There is no workaround.

- CSCty57476

  Symptoms: The BGP GSHUT feature needs to add support for the AA:NN format for community.

  Conditions: This symptom is observed when support is added for the AA:NN format for community when using the BGP GSHUT feature.

  Workaround: The <1-4294967295> community number can be used instead of the AA:NN format.

- CSCty73682

  Symptoms: A small percentage of IPv6 packets that should be blocked by an interface ACL is instead pass through.

  Conditions: This symptom occurs in certain conditions, when an IPv6 ACL is applied to an interface, a small percentage of IPv6 packets that would otherwise be dropped, will instead bypass an ACL and get through.

  Workaround: There is no workaround.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5/4.8: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:N/C:P/I:N/A:N/E:F/RL:U/RC:C

  CVE ID CVE-2012-3946 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCty74859

  Symptoms: Memory leaks on the active RP and while the standby RP is coming up.

  Conditions: This symptom is observed when ISG sessions are coming up on an HA setup.

  Workaround: There is no workaround.

- CSCtz26682

  Symptoms: Switchover/reload fails in the Cisco ASR 903 HA setup due to the "LICENSE-3-ISSU_ERR: ISSU start nego session FAILED, error:-287" error message.

  Conditions: This symptom is observed with the Cisco ASR 903 router. This issue is seen only when doing a Route Processor (RP) switchover using the **redundancy force-switchover** command.

  Workaround: There is no workaround.

- CSCtz28023

  Symptoms: Traffic is not forwarded for a few mroutes.

  Conditions: This symptom is observed when multiple routers in the network are reloaded simultaneously.

  Workaround: Using the **clear ip mroute vrf** *vrf name* command may resolve the issue.

- CSCtz34869

  Symptoms: Aps-channel stops working.

  Conditions: This symptom occurs with an open ring and is seen in the following scenario:

  ```
  A1(po2)(RPL)<======>(po2)A3 (gig3/2)<=======>(gig3/3)A4
  ```

  Shut down gig3/2 on A3 does not make A1 into protection.

  - Debugs show no SF packets are being transmitted to A1 which is connected to A3 via "Port-channel".
  - A1 (po2) is RPL of the ring. It is not going to be unblocked even after the A3-A4 link goes down.

  Workaround: Reload the line card.

- CSCtz50683

  Symptoms: Upon removing 10 x MDLP sessions, one or more hardware adj remains. This happens due to incorrect removal of LSPs.

  Conditions: This symptom is observed when more than eight sub-LSPs occur.

  Workaround: Use no more than eight sub-LSPs.

- CSCtz55979

  Symptoms: The router crashes.

  Conditions: This symptom occurs when you configure CFM, SCE over MPLS, VPLS, or G.8032 services while running SNMP polling.

  Workaround: There is no workaround.

- CSCtz58189

  Symptoms: The router crashes on using the **config replace** command with certain QoS configured on the box.

  Conditions: This symptom occurs when certain QoS are configured on the box are replaced with the configuration that is removing the configurations.

  Workaround: There is no workaround.

- CSCtz58391

  Symptoms: Ingress QoS Tcams are not cleared after certain dynamic changes.

  Conditions: This symptom is observed on removing the encapsulation from the service instance and then deleting the service instance. QoS Tcams are not cleared.

  Workaround: Instead of deleting the encapsulation first, delete the service instance first.

- CSCtz88879

  Symptoms: When testing for DMVPN in a HUB-SPOKE topology, where there are 170 tunnels protected with IPsec on Spoke and one mGRE tunnel on hub. B2B redundancy is configured. No QoS is applied on the scaled IPsec tunnels. Upon doing SSO with this configuration, the "%VPNSMIOS-3-MACEDONTUNNELVLANERR: Tunnelx: allocated idb has invalid vlan id" error message is seen repeatedly on the new active and the router becomes almost inaccessible. As can be seen from the **show vlan int usage** command output, there are more than 3K free VLANs on both the hub and spoke.

  ```
  *May 14 12:31:10.315: %VPNSMIOS-3-MACEDONTUNNELVLANERR: Tunnel87: allocated idb has
  invalid vlan id
  *May 14 12:31:10.511: %VPNSMIOS-3-MACEDONTUNNELVLANERR: Tunnel26: allocated idb has
  invalid vlan id
  *May 14 12:31:10.543: %VPNSMIOS-3-MACEDONTUNNELVLANERR: Tunnel28: allocated idb has
  invalid vlan id
  *May 14 12:31:10.575: %VPNSMIOS-3-MACEDONTUNNELVLANERR: Tunnel90: allocated idb has
  invalid vlan id
  ```

  After a continuous flood of error messages, a Granikos crash is seen, and the **show cry eli** command shows only one SPA and this SPA is stuck in INIT state.

  Conditions: This symptom occurs when doing a shut/no shut using the **interface range** command, and once all tunnels are up, doing an SSO.

  Workaround: There is no workaround.

- CSCua01641

  Symptoms: The router's NAS-IP address contained in the RADIUS accounting-on packet is 0.0.0.0:

RADIUS: Acct-Session-Id [44] 10 "00000001" RADIUS: Acct-Status-Type [40] 6 Accounting-On [7] RADIUS: NAS-IP-Address [4] 6 0.0.0.0

RADIUS: Acct-Delay-Time [41] 6 0

Conditions: This symptom occurs when you restart the router.

Workaround: There is no workaround.

- CSCua12396

  Symptoms: IPv6 multicast routing is broken when there are master switchover scenarios with a large number of members in stack. This issue is seen on platforms such as Cisco 3750E and Cisco 3750X where IPV6 multicast routing is supported.

  Conditions: This symptom is observed when IPV6 multicast routing is configured, mcast routes are populated, and traffic is being forwarded. In case of master switchover, synchronization between the master and members is disrupted. This issue is seen only for IPv6 multicast routing. This issue has been observed with a 9-member stack and either during the first or second master switchover. No issues are seen for IPv4 multicast routing.

  Workaround: This scenario was tested with a 5-member stack, and no issues were seen. It is recommended to enable IPv6 multicast routing when there is deployment with low members in a stack.

- CSCua15003

  Symptoms: When a call is canceled mid-call, the CUBE may not release the transcoder resource for the call. As a result, there is a DSP resource leak.

  Conditions: This symptom can occur in the following situations:

  - CUBE receives 180 ringing with an SDP session.
  - “media transcoder high-density” is enabled.

  Workaround: Disable “media transcoder high-density”.

- CSCua20373

  Symptoms: After SSO, all the GRE tunnels get admin down and stay down until the security module SSC-600/WS-IPSEC-3 comes up. Complete traffic loss is seen during this time.

  Conditions: This symptom is observed when Vanilla GRE tunnels are configured in the system where HA and the IPsec Module SSC-600/WS-IPSEC-3 card is present, “crypto engine mode vrf” is configured, and SSO is issued.

  Workaround: Remove the “cryto engine mode vrf” configuration if IPsec is not enabled on the router.

- CSCua24689

  Symptoms: Fragments are sent without label resulting in packet drops on the other side.

  Conditions: This symptom is observed with the following conditions:

  - MPLS enabled DMVPN tunnel on egress.
  - VFR on ingress.

  Workaround: Disable VFR, if possible.

- CSCua26064

  Symptoms: IPv6 routes in the global routing table take up different adjacency entries.

Conditions: This symptom is observed when there are four core facing tunnels that load balance traffic to these prefixes. The **show mls cef ipv6** *prefix* **detail** command shows the different adjacencies taken by different prefixes.

Workaround: Have a single tunnel on the core facing side, instead of a load balanced path.

- CSCua31934

  Symptoms: A crash is seen at __be_address_is_unspecified.

  Conditions: This symptom is observed with the following conditions:

  1. It occurs one out of three times and it is a timing issue.
  2. DMVPN tunnel setup between Cisco 2901 as the spoke and Cisco ASR 1000 as the hub.
  3. Pass IPv4 and IPv6 traffic between the hub and the spoke for 5-10 minutes.
  4. It can occur with v6 traffic alone.
  5. If you remove the tunnel interface on the Cisco ASR and add it again using **conf replace nvram:startup-config** command, the crash will occur.

  Workaround: Use CLI to change configuration instead of the rollback feature.

- CSCua39390

  Symptoms: The PRI configuration (voice port) is removed after a reload.

```
interface Serial1/0:23          ^
% Invalid input detected at '^' marker.
no ip address
% Incomplete command.
encapsulation hdlc
   ^
% Invalid input detected at '^' marker.
isdn incoming-voice voice
       ^
% Invalid input detected at '^' marker.
no cdp enable
        ^
% Invalid input detected at '^' marker.
voice-port 1/0:23
           ^
% Invalid input detected at '^' marker.
Also getting trace back
%SYS-2-INTSCHED: 'may_suspend' at level 3  -Process= "Init", ipl= 3, pid= 3
-Traceback= 0x607EE41Cz 0x630F0478z 0x607F72C0z 0x60722F38z 0x6070A300z
0x6070A9CCz 0x603E1680z 0x6029541Cz 0x60298F6Cz 0x6029AD48z 0x6029D384z
0x6062BC68z 0x60632424z 0x60635764z 0x60635CE0z 0x60877F2Cz
%SYS-2-INTSCHED: 'may_suspend' at level 3  -Process= "Init", ipl= 3, pid= 3
-Traceback= 0x607EE41Cz 0x630F04E4z 0x607F7154z
```

  Conditions: This symptom is observed with Cisco IOS Release 15.1(3)T and Cisco IOS Release 15.1(4)M4. This issue is not seen with Cisco IOS Release 12.4(24)T6 or earlier release. The issue occurs after reload.

  Workaround: Reapply the configuration after the router comes back up.

- CSCua41333

  Symptoms: A crash occurs at __be_ipsub_dp_disconnect_session with DHCP scale when routed/L2-connected sessions are brought up/down one after the other.

  Conditions: This symptom occurs when you bring up scale routed DHCP sessions, later bring them down, and then bring up scale L2-connected DHCP sessions on the same interface or vice versa.

Workaround: Reload the router after changing the configuration.

- CSCua42523

  Symptoms: The router crashes and reloads when “options-keepalive” is enabled on a dial peer which has session target as sip-server.

  Conditions: This symptom is observed when enabling “options-keepalive” which has a session target as sip-server. Also, “sip-server” is configured under “sip-ua” and has a DNS address which resolves to an IPv6 address.

  Workaround: Do not enable “options-keepalive” for dial peer.

- CSCua45206

  Symptoms: The hub router crashes while removing the Stale Cache entry.

  Conditions: This symptom occurs when two spokes are translated to the same NAT address.

  Workaround: Spokes behind the same NAT box must be translated to different post-NAT Addresses.

- CSCua49764

  Symptoms: The WAAS-Express device goes offline on WCM.

  Conditions: This symptom occurs when a certificate is generated using HTTPS when using the Cisco IOS Release 15.1(3)T image. Once upgraded to Cisco IOS Release 15.2(3)T, the WAAS-Express device goes offline on WCM.

  Workaround: Configure an rsakeypair on the TP-self-signed trustpoint with the same name and execute the **enroll** command again or delete the self-signed trustpoint point and reenable the HTTP secure-server.

- CSCua55785

  Symptoms: Build breakage occurs due to the fix of CSCtx34823.

  Conditions: This symptom occurs with the CSCtx34823 fix.

  Workaround: CSCtx34823 change may be unpatched from the code-base.

- CSCua56999

  Symptoms: Abnormal line card reload occurs.

  Conditions: This symptom occurs when an MVPNv6 scaled router acts as PE on which source traffic is ingressing and the line card is connected on the access side.

  Workaround: There is no workaround.

- CSCua61330

  Symptoms: Traffic loss is observed during switchover if,

  1. BGP graceful restart is enabled.
  2. The next-hop is learned by BGP.

  Conditions: This symptom occurs on a Cisco router running Cisco IOS XE Release 3.5S.

  Workaround: There is no workaround.

- CSCua81998

  Symptoms: Doing ISSU RV in a Cisco 7600 box with the ES40 line card may sometimes cause a crash in the ES40 line card.

  Conditions: This symptom is observed with ISSU RV with Cisco IOS XE Release 3.7S, or Cisco IOS XE Release 3.8S to Cisco IOS XE Release 3.6.1S.

Workaround: There is no workaround.

- CSCua82440

  Symptoms: FNF records do not get exported when a user reloads the router.

  Conditions: This symptom occurs if a user configures a nondefault export-protocol, that is, anything other than “netflow-v9”. If the user configures a nondefault export-protocol such as IPFIX or netflow-v5, after saving the configuration to the start-up configuration and reloading the router, the exporter will not export any records.

  Workaround: Either one of the following methods will fix this issue:

  1. Remove and reconfigure the exporter configuration after reload.
  2. Change the export-protocol to the default value (netflow-v9).

- CSCua85239

  Symptoms: Flapping BGP sessions are seen if large BGP update messages are sent out and BGP packets are fragmented because midpoint routers have the smaller "mtu" or "ip mtu" configured.

```
*Jun  3 18:20:20.792 UTC: %TCP-6-BADAUTH: Invalid MD5 digest from 6.6.6.5(179)
to 2.2.2.5(17744) tableid - 0
*Jun  3 18:20:30.488 UTC: %TCP-6-BADAUTH: Invalid MD5 digest from 6.6.6.5(179)
to 2.2.2.5(17744) tableid - 0
*Jun  3 18:20:36.451 UTC: %BGP-5-ADJCHANGE: neighbor 6.6.6.5 Down BGP
Notification sent
*Jun  3 18:20:36.451 UTC: %BGP-3-NOTIFICATION: sent to neighbor 6.6.6.5 4/0
(hold time expired) 0 bytes
*Jun  3 18:20:36.569 UTC: %BGP_SESSION-5-ADJCHANGE: neighbor 6.6.6.5 VPNv4
Unicast topology base removed from session  BGP Notification sent
*Jun  3 18:20:40.184 UTC: %TCP-6-BADAUTH: Invalid MD5 digest from 6.6.6.5(179)
to 2.2.2.5(17744) tableid - 0
*Jun  3 18:20:44.619 UTC: %BGP-5-ADJCHANGE: neighbor 6.6.6.5 Up
*Jun  3 18:20:49.926 UTC: %TCP-6-BADAUTH: Invalid MD5 digest from 6.6.6.5(179)
to 2.2.2.5(17744) tableid - 0
*Jun  3 18:20:59.604 UTC: %TCP-6-BADAUTH: Invalid MD5 digest from 6.6.6.5(179)
to 2.2.2.5(17744) tableid - 0
```

  Conditions: This symptom is observed between two BGP peers with matching MD5 passwords configured and can be triggered by the following conditions:

  - If the midpoint path has the “mtu” or “ip mtu” setting that is smaller than the outgoing interface on BGP routers, it will be force the BGP router to fragment the BGP packet while sending packets through the outgoing interface.
  - Peering down and the MD5 error do not always occur. They occur only once or twice within 10 tests.

  Workaround: There is no workaround.

- CSCua85604

  Symptoms: Ingress Qos on EVC stops working after reload or after interface flap.

  Conditions: This symptom occurs only on EVC QOS.

  Workaround: Remove and reconfigure the QOS on EVC.

- CSCua90061

  Symptoms: The WS-IPSEC-3 Module crashes post configuration change.

  Conditions: This symptom occurs when you dynamically modify the GRE tunnel protected with IPsec to the sVTI tunnel and vice versa while traffic is traversing across the IPsec tunnel.

  Workaround: There is no workaround.

- CSCua91473

  Symptoms: Memory leak occurs during rekey on the IPsec key engine process.

  Conditions: This symptom occurs after rekey, when the IPsec key engine does not release KMI memory, causing the IPsec key engine holding memory to keep increasing.

  Workaround: Clear crypto session for IPsec key engine to release memory.

- CSCua91698

  Symptoms: ephone-type disappears from the running-configuration.

  Conditions: This symptom occurs in SRST mode and after reload.

  Workaround: Reconfigure the ephone-type commands and again save to the startup-configuration.

- CSCua99969

  Symptoms: IPv6 PIM null-register is not sent in the VRF context.

  Conditions: This symptom occurs in the VRF context.

  Workaround: There is no workaround.

- CSCub04112

  Symptoms: The router may lose OSPF routes pointing to the reconfigured OSPF interface.

  Conditions: This symptom occurs after quick removal and adding of the interface IP address by script or copy and paste.

  For example, configure the following:

  ```
  interface Ethernet0/0
   ip address 1.1.100.200 255.255.255.0
   ip ospf network point-to-point
   ip ospf 1 area 0
  end
  ```

  Then, quickly remove/add the IP address:

  ```
  conf t
  interface Ethernet0/0
   no ip address 1.1.100.200 255.255.255.0
   ip address 1.1.100.200 255.255.255.0
   ip ospf network point-to-point
   ip ospf 1 area 0
  end
  ```

  Workaround: Insert a short delay in between commands for removing/adding the IP address. The delay should be longer than the wait interval for LSA origination; by default, it is 500 ms. Or, refresh the routing table by “clear ip route *”.

- CSCub04345

  Symptoms: The Cisco ASR-1002-X freezes after four hours with a scaled “path-jitter” sla probe configuration.

  Conditions: This symptom is observed with a scaled “path-jitter” sla probe configuration.

  Workaround: There is no workaround.

- CSCub04982

  Symptoms: In an IPFRR configuration, a traceback is seen about changing the FRR primary OCE where the new OCE has a different interface and next-hop, which blocks such a linkage.

Conditions: This symptom occurs while changing the FRR primary OCE interface to a new OCE with a different interface.

Workaround: There is no workaround.

- CSCub06859

  Symptoms: OSPFv2 NSR on quad-sup VSS does not work. The router stops sending hello packets after switchover.

  Conditions: This symptom is observed with quad-sup VSS with OSPFv2 NSR.

  Workaround: Clear the IP OSPF process after NSR switchover.

- CSCub07855

  Symptoms: The VRF error message is displayed in the router.

  Conditions: This symptom occurs upon router bootup.

  Workaround: There is no workaround.

- CSCub15105

  Symptoms: Traffic drop of MVPNv6 data MDT packets is seen.

  Conditions: This symptom is observed on doing a VRF delete and adding it on the encapsulated PE in a scaled MVPNv6 setup; the L3 DENY RESULT drop counters increment for the encapsulated VLAN v4. From a multicast point of view, the drop is at the point where the packet reaches the encapsulated VLAN v4 to proceed further with backbone forwarding.

  Workaround: There is no workaround.

- CSCub15402

  Symptoms: A VRF cannot be deleted. The following error message is displayed:

  ```
  error message "% Deletion of VRF VPNA in progress; wait for it to complete".
  ```

  Conditions: This symptom occurs after having previously issued “sh ip cef vrf * sum”.

  Workaround: There is no workaround. Reboot is required to remove the VRF.

- CSCub22049

  Symptoms: Native MCAST traffic is not forwarded over a nile1 after core interface shut/no shut.

  Conditions: This symptom is observed after doing shut/no shut or interface flap a couple of times.

  Workaround: “clear ip mroute <mcast_group>” or “clear ip route *”.

  Further Problem Description: Not all the multicast groups will be affected. The behavior is inconsistent.

- CSCub23231

  Symptoms: Very specific events/packet types cause the ES20 LC to stop passing traffic. Information on these events and packets that lead to the issue are not known currently.

  Conditions: This symptom occurs when the ES20 interface has an EVC or MPLS configuration.

  Workaround: Reload LC.

- CSCub31477

  Symptoms: A Cisco ISG router configured for Layer 2 Connected Subscriber Sessions does not respond to ARP replies once a subscriber ARP cache has expired.

Conditions: This symptom occurs when the router is configured as ISG L2-Connect, the router has configured HSRP as the high-availability method, and the subscriber-facing interface is configured with “no ip proxy arp”. This issue is not seen if either HSRP is removed or if “ip proxy arp” is enabled.

Workaround: Clear the subscriber session. After the subscriber is reintroduced, the issue is resolved. You can also configure “ip proxy arp” on the HSRP-configured interface.

- CSCub33470

  Symptoms: Default profiles showing up as custom.

  Conditions: This symptom is observed with a Cisco Catalyst 3000/Catalyst 4000 platform which supports the IP SLA video operation. This issue has no affect on the operation itself.

  Workaround: There is no workaround.

- CSCub34595

  Symptoms: Enabling Dynamic ARP Resolution (DAI) on a VLAN may cause ARP resolution to fail for hosts in other VLANs.

  Conditions: This symptom is seen when enabling DAI on a VLAN.

  Workaround 1: Enable DAI for the failing VLAN using the **ip arp inspection vlan x** command.

  For example:

```
ip arp inspection vlan 30
 int gi 0/10
  ip arp inspection trust
 int gi 0/11
  ip arp inspection trust
```

  Workaround 2: Enable DAI for the failing VLAN using the **ip arp inspection vlan x** command. Configure an ARP ACL to permit traffic for a valid IP source + MAC source pair using the **arp access- list** *acl_name* command. Configure the DAI filter and associate with the ARP ACL using the **ip arp inspection filter** *acl_name* **vlan x** command. Configure the DAI trust on the egress port using the **ip arp inspection trust**.

  For example:

```
ip arp inspection vlan 20
        arp access-list testacl
            permit ip 10.1.1.3 255.255.255.0 mac 01:00:00:0E:0E:0F
        ip arp inspection filter testacl vlan  20
        int gig0/10
            ip arp inspection trust
```

- CSCub34756

  Symptoms: RP crash is observed at rrr_lm_resource_link_ready after performing SSO on the midpoint router on protect LSP.

  Conditions: This symptom is observed when an RP card hosting the TP tunnel midpoint is undergoing the SSO operation. During SSO recovery, the TP fails to recover the TP tunnel midpoint interface (virtual) that is causing it to send a NULL interface to TE for checking its readiness. TE is not checking the NULL pointer condition and accessing the link elements that are causing the crash.

  Workaround: There is no workaround.

- CSCub36356

  Symptoms: Scaling up routes result in huge memory allocations, eventually depleting the SP memory, leading to MALLOC FAIL and subsequent system crash.

Conditions: This symptom occurs in normal conditions.

Workaround: There is no workaround.

- CSCub38559

  Symptoms: When static recursive routes are used in an MVPNv6 environment, multicast traffic loss can occur due to failure to determine the correct RPF interface for a multicast source or rendezvous point.

  Conditions: This symptom occurs if a static route to an IPv6 address at a remote site (remote side of a VPN cloud) resolves via a BGP route, resulting in a failure to install the required MDT alternate next-hop in the recursively referenced BGP route.

  Workaround: Executing "show ipv6 rpf vrf X <address>" for any address within the recursively referenced BGP prefix range will cause installation of the required alternate next-hop.

- CSCub39296

  Symptoms: Unexpected exception to CPU: vector 200, PC = 0x0. Traceback decode is irrelevant.

  Conditions: This symptom is observed on the ES+ series linecards on a Cisco 7600 series router. Symptom is reported on the ES+ console and in the crashinfo file on the ES+ flash disk. It is not reported in the syslog.

  Workaround: There is no workaround.

- CSCub45809

  Symptoms: Cisco IOS configured for Voice over IP may experience stack corruption due to multiple media loops.

  Conditions: This symptom is observed with a special configuration of IP features, along with disabling the recommended **media flow-around** command. This issue is seen with Cisco IOS Release 15.2(2)T.

  Workaround: Apply the **media flow-around** command.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5.4/4.4: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:H/Au:N/C:N/I:N/A:C/E:U/RL:W/RC:C

  CVE ID CVE-2012-5044 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCub48120

  Symptoms: SP crash is observed at oce_to_sw_obj_type on a router reload.

  Conditions: This symptom is seen with a core link flap at the remote end during IP- FRR cutover.

  Workaround: There is no workaround.

- CSCub49985

  Symptoms: MPLS pseudowire ping from the peer to the Cisco ASR 903 fails if the peer is using TTL-based ping.

  Conditions: This symptom occurs when the peer is using TTL-based ping.

  Workaround: There is no workaround.

- CSCub53398

  Symptoms: The router crashes on bootup.

Conditions: This symptom occurs when the router is booted up with a scaled MVPNv6 configuration. This issue is highly dependent on the "back walk" timing and sequence; hence, the probability to encounter the issue is low.

Workaround: Disable power to all DFC modules on reload and bring them up one by one post reload.

- CSCub54261

  Symptoms: In an MLDP + MVPNv6 setup, abnormal RP reload occurs after the deletion and addition of few subinterfaces on the encapsulated PE.

  Conditions: This symptom occurs after deletion and addition of few subinterfaces on the router acting as the encapsulated PE on the access side for a few VRFs running MLCP inband.

  Workaround: There is no workaround.

- CSCub58312

  Symptoms: When IGMP query with source IP address 0.0.0.0 is received on an interface, it is marked as mrouter port for that VLAN.

```
Router#show ip igmp int vlan 1
Vlan1 is up, line protocol is up
  IGMP querying router is 0.0.0.0 <----

Router#sh ip igmp snooping mrouter
vlan            ports
-----+----------------------------------------
   1  Po1,Po8,Router<-----
```

  Conditions: This symptom is observed when IGMP query with source IP address 0.0.0.0 is received.

  Workaround: There is no workaround.

- CSCub68933

  Symptoms: Incorrect MAC learning is observed over pseudowires that are part of HVPLS, causing traffic failure.

  Conditions: This symptom is observed when VPLS autodiscovery is in use, with MPLS over SVI in the core. This issue is also seen with LDP-based VPLS, when split horizon-enabled pseudowires are configured after the non-split horizon-enabled pseudowires.

  Workaround: There is no workaround.

- CSCub70336

  Symptoms: The router can crash when "clear ip bgp *" is done in a large-scale scenario.

  Conditions: This symptom is observed only in a large-scale scenario, with tens of thousands of peers and several VPNv4/v6 prefixes.

  Workaround: "clear ip bgp *" is not a very common operation. Hence, this issue has not been observed by customers. The crash can only happen when "clear ip bgp *" is done. The workaround is not to execute "clear ip bgp *".

- CSCub73177

  Symptoms: RP crash occurs.

  Conditions: This symptom occurs upon router reload

  Workaround: There is no workaround.

- CSCub73787

  Symptoms: The RSP720 may crash if a high rate of traffic is punted to the RP.

Conditions: This symptom occurs on a Cisco 7600 with RSP720. It is specific to a driver used only by the RSP720. Other supervisor models are not affected. The issue is only seen in Cisco IOS Release 15.1(03)S and later releases, because of a code change made to the RSP720 driver.

Workaround: Isolate and stop the traffic being punted to the RP.

- CSCub79035

  Symptoms: Multicast traffic will get route cached on the receiver/decap node resulting in traffic drop and slight increase in RP/SP CPU.

  Conditions: This symptom is seen when multicast traffic flowing over GRE tunnel protected with IPsec and PIM is enabled on the GRE tunnel.

  Workaround: There is no workaround.

- CSCub79590

  Symptoms: The **match user-group** commands do not appear in the running configuration after being configured.

  Configure an inspection type class-map:

```
class-map type inspect TEST
    match protocol tcp
    match user-group cisco
```

  Save the configuration. Try to view the configuration in the running configuration:

```
hostname# show run class-map
building configuration...

Current configuration : 66 bytes
!
class-map type inspect match-all TEST
   match protocol tcp
end
```

  But, view the configuration directly in the class-map:

```
hostname# show class-map type inspect
   Class Map type inspect match-all TEST (id 1)
     Match protocol tcp
     Match user-group cisco
```

  The configuration never shows up in the running configuration, but it is in the class-map configuration. As a note, the functionality exists on the ZBFW, but the configuration does not show up in the running configuration.

  Conditions: This symptom is only observed with the **match user-group** commands.

  Workaround: This issue only affects devices after a reload as the router will read the startup configuration, which will not have the **match user-group** command. As a result, the **match user-group** commands need to be reentered after ever reload.

- CSCub80386

  Symptoms: The following interface configuration should be used:

```
interface Ethernet2/1
description lanethernet1
ipv6 enable
ospfv3 100 network manet
ospfv3 100 ipv6 area 0
```

Dead interval is calculated according to network type; in this case, it is 120s. Issue the **no ospfv3 dead-interval**command on dead interval. Dead interval is set to the default of 40s instead of 120s, which is correct for manet or P2MP interface types.

Conditions: This symptom is an OSPFv3-specific issue (see the configuration example).

Workaround: Configure dead interval explicitly or reapply the network command.

- CSCub80710

  Symptoms: SSL handshake between Cisco VCS and the Cisco ASR fails if the Cisco ASR is running Cisco IOS XE Release 3.7S.

  Conditions: This symptom occurs in a working setup, if the Cisco ASR is upgraded to Cisco IOS XE Release 3.7S, then SSL handshake and subsequently SIP-TLS calls start to fail. If in the same setup, the Cisco ASR is downgraded back to Cisco IOS XE Release 3.5S or Cisco IOS XE Release 3.4.4S, then the calls work (without requiring any additional changes).

  Workaround: There is no workaround.

- CSCub82471

  Symptoms: BFD session flapping occurs or fails to get established on flapping REP ring.

  Conditions: This symptom is observed with the software BFD session or echo mode.

  Workaround: Disable echo mode.

- CSCub86706

  Symptoms: After multiple RP switchover, the router crashes with the “UNIX-EXT-SIGNAL: Segmentation fault(11), Process = BGP HA SSO” error.

  Conditions: This symptom is observed with MVPN with 500 VRFs, when performing multiple switchovers on PE1.

  Workaround: There is no workaround.

- CSCub87579

  Symptoms: Multicast traffic gets forwarded to the wrong tunnel protected with IPsec.

  Conditions: This symptom is observed when Multicast (PIM) is enabled on the GRE tunnel protected with IPsec on the Cisco 7600.

  Workaround: Shut/no shut on the tunnel protected with IPsec resolves the issue.

- CSCub88742

  Symptoms: A crash occurs due to NULL pointer access in a BGP C-Route function.

  Conditions: This symptom is very timing-sensitive and occurs only in a specific sequence of runtime events at a specific timing instance. In this case, it is triggered on a scaled setup when “mpls mldp” is toggled after two SSOs and when each SSO takes a very long time to complete due to HA Bulk Sync failure in IP Multicast that has addresses separately.

  Workaround: There is no workaround.

- CSCub89711

  Symptoms: The **atm** keyword for the **show** command disappears.

  Conditions: This symptom occurs when you do a powered shutdown of the SPA card and bring it back up using the **no** form the previous command.

  Workaround: There is no workaround.

- CSCub91428

  Symptoms: Internal VLAN is not deleted even after waiting for 20 minutes, and the VLAN cannot be reused.

  Conditions: This symptom is seen with any internal VLAN allocated dynamically that is not freed up after 20 minutes in the pending queue.

  Workaround: There is no workaround.

- CSCub91429

  Symptoms: CEF does not get programmed and traffic does not flow across IPv6 VTI tunnels post router reload.

  Conditions: This symptom occurs when reloading the box that has scale IPv6 sVTI IPsec tunnels configured.

  Workaround: Shutdown/no shutdown on the IPv6 tunnels resolves the issue.

- CSCub91546

  Symptoms: Traffic is dropped silently on the VLAN.

  Conditions: This symptom is observed when all the VLANs in the router are used (0 free VLAN). Any new internal VLAN creation will fail, and an appropriate error message is not shown.

  Workaround: There is no workaround.

- CSCub91815

  Symptoms: Certificate validation fails with a valid certificate.

  Conditions: This symptom is observed during DMVPN setup with an empty CRL cache. This issue is usually seen on the responder side, but the initiator can also show this behavior.

  Workaround: There is no known workaround.

- CSCub94438

  Symptoms: Traceback is observed with the following error message:

  ```
  SP-STDBY: pm_get_standby_vlan:Cannot allocate VLAN for IPv6 VPN 0x1E000050 Egress
  multicast VLAN 1019 is use by Tunnel2
  ```

  Conditions: This symptom occurs when applying a scaled MLDP configuration.

  Workaround: There is no workaround.

- CSCub95141

  Symptoms: FP Pending Refs are observed when "crypto map <> local-address loopbackX" is removed from the configuration when the crypto map is applied on a subinterface.

  Conditions: This symptom is observed with the following configuration:

  ```
  crypto map cry local-address Loopback0
  interface GigabitEthernet0/0/0.100 crypto map cry
  interface GigabitEthernet0/0/0.200 crypto map cry
  ```

  Workaround: Remove "crypto map" from the subinterface first and then remove "crypto map <> local-address loopbackX".

- CSCub98385

  Symptoms: CFMoXconnect remote MEPs are not learned.

  Conditions: This symptom is observed with CfmoXconnect on the Cisco ME3600X and TE tunnels in the core. This issue is seen when the core link is mapped to NILE 1.

Workaround: Remove TE tunnels in the core or have the core link on NILE 0.

- CSCuc05570

  Symptoms: The “PM-SP-STDBY-3-INTERNALERROR” error message is seen on Active for the Tunnel Reserved VLAN and the Tunnel Global Reserved VLAN.

  Conditions: This symptom is observed with an HA router with a scale configuration of the MDT Tunnel.

  Workaround: There is no workaround.

- CSCuc06024

  Symptoms: Traffic flowing through EVCs that do not belong to any service group will see incorrect bandwidth values because of wrong bandwidth value programmed on the port-default node.

  Conditions: This symptom is seen when a mixture of flat and HQoS SGs having bandwidth configurations on their policies are applied on PC EVCs. Two mem- links are part of this PC, and default load-balancing is used.

  Workaround: There is no workaround.

- CSCuc10586

  Symptoms: In the Cisco 7600, multicast traffic does not flow in some scenarios. In the case of PIM SM mode, many times, (*,G) is present, but not (S,G) in mroute. In the case of PIM SSM mode, (S,G) is present but still traffic does not flow through.

  Conditions: This symptom is observed only with Cisco IOS Release 15S-based releases.

  Workaround:

  - Either use a different source IP or a different group IP.
  - Reload the module.

- CSCuc10706

  Symptoms: When Cisco IOS XE is configured to use subscriber-service for authorization, it will ignore this configuration for the named list and fall back on the default for subscriber-profile or, if this is not present, on the default authorization method for the network. If none of these default authorization methods are configured, authorization will not take place.

  Conditions: This symptom occurs when a named authorization list is configured.

  Workaround: Set the default authorization list (subscriber-service or network) to use the correct Radius server.

- CSCuc11853

  Symptoms: T1 controller will stay DOWN after switchover.

  Conditions: This symptom is seen when SATOP is configured on T1.

  Workaround: Do a shut and no shut.

- CSCuc13992

  Symptoms: The Cisco IOSd process crashes due to a segmentation fault in the PPP process:

  ```
  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = PPP Events
  ```

  The root cause for the PPP process crash is wrong IPCP option processing inside PPP control packets.

  Conditions: This symptom occurs when the BRAS functionality is configured, which includes ISG and PPPoE session termination.

Workaround: There is no workaround.

- CSCuc14088

  Symptoms: The default class is not being exported with the class option template.

  Conditions: This symptom occurs when class-default is not exported when typing the option c3pl-class-table under the flow exporter.

  Workaround: There is no workaround.

- CSCuc15810

  Symptoms: MVPN over GRE PIM VRF neighbor is not up after SSO.

  Conditions: This symptom is seen when MVPN over GRE PIM VRF neighbor is not up after SSO.

  Workaround: There is no workaround.

- CSCuc28757

  Symptoms: IPv6 HbH Traffic traversing across BD SVIs will not be rate-limited by HbH rate-limiter that is configured.

  Conditions: This symptom is seen when enabling HbH rate-limiter on an NP of ES+ and IPv6 HbH traffic traversing across SVIs part of EVC BD of ES+ interface.

  Workaround: There is no workaround.

- CSCuc29884

  Symptoms: Outage and CPU remain astonishingly high against XDR MCAST process on a scaled HWO BFD testbed.

  Conditions: This symptom is seen after a router reload, when OSPF converge is getting completed, and started 10g traffic through the box.

  Workaround: There is no workaround.

- CSCuc29966

  Symptoms: Traffic loss is seen on switchover over interfaces on TDM IM.

  Conditions: This symptom occurs when the Cisco A900-IMA16D TDM IM crashes upon switchover.

  Workaround: There is no workaround.

- CSCuc31534

  Symptoms: With a primary PW in the down state, if the Xconnect redundancy configuration is removed and added, then switching may remain down and the VC goes down.

  Conditions: This symptom is observed with the following conditions:

  1. The platform supports hot standby (Cisco ASR 903/Cisco 7600/Cisco ASR 901).
  2. PW redundancy with primary down.
  3. Configuration removed + added or added afresh.

  Workaround: Fix the primary PW and then remove/add the configuration.

- CSCuc34088

  Symptoms: The router passes lower traffic levels when you add links to an IMA bundle and perform IM OIR/router reload.

  Conditions: This symptom occurs when you send traffic above the E1 line rate on one link within an IMA bundle and perform IM OIR.

Workaround: Removing and re-applying the IMA interface brings it back up

- CSCuc34574

  Symptoms: A pending-issue-update is seen at SSL CPP CERT on the Cisco ASR 1002, ESP-1000 platform.

  Conditions: This symptom is observed with the following configuration:

  ```
  show platform software object-manager fp active pending-issue-update

  Update identifier: 128
    Object identifier: 117
    Description: SSL CPP CERT AOM show
    Number of retries: 0
    Number of batch begin retries: 0
  ```

  Workaround: There is no workaround.

- CSCuc35935

  Symptoms: Traffic coming in with a particular label might experience drops on ES+.

  Conditions: This symptom is observed with traffic coming in on the ES+ interface with MPLS enabled. This issue is seen when the box has AToM (Scalable mode on the Cisco 7600) configured.

  Workaround: Reset the core facing ES+ module.

- CSCuc36049

  Symptoms: The Cisco ME3600 and Cisco ME 3800 switches crash.

  Conditions: This symptom occurs on triggering POCH LACP fast switchover that is part of G.8032 ring carrying UCAST and MCAST traffic.

  Workaround: There is no workaround.

- CSCuc36522

  Symptoms: The router does not timestamp traffic on port-channel interfaces.

  Conditions: This symptom cccurs when you configure a CFM EVC bridge-domain up MEP on a port-channel.

  Workaround: There is no workaround.

- CSCuc37047

  Symptoms: VSS crashes on reconfiguring “ipv6 unicast-forwarding” multiple times.

  Conditions: This symptom occurs when CTS is configured on an interface and “ipv6 unicast” is toggled multiple times.

  Workaround: There is no workaround.

- CSCuc38446

  Symptoms: The upgrade for Handoff FPGA from version 3000F to 30017 fails.

  Conditions: This symptom is observed when upgrading Handoff FPGA.

  Workaround: There is no workaround.

- CSCuc38851

  Symptoms: DHCP snooped bindings are not restored after an RTR reload.

  Conditions: This symptom might occur when bindings are learnt on Cisco ES20 EVCs.

  Workaround: After the RTR is UP, renew from the agent database by issuing the **renew ip dhcp snooping database** *URL* command.

- CSCuc41369

  Symptoms: Complete traffic loss occurs for V6 mroutes.

  Conditions: This symptom occurs during deletion and addition of VRFs for the MVPNv6 inband signaling configuration.

  Workaround: There is no workaround.

- CSCuc41879

  Symptoms: Multicast traffic for few mroutes gets dropped on the bud node. This issue occurs as sub-LSPs are not created due to LSP IDs getting exhausted.

  Conditions: This symptom occurs after reload, TE-FRR, and churning of mroutes.

  Workaround: There is no workaround.

- CSCuc42002

  Symptoms: The router crashes when configuring the ATM interface.

  Conditions: This symptom is observed with the following sequence:

  1. Move OC3 IM with the ATM configuration to a different bay.
  2. Configure an ATM interface on the new bay.
  3. Cisco IOSd crash is seen due to a segmentation fault.

  Workaround: There is no workaround.

- CSCuc42117

  Symptoms: The router does not include 0xff03 flag leading bits within ppp fragment messages.

  Conditions: This symptom occurs when the router has not negotiated ACFC.

  Workaround: There is no workaround. Most remote devices should ignore this behavior by design, but some devices may display unexpected behavior, such as for IPCP PROTREJ messages.

- CSCuc44555

  Symptoms: Multicast traffic is not forwarded to downstream, even when the groups show up in the group list.

  Conditions: This symptom is observed only when the traffic comes on RPF fail interface, and the downstream port is blocked due to STP or similar protocol.

  Workaround: Disable IGMP snooping.

- CSCuc45115

  Symptoms: EIGRP flapping is seen continuously on the hub. A crash is seen at nhrp_add_static_map.

  Conditions: This symptom is observed after shut/no shut on the tunnel interface, causing a crash at the hub. A related issue is also seen when there is no IPv6 connectivity between the hub and spoke, causing continuous EIGRP flapping on the hub.

  Workaround: There is no known workaround.

- CSCuc45528

  Symptoms: Incremental leaks are seen at :__be_nhrp_recv_error_indication.

  Conditions: This symptom occurs when the NHRP error indication is received on the box. This issue is seen only if CSCub93048 is already present in the image. CSCub93048 is available from Cisco IOS Release 15.3M&T onwards.

Workaround: There is no workaround.

- CSCuc46356

  Symptoms: The router hangs and crashes by WDOG.

  Conditions: This symptom occurs when IPv6 ACL is applied to a port-ch sub-if. The sub-if is deleted followed by deletion of the ACL.

  Workaround: Delete the ACL before deleting the port-ch sub-if.

- CSCuc47399

  Symptoms: IKEv2 STOP Accounting records show wrong counters for packets/octets, when the sessions are locally cleared using “clear crypto sa” or “clear crypto session”.

  Conditions: This symptom is observed with the latest Cisco IOS XE Release 3.8S images when IKEV2-Accouting is enabled. This issue is easily reproducible with a single session, and may be service impacting as STOP Accounting records are usually used for billing purposes.

  Workaround: The STOP records reflect the right counters when the disconnect is through the remote end.

- CSCuc48162

  Symptoms: EVC Xconnect UP MEP is sending CCMs when the remote EFP is shut.

  Conditions: This symptom occurs when EFP is admin down.

  Workaround: There is no workaround.

- CSCuc48211

  Symptoms: Traffic from the Label Edge Router (LER) is dropped at the Label Switch Router (LSR) peer. LER is using a invalid/outdated label, unknown to LSR. This issue can be seen with a regular MPLS connection over a physical interface or with a connection over an MPLS TE tunnel interface. The root cause is that LER is using CEF long-path extension, installed to the prefix by a different routing protocol in the past.

```
TUNNEL-HEADEND/LER#show ip cef 172.25.0.1 internal
172.25.0.0/16, epoch 6, flags rib only nolabel, rib defined all labels, RIB[B],
refcount 5, per-destination sharing
  sources: RIB
  feature space:
   IPRM: 0x00018000
   Broker: linked, distributed at 4th priority
   LFD: 172.25.0.0/16 0 local labels
        contains path extension list
  ifnums:
   TenGigabitEthernet1/0/0(31): 10.10.243.48
   Tunnel11(38)
  path 1F13EC1C, path list 1436FC80, share 1/1, type recursive, for IPv4
  recursive via 10.10.254.3[IPv4:Default], fib 21B2A5CC, 1 terminal fib,
v4:Default:10.10.254.3/32
    path 13A71668, path list 20C50DB0, share 1/1, type attached nexthop, for IPv4
      MPLS short path extensions: MOI flags = 0x1 label 1683
    nexthop 10.10.243.48 TenGigabitEthernet1/0/0 label 1683, adjacency IP adj
out of TenGigabitEthernet1/0/0, addr 95.10.243.48 20BCED00
    path 13A745A8, path list 20C50DB0, share 1/1, type attached nexthop, for IPv4
      MPLS short path extensions: MOI flags = 0x1 label 623
      MPLS long path extensions: MOI flags = 0x1 label 18
    nexthop 10.10.255.130 Tunnel11 label 18, adjacency IP midchain out of
Tunnel11 22923160
  long extension for path if Tunnel11 next hop 10.10.255.130:
    MPLS long path extensions: MOI flags = 0x1 label 18
  long extension for path if Tunnel22 next hop 10.10.255.129:
    MPLS long path extensions: MOI flags = 0x1 label 651
  output chain:
    loadinfo 212F8810, per-session, 2 choices, flags 0083, 4 locks
    flags: Per-session, for-rx-IPv4, 2buckets
    2 hash buckets
      < 0 > label 1683 TAG adj out of TenGigabitEthernet1/0/0, addr
10.10.243.48 20BDC860
      < 1 > label 18 TAG midchain out of Tunnel11 20C92B00 label implicit-null
TAG adj out of TenGigabitEthernet1/0/1, addr 10.10.243.50 20B21440
    Subblocks:
     None

TUNNEL-TAILEND/LSR# sh mpls forwarding-table labels 18
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
TUNNEL-TAILEND#
```

Conditions: This symptom occurs when the prefix is learned by both BGP and IGP, while BGP has lower Administrative Distance, pointing via the MPLS TE tunnel carrying MPLS. This issue is seen once the prefix is installed to RIB by IGP and then by BGP (Reload, BGP flap, etc.); then, the CEF will keep using the IGP/LDPs label without updating it in case of LDP label change.

Workaround: Issue the **clear ip route** *prefix mask* command.

- CSCuc49967

  Symptoms: Router crash points to the "IP SLAs XOS Event Processor" process and decodes point to "ecfm_pal_pd_encap_pak".

  Conditions: This symptom occurs when configuring IPSLA sessions with a Mac-Address that is not present in the CFM CCDB.

  Workaround: This issue is not seen when Mac-Addresses are learned in CCDB.

- CSCuc51692

  Symptoms: The router crashes while enabling L2TP debugs using the **debug l2vpn l2tp error | event** command.

  Conditions: This symptom always occurs on enabling the **debug l2vpn l2tp error | event** command.

  Workaround: The same debugs can be enabled using the alternate command **debug xcl2 error | event**.

- CSCuc52506

  Symptoms: 6PE and 6VPE traffic drops on shutting the ECMP link.

  Conditions: This symptom occurs after configuring the 6PE/6VPE between UPE-2 and UPE-1 with ECMP paths between both nodes and then shutting the ECMP link.

  Workaround: There is no workaround.

- CSCuc53135

  Symptoms: LDP sessions are not established.

  Conditions: This symptom is observed on a router with more than one LDP adjacency to a neighbor. This issue is seen when the TCP session establishment to that neighbor is delayed, and while it is delayed, the adjacency that is the active adjacency times out (no more UDP packets are received), resulting in the TCP listen socket being deleted and not created.

  Workaround: Issue the **clear mpls ldp neighbor *** command.

- CSCuc56259

  Symptoms: A Cisco 3945 that is running 15.2(3)T2 and running as a voice gateway may crash. Just prior to the crash, these messages can be seen:

  ```
  %VOIP_RTP-6-MEDIA_LOOP: The packet is seen traversing the system multiple times
  ```

  and

  ```
  Delivery Ack could not be sent due to lack of buffers.
  ```

  Conditions: This symptom occurs when a media loop is created (which is due to misconfiguration or some other call forward/transfer scenarios).

  Workaround: Check the configurations for any misconfigurations, especially with calls involving CUBE and CUCM.

- CSCuc57130

  Symptoms: Interface configurations do not work post HA switchover.

  Conditions: This symptom occurs after HA switchover and is observed with OC3 IM.

  Workaround: There is no workaround.

- CSCuc59049

  Symptoms: The Cisco ME3800x crashinfo files may be incomplete.

  Conditions: This symptom occurs when a crashinfo file is created when a crash occurs.

  Workaround: Gather console logs and syslogs to help troubleshoot crashes.

- CSCuc59105

  Symptoms: The switch may crash when issuing “show platform qos policer cpu x x”.

  Conditions: This symptom occurs only when issuing “show platform qos policer cpu x x” through an SSH session with AAA configured.

  Workaround: Execute the command through Telnet or the console.

- CSCuc64719

  Symptoms: A Cisco ME 3600X HSRP failover is seen in VPLS.

  Conditions: This symptom occurs when HSRP state changes from active to standby. The MAC address on the active router is not flushed.

  Workaround: Clear the MAC table on the HSRP active router.

- CSCuc66895

  Symptoms: Layer 2 traffic loop seen in REP topology for a transient time, when the Cisco ASR 903 which is a part of the REP ring is reloaded.

  Conditions: This symptom is observed when the Cisco ASR 903 is part of an REP ring, and the box is reloaded with saved REP configurations.

  Workaround: Traffic loop is transient, once REP convergence looping is stopped.

- CSCuc67687

  Symptoms: With a rare combination, and VRF-related RG configurations, the router may crash following the configuration commands.

  Conditions: This symptom is observed with the following configuration:

  ```
  R1-13RU(config-if)#ip vrf forwarding b2b-vrf
  % Interface GigabitEthernet0/1/0 IPv4 disabled and address(es) removed due to
  ```

```
enabling VRF b2b-vrf
% Interface GigabitEthernet0/1/0 virtual IP address <ip> removed due to VRF change
% Zone security Z1 is removed due to VRF config change on interface
GigabitEthernet0/1/0

R1-13RU(config-if)#ip address <ip> <mask>
R1-13RU(config-if)#zone-member security Z1
R1-13RU(config-if)#redundancy group 1 ip <ip> exc dec 50
```

Workaround: There is no known workaround.

- CSCuc68246

  Symptoms: The standby IOMD crashes on booting up the standby RSP.

  Conditions: This symptom occurs when booting up the standby RSP with a configuration that is already present.

  Workaround: Boot up the standby without any configurations and start configuration once the standby has reached STANDBY_HOT state.

- CSCuc71706

  Symptoms: Execution of the **show run** command and other commands such as **copy run start** and **show access-list** cause the router to stop for a few minutes before completing.

  Conditions: This symptom is observed with Cisco ISR G2 routers. This issue is seen only with IPV6 configured and used.

  Workaround: There is no workaround.

- CSCuc72244

  Symptoms: On the Cisco 7609, both sides running Cisco IOS Release SRE4 SIP-400 with SPA-2X1GE-V2 configured with “negotiation Auto” and changed to “no negotiation auto”. The GE interface of the router is operating in half-duplex mode after falling back. The interface is operating in half-duplex instead of the expected (nonconfigurable) full-duplex.

  Conditions: This symptom does not occur under any specific conditions. This issue is observed due to a timing constraint upon updating the duplex state.

  The steps to reproduce are as follows:

  1. The interface in Router A is configured to “negotiation auto” with no change in duplex state on both sides.
  2. The interface in Router B is configured to “negotiation auto” with no change in duplex state on both sides.
  3. The interface in Router A is configured to “no negotiation auto”. The duplex state for both interfaces is changed to half-duplex.
  4. The interface in Router B is configured to “no negotiation auto”. The interface duplex state for Router B is changed to full-duplex. But, the Router A interface remains in half-duplex.

  Workaround: There is no workaround.

- CSCuc72594

  The Cisco IOS Software implementation of the IP Service Level Agreement (IP SLA) feature contains a vulnerability in the validation of IP SLA packets that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

  Cisco has released free software updates that address this vulnerability. Mitigations for this vulnerability are available.

  This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-ipsla

Note: The March 27, 2013, Cisco IOS Software Security Advisory bundled publication includes seven Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the March 2013 bundled publication.

Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar13.html

- CSCuc76670

  Symptoms: 2X1GE-SYNCE (metronome) SPA does not boot on a 2RU (Cisco ASR 1002).

  Conditions: This symptom is observed with Cisco IOS XE Release 3.7S onwards, when metronome SPA (2X1GE-SYNCE) fails to boot on a 2RU. An error message indicating that the SPA is not supported is displayed on the RP console.

  Workaround: There is no workaround.

- CSCuc77283

  Symptoms: Upon reload or OIR, the CFM MEP configuration on an xconnect EFP is removed and cannot be reconfigured.

  Conditions: This symptom is observed with a CFM MEP on xconnect service instance. This issue is seen when reload or OIR is performed.

  Workaround: Remove the domain configuration.

- CSCuc77704

  Symptoms: The GETVPN/GDOI Secondary Cooperative Key Server (COOP-KS) does not download the policy (that is, when the **show crypto gdoi ks policy** command is issued on the Secondary COOP-KS and the command output shows that no policy is downloaded) and Group Members (GMs) registering to the Secondary COOP-KS fail to register without any warning/error message.

  Conditions: This symptom is observed when the GETVPN/GDOI group (with COOP configured) has an IPsec profile configured with one of the following transforms in its transform-set:

  - esp-sha256-hmac
  - esp-sha384-hmac
  - esp-sha512-hmac

  Workaround: Use esp-sha-hmac as the authentication transform instead.

- CSCuc79161

  Symptoms: Memory leak is observed.

  Conditions: This symptom occurs after flapping the interface, keeping the setup idle, and executing "clear xconnect".

  Workaround: There is no workaround.

  Further Problem Description: The PI front-end pseudoport is not deleted when the xconnect is removed, which causes the memory leak. This issue occurs because PD returns BDOMAIN_PP_FAILED to PI when pp_engine_context is a NULL pointer.

- CSCuc79923

  Symptoms: On a Cisco 7600 running Cisco IOS Release 15.2(4)S1, packets from FWSM are dropped when the servicemodule session is enabled. Ping fails for the VLAN interface on the FWSM module from the supervisor. The ARP entry is incomplete on the Cisco 7600.

  Conditions: This symptom is observed with the following conditions:

  - This issue is seen on the Cisco 7600 with FWSM and SUP-720-3B running Cisco IOS Release 15.2(4)S1.
  - The FWSM is in Crossbar mode.
  - The system is in "distributed" egress SPAN replication mode.

  This issue is not seen with Cisco IOS Release 12.2(33)SRE7.

  Workaround:

  - Disable the servicemodule session.
  - Change the fabric switching mode to bus.
  - Change SPAN egress replication mode to "centralized".

- CSCuc82551

  Symptoms: A Cisco ASR 1001 running Cisco IOS XE Release 3.6.2S or Cisco IOS XE Release 3.7.1S crashes with SNMP traffic.

  Conditions: This symptom is observed with SNMP polling with an IP SLA configuration.

  The crash signature is as follows:

  ```
  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = SNMP ENGINE
  ```

  Workaround: Remove the SNMP configuration from the router or schedule the probe before polling via SNMP.

- CSCuc91582

  Symptoms: Adding EFP to Bridge-Domain fails and errors are seen when reloading with Cisco IOS XE Release 3.7.1a.

  Conditions: This symptom is observed when reloading the Cisco ASR 903 with Cisco IOS XE Release 3.7.1a, when EFP and PW are in the same Bridge-Domain.

  Workaround: Post reload, remove the EFP configurations, and configure PW first and then EFP.

- CSCuc97711

  Symptoms: After SSO, traffic on the P2P-GRE tunnel within an MVPN may be affected.

  Conditions: This symptom is observed with Cisco IOS Release SREx- and RLSx-based releases.

  Workaround: Shut/no shut the P2P tunnel interface.

- CSCuc98226

  Symptoms: When a PC is moved between two VLAN ports (on one port, ISG is enabled, and the other is non-ISG) several times by its LAN cable connection on the L2SW that is connected to the Cisco ASR 1000 router, the PC becomes unable to acquire an IP address from DHCP on the router. At that time, an incorrect interface is shown in "show ip dhcp binding".

  Conditions: This symptom is observed with Cisco IOS Release 15.2(4)S1.

  Workaround: There is no workaround.

- CSCuc98590

  Symptoms: The router can crash on removal of the boundary clock (BC). configuration.

  Conditions: This symptom is observed upon removal of the BC configuration. This issue is seen very rarely, and there is no other specific trigger.

  Workaround: There is no workaround. The chances of encountering this issue have been found to be remote as it is seen rarely.

- CSCud03877

  Symptoms: After volume rekey, the IPsec PD flow sets both the hard and soft limit of the traffic limit to 0.

  Conditions: This symptom is observed when the volume rekey is set to 0.

  Workaround: Clear crypto session to recover the volume rekey value.

- CSCud07856

  Symptoms: SP crashes at “cfib_update_ipfrr_lbl_ref_count”.

  Conditions: This symptom is observed with a scaled IP-FRR configuration.

  Workaround: Remove the IP-FRR configuration.

- CSCud16693

  Symptoms: The Cisco ME3600X/ME3800X switch crashes as soon as you apply policy-map referencing table-map.

  Conditions: This symptom occurs when applying a service policy which has an unsupported combination of police action with table-map and without table-map.

  Workaround: Configure a service policy which does not have the combination of police action with table-map and without table-map.

- CSCud17934

  Symptoms: PW redundancy on the Cisco 7600 does not work when the primary VC goes down and the backup VC takes over, and CE to CE communication is broken.

  Conditions: This symptom is observed with the following conditions:

  - The MPLS facing LC is WS-X6704-10GE.
  - The CE facing LC is ES+.

  Workaround: Use another HW on the MPLS core.

- CSCud19230

  Symptoms: ES+ line card reload occurs with the following error messages:

  ```
  %PM_SCP-SP-1-LCP_FW_ERR: System resetting module 2 to recover from error:
  x40g_iofpga_interrupt_handler: LINKFPGA IOFPGA IO Bus Err val: 4214784 Bus
  Error Add:332 Bus Err
  data: 0

  %OIR-SP-3-PWRCYCLE: Card in module 2, is being power-cycled Off (Module Reset
  due to exception or
  user request)

  %C7600_PWR-SP-4-DISABLED: power to module in slot 2 set Off (Module Reset due
  to exception or user
  request)
  ```

  Conditions: This symptom is observed with the ES+ line card.

Workaround: There is no workaround.

- CSCud19257

  Symptoms: NAT CLIs expose the **vrf** keyword on the Cisco 7600, which is not supported.

  Conditions: This symptom is observed with a NAT configuration.

  Workaround: Do not use the **vrf** keyword for NATing on the Cisco 7600.

- CSCud22601

  Symptoms: MPLS-TP tunnels stay down.

  Conditions: This symptom occurs when the standby boots up after the TP configuration is done and SSO is performed. This issue is seen once in 100 iterations.

  Workaround: Shut/no shut the MPLS-TP tunnel. A nonintrusive workaround is to flap the protect LSP (by reconfiguring or by physical interface flap).

- CSCud24084

  Symptoms: Performing a default MDT toggling on a VRF results in the encapsulation tunnel adjacency's MTU being set to a lower MTU.

  Conditions: This symptom is observed with Cisco IOS XE Release 3.7S (Cisco IOS Release 15.2(4)S) and later releases when the mdt default <> is toggled on a VRF.

  Workaround: Delete and add the affected VRF.

  Further Problem Description: Software adjacency does not updated with the correct MTU.

- CSCud26339

  Symptoms: Changing policy-map parameters triggers a Cisco IOSd crash.

  Conditions: This symptom is observed when the policy-map is attached to a service instance on the Cisco ASR 903.

  Workaround: Remove the policy-map from the target and then make the changes.

- CSCud31012

  Symptoms: MVPNv6 does not work in the Cisco IOS XE Release 3.7S image.

  Conditions: This symptom is observed only with the IP services image.

  Workaround: Use the enterprise image.

- CSCud33028

  Symptoms: Segmentation crash occurs.

  Conditions: This symptom occurs upon executing "config replace".

  Workaround: There is no workaround.

- CSCud38004

  Symptoms: RPF failure is not supported for EFP/EVC BD. As a result, multicast traffic is not forwarded.

  Conditions: This symptom is observed in the following scenario:

```
Source------N1------N2
            \        /
              \     /
               Switch
                 |
                 Rx
```

Considering the above dual-home scenario, this symptom is observed when the below conditions are true:

1. N2 acts as the DR.
2. One of the dual-home links to the receiver (N2-Switch) is down.
3. EVC is configured between N1 and N2.

Workaround:

1. Move the DR to N1.
2. Use SVI between N1 and N2.

- CSCud45445

  Symptoms:

  Scenario 1: Y.1731PM does not work with “rewrite ingress tag pop 1 symmetric” at the core facing interface.

  Scenario 2: Y.1731Pm does not work on the Q-in-Q configured interface.

  Conditions: This symptom is observed with the following conditions:

  – When the core facing interface is configured as “rewrite ingress tag pop 1 symmetric”, as follows.

```
interface GigabitEthernet0/9

 switchport trunk allowed vlan none

 switchport mode trunk

 service instance 1 ethernet test

  encapsulation dot1q 151

  rewrite ingress tag pop 1 symmetric

  bridge-domain 151

 !

end
```

  – In the q-in-q configured interface, as follows.

```
interface GigabitEthernet0/1

 switchport trunk allowed vlan none

 switchport mode trunk
```

```
service instance 1 ethernet test

 encapsulation dot1q 151 second-dot1q 110

 bridge-domain 151

 cfm mep domain 17 mpid 555

  cos 1

!
```

Workaround: There is no workaround.

- CSCud48005

  Symptoms: The router crashes on applying the QoS policy-map with a classification based on ACL on the main interface.

  Conditions: This symptom is observed when you apply the policy-map on the main interface.

  Workaround: There is no workaround.

- CSCud50514

  Symptoms: DEJAVU check fails for multicast traffic for the EVC BD interface.

  Conditions: This symptom is a regression caused by bug CSCud38004. Once CSCud38004 has the complete fix, this issue will not be seen.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 15.2(4)S1

Cisco IOS Release 15.2(4)S1 is a rebuild release for Cisco IOS Release 15.2(4)S. The caveat in this section is open in Cisco IOS Release 15.2(4)S1. This section describes only select open caveats.

- CSCtx31177

  Symptoms: RP crash is observed on avl search.

  Conditions: This crash is observed on configuration of rich system with high load. Sometimes the crash is happening when system is not being used.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.2(4)S1

Cisco IOS Release 15.2(4)S1 is a rebuild release for Cisco IOS Release 15.2(4)S. The caveats in this section are resolved in Cisco IOS Release 15.2(4)S1 but may be open in previous Cisco IOS releases.

- CSCsq83006

  Symptoms: When some port-channels go down at the same time on a router, it can cause EIGRP SIA errors.

Conditions: The symptom occurs with full mesh four routers which are connected via port-channels. Additionally, it occurs with over five routers which are connected via a partial mesh port-channel.

Workaround: Use the port-channel interface settings below:

```
(config)# interface port-channel <port-channel interface number>
  (config-if)# bandwidth <bandwidth value>
  (config-if)# delay <delay value>
```

Further Problem Description: If a test is done with a physical interface, not a port-channel, this issue is not seen.

- CSCtg47129

  The Cisco IOS Software implementation of the virtual routing and forwarding (VRF) aware network address translation (NAT) feature contains a vulnerability when translating IP packets that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are not available.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-nat

  Note: The March 27, 2013, Cisco IOS Software Security Advisory bundled publication includes seven Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the March 2013 bundled publication.

  Individual publication links are in “Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication” at the following link:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar13.html

- CSCti62247

  Symptoms: If a packet is sent to a null interface, a Cisco ASR 1000 router will not respond with an ICMP packet.

  Conditions: This symptom is seen when a prefix is routed to Null0 interface.

  Workaround: There is no workaround.

- CSCto87436

  Symptoms: A Cisco device that is running Cisco IOS may crash due to a watchdog timeout with the following error messages:

```
%SYS-3-CPUHOG: Task is running for (126004)msecs, more than (2000)msecs
(30/1),process = SSH Process.
-Traceback= 0x63D827CCz 0x6496A670z 0x649774CCz 0x649776A0z 0x6497777Cz
0x6496BCFCz 0x6496BEA4z 0x6496BFF8z 0x61E122A0z 0x61DFC6CCz 0x61DFCF94z
0x61DFF270z 0x61DFC5F8z 0x61E980E0z 0x61E984ACz 0x61E3DF6Cz
%SYS-3-CPUHOG: Task is running for (128004)msecs, more than (2000)msecs
(31/1),process = SSH Process.
-Traceback= 0x63D7AA5Cz 0x62A47F68z 0x62A48500z 0x62A45F9Cz 0x649774E8z
0x649776A0z 0x6497777Cz 0x6496BCFCz 0x6496BEA4z 0x6496BFF8z 0x61E122A0z
0x61DFC6CCz 0x61DFCF94z 0x61DFF270z 0x61DFC5F8z 0x61E980E0z
 %SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = SSH Process.
```

  Reason for the crash is that we are not handling the error condition properly in the call flow.

Conditions: This symptom occurs mainly due to slow response from the client. This can occur because of the below mentioned scenario. Condition that can leads to this:

Client is out of its window, and we expect window adjust message:

1. Foreign reset happens to the connection.
2. Idle timeout.
3. Timer timeout.
4. Other error to the connection.

We failed to handle this kind of error properly and we loop again and again expecting that message will come from the client even though we set the tcp->pid to No_PROCESS.

Workaround: There is no workaround. Use a stable connection and use a noise free fast underlying physical connection between the two devices.

- CSCtq17444

  Symptoms: A Cisco AS5400 crashes when performing a trunk call.

  Conditions: The following conditions are observed:

  - Affected Cisco IOS Release: 15.1(3)T.
  - Affected platforms: routers acting as voice gateway for H.323.

  Workaround: There is no workaround.

- CSCtr45287

  Symptoms: Router crashes in a scale DVTI scenario.

  Conditions: The symptom is observed when the IPsec tunnel count reaches around 2500.

  Workaround: Use fewer tunnels or use a different platform.

- CSCts54641

  Symptoms: Various small, medium, or big VB chunk leaks are seen when polling EIGRP MIB or during SSO.

  Conditions: This symptom is observed when MIBs are being polled or SSO is done.

  Workaround: There is no workaround.

- CSCtw88689

  Symptoms: A crash is seen while applying the policy map with more than 16 classes with the Cisco 3900e platform.

  Conditions: This symptom occurs when applying the policy map with more than 16 classes.

  Workaround: There is no workaround.

- CSCtx23593

  Symptoms: Some virtual circuit (VC) information is missing in the Simple Network Management Protocol (SNMP) MIB object cAal5VccEntry from the output of the **snmpwal** command, but not in the router configuration command. For example, The ATM VCs 4/0.120 exist on the router but are missing in the MIB.

  Conditions: This symptom is observed on a Cisco 7204VXR (NPE-G2) router that is running Cisco IOS Release 12.2(33)SRE5 (c7200p-advipservicesk9-mz.122-33.SRE5.bin) image in the customer network. This issue may also occur in other releases.

This issue typically occurs over a period of time due to create/delete of subinterfaces. It also occurs if the customer uses the **snmp ifmib ifIndex Persist** command, which retains ifIndicies assigned to the @~@subinterfaces across router reload.

Workaround: There can be two workarounds where there is no fix present in the Cisco IOS code for this bug.

Workaround 1:

- Enter the **show atm vc** privileged EXEC command on the same device to obtain a complete list of all the VCs. Or,
- Do the SNMPWALK suffixing the ifIndex of the interface to get the value.

```
$ snmpwalk -v 2c -c <community> <ip address> 1.3.6.1.2.1.2.2.1.2 | grep
"4/0.120"
IF-MIB::ifDescr.253 = STRING: ATM4/0.120-atm subif
IF-MIB::ifDescr.254 = STRING: ATM4/0.120-aal5 layer

$  snmpwalk -v 2c -c <community> <ip address> 1.3.6.1.4.1.9.9.66.1.1.1.1.3 |
grep 9.9.66.1.1.1.1.3.254 ===> Got no entry of ifindex here in complete
snmpwalk
$
$ snmpwalk -v 2c -c <community> <ip address> 1.3.6.1.4.1.9.9.66.1.1.1.1.3.254
```

Doing the SNMPWALK suffixing the ifindex and getting the value can be one workaround. SNMPv2-SMI::enterprises.9.9.66.1.1.1.1.3.254.200.106 = Counter32: 403633041

Workaround 2:

1. Under configuration mode: no snmp ifmib ifIndex Persist.
2. On all the ATM main interfaces: no snmp ifindex persist.
3. Save the configuration: copy running start.
4. Reload the box: reload. Reapply the persist configurations.
5. Configure in configuration mode: snmp ifmib ifIndex Persist.
6. Under the ATM main interface: snmp ifindex persist.

After this workaround, the problem may reappear over a period of time, but chances are very less.

The workaround/fix which needs to be enabled where the code fix is present in the Cisco IOS code for this bug.

Since this will go over all the possible ifIndicies, it will take more CPU cycles, causing some delay. The below global CLI can be used to enable/disable the fix based on the need.

CLI: snmp-server enable traps atm snmp-walk-serial

- CSCtx54882

  Symptoms: A Cisco router may crash due to Bus error crash at voip_rtp_is_media_service_pak.

  Conditions: This symptom has been observed on a Cisco router running Cisco IOS Release 15.1(4)M2.

  Workaround: There is no known workaround.

- CSCtx80535

  Symptoms: DHCP pool that is configured for ODAP assigns the same IP to multiple sessions.

Conditions: PPP users receive pool via Radius. The pool is defined on the Cisco 10000 series router to use ODAP. ODAP is receiving the subnets from Radius correctly, and assigns IPs to PPP sessions, but sometimes two users end up having the same IP address.

Workaround: Clear both sessions sharing the same IP.

- CSCtx89615

  Symptoms: Classification on the switchport interface will not work on reload of the box.

  Conditions: This symptom occurs when reloading the box.

  Workaround: Remove the policy-map and apply it back.

- CSCty01237

  Symptoms: The router logs show:

  ```
  <timestamp> %OER_BR-5-NOTICE: Prefix Learning STARTED CMD: 'show run' <timestamp>
  ```

  This is followed by the router crashing.

  Conditions: This issue is seen under the following conditions:

  1. Configure PfR with a learn-list using a prefix-list as a filter and enable learn.
  2. Use a configuration tool, script or NMS that periodically executes **show run** on the MC over HTTP or some other means.

  Workaround 1: If you use PfR learn-list feature, do not execute **show run** periodically.

  Workaround 2: If you use a monitoring tool that executes **show run** periodically, avoid using a learn-list configuration in PfR.

- CSCty07558

  Symptoms: DHCPv6 packets are dropped on a Cisco 7600 switch. For example, they are not flooded.

  Conditions: This symptom is observed when there is no IPv6 address on an SVI or if l2 VLAN has SVI in shut state (default existence after a new ACL feature).

  Workaround: Two possible workarounds which essentially serve as the fix due to the limitations they impose:

  1. When working with a pure L2 VLAN, remove ttl rate limiter (selected as default rate limiter on Cisco7600, but not on other boxes) using “no mls rate-limit all ttl-failure”.
  2. If the design permits and TTL rate limiter is necessary, put a dummy IPv6 address on the SVI or simply configure IPv6 enable on the SVI.

- CSCty12312

  Symptoms: Multilink member links move to an up/down state and remain in this condition.

  Conditions: This symptom occurs after multilink traffic stops flowing.

  Workaround: Remove and restore the multilink configuration.

- CSCty30952

  Symptoms: QoS policy-map gets rejected on shut/no shut of the interface or when the router reloads.

  Conditions: This symptom occurs when the router reloads or shut/no shut of the interface.

  Workaround: Apply the policy-map back.

- CSCty35726

  Symptoms: The following is displayed on the logs:

```
InterOp:Cube-NavTel : LTI: Video Xcode Call with plain Audio FAILS
```

Conditions: This symptom is seen when video Xcode call with plain audio fails.

Workaround: There is no workaround.

- CSCty41336

  Symptoms: Forward-alarm ais does not work on CESoPSN circuits.

  Conditions: This symptom occurs when you create SAToP and CESoPSN circuits and configure "forward-alarm ais".

  Workaround: There is no workaround.

- CSCty59891

  Symptoms: On the node where shut/no shut is issued, traffic does not reach IPsec VSPA, which is supposed to get encrypted.

  Conditions: This symptom is observed when issuing shut/no shut on the GRE tunnel protected with IPsec and QoS configured on this IPsec tunnel.

  Workaround: Remove and attach "tunnel protection ipsec profile".

- CSCty64216

  Symptoms: On unconfiguring a scaled ACL, the router crashes.

  Conditions: This symptom is observed when an ACL having 1000 ACEs or more is unconfigured.

  Workaround: There is no workaround.

- CSCty64255

  Symptoms: BGP L3VPN dynamic route leaking feature from the VRF to global export feature, the prefix-limit is incorrect upon soft clear, or new prefix added, or prefix deleted.

  Conditions: This symptom is observed when VRF to global export is enabled, and prefix-limit is configured.

  Workaround: BGP hard clear.

- CSCty65189

  Symptoms: Incoming register packets are dropped at the RP when zone-based firewall (ZBFW) is configured on the RP.

  Conditions: The symptom is observed when ZBFW is configured.

  Workaround: There is no workaround.

- CSCty79284

  Symptoms: Source connected to dual home node is not forwarded to receivers in PIM SSM mode. The issue was due to the PIM joins not reaching the source node.

  Conditions: This symptom occurs with dual home node with PIM SSM with traffic source.

  Workaround: Add static group to forward the traffic to next hop router.

- CSCty80541

  Symptoms: Having EVC BD, with split-horizon group as 0 or 2 as CE-facing, drops the traffic over VPLS core pseudowire (split-horizon enabled).

  Conditions: This symptom is observed when CE-facing interface is EVC BD with split-horizon group as 0 or 2. For split-horizon group 1, traffic flows fine. The issue with CE-facing as group 0, cannot be fixed because of hardware limitation.

  Workaround: There is no workaround.

- CSCty86039

  Symptoms: Shut down the physical interface of tunnel source interface. The router crashes with traffic going through some of the tunnels.

  Conditions: This symptom is seen with tunnel interface with QoS policy installed.

  Workaround: There is no workaround.

- CSCty89224

  Symptoms: A Cisco IOS router may crash under certain circumstances when receiving a mvpnv6 update.

  Conditions: This symptom is observed when receiving mvpnv6 update.

  Workaround: There is no workaround.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.8/5.6: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:S/C:N/I:N/A:C/E:F/RL:OF/RC:C CVE ID CVE-2012-3895 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtz00430

  Symptoms: The static route is removed from the routing table.

  Conditions: This symptom is observed when pulling out and replacing a connection to the management interface.

  Workaround 1: Default the management interface and reconfigure IP.

  Workaround 2: Do a shut and no shut on the management interface through the CLI.

- CSCtz07419

  Symptoms: The PTP session is PHASE_ALIGNED for a day, and then the PTP master crashes.

  Conditions: This symptom is seen during longevity run.

  Workaround: There is no workaround.

- CSCtz12525

  Symptoms: Accounting stop is sent without Acct-Input-Packets Acct-Output-Packets Acct-Input-Octets Acct-Output-Octets when service stop is performed.

  Conditions: This symptom is observed when service stop is issued for the prepaid service.

  Workaround: There is no workaround.

- CSCtz16798

  Symptoms: On configuring "ip pim snooping" on a L3 MCAST box, crash is observed.

  Conditions: This symptom when L2 specific functionality is enabled on a L3 box. This is more of an unsupported and undesired configuration as the L3 box is capable of building the MCAST database on its own.

  Workaround: Do not configure "ip pim snooping" on L3 Cisco ME 3600X and ME 3800X boxes.

- CSCtz17977

  Symptoms: Not able to ping HSRP VIP address over Routed VPLS.

Conditions: This is seen when two Cisco ME 3600s (me360x-universalk9-mz.152-2.S.bin) are connected together via VPLS. The Cisco ME 3600X-1 is configured with HSRP under VLAN50, and the R1 is able to ping. The R2 and Cisco ME 3600X-2 are not able to ping the VIP (HSRP) address. The R2 and Cisco ME 3600X-2 are able to ping physically the IP address of R1 and the Cisco ME 3600X-1. We do have ARP entry for the VIP address on all routers.

-----VPLS--------- R1(fa0/1)--------Vlan50 ME3600X-1-0/2--------Ten-------0/2-ME3600X-2-Vlan50-- -----fa0/1-R2

Workaround: There is no workaround.

- CSCtz26683

  Symptoms: An unsupported "ip verify unicast ..." configuration applied to an interface may still be shown in **show running-config** after being rejected. Output similar to the following will appear when applying the configuration:

  ```
  % ip verify configuration not supported on interface Tu100
    - verification not supported by hardware
  % ip verify configuration not supported on interface Tu100
    - verification not supported by hardware
  %Restoring the original configuration failed on Tunnel100 - Interface Support
  Failure
  ```

  Conditions: This occurs when there is no prior "ip verify unicast ..." configuration on the interface and when the interface and/or platform do not support the given RPF configuration.

  Workaround: In some cases it may be possible to get back to the previous configuration by using a **no** form of the command. In other cases, it will be necessary to reload the device without saving the configuration, or editing the configuration manually if already saved.

- CSCtz37164

  Symptoms: The requests to the RADIUS server are retransmitted even though the session no longer exists, causing unnecessary traffic to RADIUS, and RADIUS getting requests for an invalid session.

  Conditions: This symptom occurs when the RADIUS server is unreachable and the CPE times out the session.

  Workaround: The fix is currently being worked upon. This issue can be seen as per the conditions mentioned above. This issue can be avoided by making sure that the RADIUS server is always reachable.

- CSCtz43626

  Symptoms: Minor or major temperature alarms reported in the syslog:

  ```
  %C7600_ENV-SP-4-MINORTEMPALARM: module 2 aux-1 temperature crossed threshold
  #1(=60C). It has exceeded normal operating temperature range.
  %C7600_ENV-SP-4-MINORTEMPALARM: EARL 2/0 outlet temperature crossed threshold
  #1(=60C). It has exceeded normal operating temperature range.
  ```

  Conditions: This symptom is observed on ES+ series line cards of Cisco 7600 series routers. Specifically, reported temperature will be far off from reading of other sensors on the line card.

  Workaround: There is no workaround.

  Further Problem Description: This is en enhancement in temperature reading on ES+ line cards of Cisco 7600 series routers. Reading of any temperature sensor is compared to its adjacent sensors. If the reading deviates too much from adjacent sensors, this reading is ignored. This enhancement is eliminating the single point of failure, by which one faulty sensor can trigger an environmental alarm. Nature of heat dissipation and the number and placement of temperature sensors on ES+ line cards allow for such logic to be introduced.

- CSCtz44989

  Symptoms: A EIGRP IPv6 route redistributed to BGP VRF green is not exported to VRF RED. Extranet case is broken for IPv6 redistributed routes.

  Conditions: The issue is seen with IPv6 link-local nexthop. When the EIGRP route is redistributed to BGP VRF, it clears the nexthop information (it become 0.0.0.0). Now this route becomes invalid and BGP is not able to export to another VRF.

  Workaround: There is no workaround.

- CSCtz48338

  Symptoms: A router may crash with setup with configuration of BGP L3VPN VRF to global export, NSR, and large scale, hard clear or link flap.

  Conditions: This symptom is seen under the following conditions:

  1. BGP L3VPN VRF to global import
  2. NSR
  3. Large scale

  Workaround: There is no workaround.

- CSCtz50204

  Symptoms: A crash is observed on EzVPN Server if VRF configuration under the ISAKMP profile is modified.

  Conditions: The crash is observed only if there are active sessions at the time of configuration change.

  Workaround: Prior to applying a configuration change, clear the sessions.

- CSCtz58941

  Symptoms: The router crashes when users execute the **show ip route XXXX** command.

  Conditions: This symptom is observed during the display of the **show ip route XXXX**, when the next-hops of “XXXX” networks are removed.

  Workaround: The **show ip route XXXX** command (without “XXXX”) does not have the problem.

- CSCtz61556

  Symptoms: ATM local switching segments do not come up after changing encap on both interfaces.

  Conditions: This symptom is seen with ATM VC local switching. If the encap on both the ATM VC segments are changed, the segments remain in DOWN state.

  Workaround: There is no workaround.

- CSCtz71084

  Symptoms: When the prefix from CE is lost, the related route that was advertised as best-external to RR by PE does not get withdrawn. Even though the BGP table gets updated correctly at PE, RIB still has a stale route.

  Conditions: This symptom is observed with a topology like shown below, where CE0 and CE1 advertise the same prefixes:

  CE0------------------PE0---------------------RR | | | | CE1------------------PE1----------------------|

  Best-external is configured at PEs. PE0 prefers the path via PE1 and chooses it as its best path and advertises its eBGP path as the best-external path to RR. RR has two routes to reach the prefix, one via PE0 and the other via PE1. This issue occurs when CE0 loses the route; therefore, PE0 loses its best-external path and it has to withdraw, but this does not happen.

This issue does not occur if the interface between PE0-CE0 is shut from either side. Instead, the following command should be issued to stop CE0 from advertising the prefix: no network x.x.x.x mask y.y.y.y

Even though the trigger has SOO, it is not necessary for the repro. This same issue can be observed by PIC (stale backup path at RIB under the similar scenario), diverse-path, and inter-cluster best-external, and is day 1 issue with all.

Workaround: Hard clear.

- CSCtz83221

  Symptoms: Active or standby route processor crashes.

  Conditions: This symptom can be seen during the configuration or removal of ATM virtual circuits.

  Workaround: There is no workaround.

- CSCtz92606

  Symptoms: MFR memberlinks-T1 serial interfaces created under a CHOC12 controller, do not get decoupled from MFR even after the MFR bundle interface is deleted. Once the MFR bundle interface is reconfigured, the memberlinks do not appear under it.

  Conditions: This symptom is seen with MFR with memberlinks as T1 serials from CHOC12 sonet controller.

  Workaround: Unconfigure and reconfigure the “encap frame-relay MFRx” under each memberlink after reconfiguring the MFR bundle interface.

- CSCtz94902

  Symptoms: Memory allocation failure is seen when attaching to SIP-40 using a web browser.

  Conditions: This symptom is seen on the line card with a memory allocation failure.

  Workaround: Reset the line card.

- CSCtz96504

  Symptoms: Some of the backup VCs are down after SSO.

  Conditions: This symptom happens only on scale scenario where 500 primary and 500 backup VCs were created.

  Workaround: These backup VCs can be brought to SB state by issuing the **clear xconnect peerid** p*eerid of the PW* **vcid** *vcid* command. Although it is not usually recommended, it is the only way to recover.

- CSCua06598

  Symptoms: Router may crash with breakpoint exception.

  Conditions: The symptom is observed when SNMP polls IPv6 MIB inetCidrRouteEntry and there is a locally-sourced BGP route installed in IPv6 RIB.

  Workaround: Disable SNMP IPv6 polling.

- CSCua06629

  Symptoms: The **sh ipv6 mobile pmipv6 mag** global command does not show any output.

  Conditions: The symptom is observed only when domain and MAG configurations are present.

  Workaround: If MAG configuration is complete (all requisite access interfaces and peers are configured) then this issue will not be seen.

- CSCua07791

  Symptoms: A Cisco ISR G2 running Cisco IOS Release 15.2(2)T or later shows a memory leak in the CCSIP_SPI_CONTRO process.

  Conditions: The leak is apparent after 3-4 weeks. The process is CCSIP_SPI_CONTRO.

  Workaround: There is no workaround.

- CSCua07927

  Symptoms: MLDP traffic is dropped for local receivers on a bud node.

  Conditions: This issue is seen on doing stateful switchover (SSO) on bud node.

  Workaround: Using the **clear ip mroute vrf** *vrf name* ***** command for the effected VRFs will resume the MLDP traffic.

- CSCua13418

  Symptoms: RP-Announce packets are being replicated across all the tunnel interfaces and the count of replication is equal to the number of tunnel interfaces. For example, if there are 3 tunnel interfaces, then each tunnel should forward 1 RP-Announce packet each minute (with the default timer configured). However, in this case, each tunnel is forwarding 3 RP-Announce packets across each tunnel interface. This issue is not specific to the number of interfaces. It can happen with any number of tunnel interfaces.

  Conditions: This symptom is observed when filter-autorp is configured with the **ip multicast boundary** command. This issue is seen on the Cisco 3725 router too, where the incoming packets are being replicated because of the **filter-autorp** command.

  Workaround: Removing filter-autorp resolves the issue. However, you need to remove the **pim** and **boundary** commands first and then reapply the pim and boundary list without the **filter-autorp** keyword. Also, doing this might lead to redesigning of the topology to meet specific requirements.

  int Tun X no ip pim sparse-dense mode no ip multicast boundary XXXXXX filter-autorp

  int TuX ip pim sparse-dense mode ip multicast boundary XXXXXX

- CSCua13561

  Symptoms: After upgrading to Cisco IOS Release 15.2(2)S, users cannot get IP address via PPP IPCP from DHCP pool on a Cisco ASR router. There was no configuration change.

  Conditions: This symptom occurs when upgrading to Cisco IOS Release 15.2(2)S.

  Workaround: Remove the **vpdn authen-before-forward** command.

- CSCua14594

  Symptoms: Memory leak is seen when polling for the following PW MIBS:

  ```
  1.3.6.1.4.1.9.10.106.1.5.1.1 (cpwVcPerfTotalInHCPackets)
  1.3.6.1.4.1.9.10.106.1.5.1.2 (cpwVcPerfTotalInHCBytes)
  1.3.6.1.4.1.9.10.106.1.5.1.3 (cpwVcPerfTotalOutHCPackets)
  1.3.6.1.4.1.9.10.106.1.5.1.4 (cpwVcPerfTotalOutHCBytes)

  Address    Size   Alloc_pc  PID  Alloc-Proc       Name
  34417B84      308 13774B30  473  SNMP ENGINE     AToM VC event trace
  ```

  This memory leak, on repeated polling, may lead to device crash.

  Conditions: This symptom is observed with Cisco IOS Release 3.6S upon polling of the SNMP VC statistics query.

  Workaround: There is no workaround.

- CSCua15292

  Symptoms: Router may report unexpected exception with overnight stress traffic.

  Conditions: The symptom is observed with the following conditions:

  - Cisco ISR 3925E is deployed as DMVPN hub router and about 100Mbps traffic is controlled by PfR MC with dynamic PBR.
  - Router logs with

  ```
  %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for
  destaddr=172.8.9.8, prot=50, spi=0xE8FB045F(3908764767), srcaddr=10.0.100.1, input
  interface=GigabitEthernet0/0
  ```

  Workaround: There is no workaround.

- CSCua16492

  Symptoms: Some IPv6 multi-hop BFD over BGP sessions flap.

  Conditions: Occurs on port-channel interfaces running IPv6 multi-hop BFD over BGP sessions after you perform an SSO.

  Workaround: There is no workaround.

- CSCua19425

  Symptoms: RP crashes at the far end, pointing to Watchdog Process BGP.

  Conditions: This symptom is observed when doing an FP reload at the near end. This issue is seen with EBGP sessions with BFD configured between near end and far end routers.

  Workaround: There is no workaround.

- CSCua21166

  Symptoms: Unable to form IPSec tunnels due to the following error:

  ```
  RM-4-TUNNEL_LIMIT: Maximum tunnel limit of 225 reached for Crypto functionality with
  securityk9 technology package license.
  ```

  Conditions: Even though the router does not have 225 IPsec SA pairs, error will prevent IPSec from forming. Existing IPSec SAs will not be affected.

  Workaround: Reboot to clear out the leaked counter, or install hsec9 which will disable CERM (Crypto Export Restrictions Manager).

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 2.8/2.3: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:M/C:N/I:N/A:P/E:U/RL:W/RC:C No CVE ID has been assigned to this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCua25943

  Symptoms: CPU Hog is observed on the LC when the number of IPv6 prefixes pumped in is more than 10,000.

  Conditions: This symptom is observed when more than 10,000 IPv6 prefixes are pumped into the router.

  Workaround: There is no workaround.

- CSCua26487

  Symptoms: SNMP loops at OID 1.3.6.1.4.1.9.9.645.1.2.1.1.1, and as a result, SNMP walk fails.

Conditions: This symptom is observed only on the SNMP getbulk request on 1.3.6.1.4.1.9.9.645.1.2.1.1.1.

Workaround: Exclude the MIB table from SNMP walk using SNMP view. See the below configurations.

```
snmp-server view <view name> iso included
snmp-server view <view name> ceeSubInterfaceTable excluded
snmp-server community <community> view <view name>nterfaceTable excluded
snmp-server community <community> view <view name>
```

- CSCua27852

  Symptoms: Traffic loss is seen in pure BGP NSR peering environment.

  Conditions: The symptom is seen on a Cisco router that is running Cisco IOS Release 15.2(2)S, and the BGP peerings to CEs and RR are all NSR enabled.

  Workaround: Enable the **bgp graceful-restart** command for RR peering.

- CSCua28346

  Symptoms: A router crashes during second rekey.

  Conditions: This symptom occurs with IKEv2 with RSA authentication.

  Workaround: There is no workaround.

- CSCua30053

  Symptoms: Authentication is failing for clients after some time because the radius_send_pkt fails, because it complains about the low IOMEM condition.

  Conditions: In AAA, minimum IO memory must be 512KB to process the new request. If the memory is less than this, AAA does not process the new authentication request. This is AAA application threshold. This application barriers are not valid in dynamic memory case. Such conditions are removed for NG3K platform.

  Workaround: There is no workaround.

- CSCua31794

  Symptoms: After reload with the debug image, framed E1 lines are down.

  Conditions: On checking the “show controller SONET”, the default controller framing mode is taken as “crc4”. However before reload the configuration for those E1s were configured as “no-crc4”. Customer configured them on the E1s as “no-crc4” and it started working fine and the “show controller SONET” framing output changed to “no-crc4”. As per running configuration still the configuration is not showing “no-crc4”, as it should show as the default is CRC4. So the current issue is configuring “no-crc4”, it is not showing in running configuration and not saved and after reload it shows again CRC4 and services go down again.

  Workaround: Configure E1s as “no-crc4” and they would be working fine, but such changes are not being saved in configuration, so if reload reoccurs all these services go down again.

- CSCua31903

  Symptoms: IPv6 traffic is forwarded to wrong VRF when address is the same on both VRFs.

  Conditions: This symptom is observed in an IPv6 MPLS VPN network that has PE routers, which have multiple CE routers connected. The CE routers are in different IPv6 VRFs. The CE routers have the same IPv6 address. The PE routers are dual and use dual stack. The problem happens on a 6VPE setup when the CEs share same the IP address.

  Workaround: There is no workaround.

- CSCua33287

  Symptoms: ES+: L2TPv3 entries are programmed incorrectly after restart.

  Conditions: This symptom is observed when some L2TPv3 sessions are established on ES+ module. After the restart of ES+, some np entries may not program correctly. As the result, ES+ will stop to transmit packets.

  This condition will recover after executing **shut/no shut** on physical interfaces.

  Workaround: There is no workaround.

- CSCua33527

  Symptoms: Traceback seen after second or third switchover:

  ```
  %LFD-SW2-3-SMBADEVENT: Unexpected event CO_WAIT_TIMEOUT for state RUNNING -Traceback=
  7908E9Cz 7909848z 79099CCz 7909B9Cz 78DBF20z 523292Cz 522C1D4z
  ```

  Conditions: The symptom is observed with a quad-sup scenario/setup. This traceback is seen on the new active RP after second switchover onwards.

  Workaround: There is no workaround.

- CSCua33821

  Symptoms: CPU utilization shoots up to 99% after configuring crypto maps.

  Conditions: The symptom is observed after applying crypto maps.

  Workaround: There is no workaround.

- CSCua34033

  Symptoms: A Cisco ME 3800X hangs after boot.

  Conditions: It is possible for an evaluation scaled license to be configured on the router and scaled services license configured. EULA acceptance can be ignored when configuring this. When the Cisco ME 3800X is rebooted, the router needs to program itself differently for a scaled license than a base license, but it cannot do so without the EULA being accepted so the router issues a prompt on the console port. The router will wait here until a user has responded. However, if a user is not on the console port to see this EULA message, they will not know that it is waiting for an EULA response. The router will continue to wait.

  This is not seen on purchased licenses as they are not installed unless the EULA is accepted.

  Workaround: When using evaluation licenses, accept the EULA upon configuring a license on the router or only reload the router from a connection to the console port after configuring the router to use an evaluation license.

- CSCua34638

  Symptoms: A crash is seen on RP2, when the **show platform software shell command package** command is issued.

  Conditions: This symptom is observed when the **show platform software shell command package** command is issued. It impacts the RP2 (x86_64_*) image only.

  Workaround: There is no workaround. Do not issue the **show platform software shell command package** command.

- CSCua35235

  Symptoms: Trace route for TP does not work as expected.

  Conditions: This symptom occurs with a TP setup.

  Workaround: There is no workaround.

- CSCua37898

  Symptoms: Memory leaks are observed with @crypto_ss_enable_ipsec_profile on VSS.

  Conditions: The memory leaks are seen when OSPFv3 authentication is enabled over virtual link, and the OSPFv3 process is restarted.

  Workaround: There is no workaround.

- CSCua38881

  Symptoms: Router reloads at clear_dspm_counter_per_bay.

  Conditions: This issue is observed from Cisco IOS interim Release 15.2(3.16)M0.1 on Cisco 5350 and Cisco 5400 routers.

  Workaround: There is no workaround.

- CSCua39107

  Symptoms: In a FlexVPN Spoke to Spoke setup, Resolution reply goes via the Tunnel interface to the Hub.

  Conditions: This symptom is only observed when NHO is added for the V-Access, overriding an existing route. This issue is not seen when H route is added.

  Workaround: Distribute the summarized address from the Hub, thus avoiding addition of NHO at the Spokes. The Spokes will then add H route instead of NHO.

- CSCua40273

  Symptoms: The ASR1k crashes when displaying MPLS VPN MIB information.

  Conditions: Occurs on the ASR1K with version 15.1(02)S software.

  Workaround: Avoid changing the VRF while querying for MIB information.

- CSCua40369

  Symptoms: DMM timestamping is not happening for IFM over EVC Xconnect and OFM over port-channel.

  Conditions: DMM timestamping is not happening in the following conditions when:

  1. Interface is used as core interface in EVC Xconnect.
  2. Interface is used as a member in a port-channel.

  Workaround: There is no workaround.

- CSCua40790

  Symptoms: Memory leaks when SNMP polling cbgpPeer2Entry MIB.

  Conditions: This symptom occurs when BGPv4 neighbors are configured.

  Workaround: There is no workaround if this MIB is to be polled.

- CSCua41082

  Symptoms: In/op traffic drop is observed on endor 10 gig port in mixed mode.

  Conditions: This issue is seen after upgrading Cisco IOS Release 15.2(2)S.

  Workaround: There is no workaround.

- CSCua41398

  Symptoms: The SUP720 crashes.

  Conditions: Occurs when you issue the sh clns interface | i ^[A-Z]|Number of active command multiple times via script with following error and decodes:

```
%ALIGN-1-FATAL: Corrupted program counter 00:53:22 EET Tue Jun 5 2012
pc=0x0 , ra=0x411514F4 , sp=0x55A8B080

c7600s72033_rp-adventerprisek9-m.122-33.SRE5.symbols.gz read in
Enter hex value: 0x407F5B70 0x407F612C 0x407E026C 0x42BCA588 0x407EDDFC
0x41A78BB8 0x41A78B9C
0x407F5B70:get_alt_mode(0x407f5b68)+0x8
0x407F612C:get_mode_depth(0x407f6118)+0x14
0x407E026C:parse_cmd(0x407ded18)+0x1554
0x42BCA588:parser_entry(0x42bca360)+0x228
0x407EDDFC:exec(0x407ed344)+0xab8
0x41A78BB8:r4k_process_dispatch(0x41a78b9c)+0x1c
0x41A78B9C:r4k_process_dispatch(0x41a78b9c)+0x0
```

Workaround: There is no workaround.

- CSCua43930

  Symptoms: Checksum value parsed from GRE header is not populating causing the GRE tunnel checksum test case to fail.

  Conditions: The issue is seen on a Cisco ISR G2.

  Workaround: There is no workaround.

- CSCua45114

  Symptoms: Default sessions will not establish when you apply VRF as a service to the default policy. VRF can only be applied to a default session by assigning a VRF on the access-interface. However with dedicated sessions, one cannot apply a VRF on the access-interface and VRF transfer at the same time. If we require VRF transfer on dedicated sessions, we need VRF transfer on lite sessions as well.

  Conditions: This symptom is seen when access-side interface is in the default VRF. VRF is applied as a service to the default policy.

  Workaround: There is no workaround.

- CSCua45122

  Symptoms: Multicast even log preallocated memory space needs to be conserved on the low-end platform.

  Conditions: This symptom is observed with multicast even log.

  Workaround: There is no workaround.

- CSCua45548

  Symptoms: Router crashes with **show ip sla summary** on longevity testing.

  Conditions: The symptom is observed with Cisco 2900, 1900, and 3945 routers configured with IPSLA operations. The router which was idle for one day crashes on issuing the command **show ip sla summary**.

  Workaround: There is no workaround.

- CSCua47570

  Symptoms: The **show ospfv3 event** command can crash the router.

  Conditions: The symptom is observed when “ipv4 address family” is configured and redistribution into OSPFv3 from other routing protocols is configured.

Workaround: Do not use the **show ospfv3 event** command.

- CSCua48584

  Symptoms: The Cisco ME 3600X's ARP resolution may fail after flexlink switchover.

  Conditions: This symptom is observed on the Cisco ME 3600X running Cisco IOS Release 15.2(S) or Cisco IOS Release 15.2(2)S1 with flexlink configured.

  Workaround: Shut the active port of the flexlink pair. In other words, do a manual switchover through CLI.

- CSCua48807

  Symptoms: Complete traffic loss is observed.

  Conditions: This symptom is observed when queue-limit and default WRED "random-detect" are configured in a class and dynamically modify queue- limit of that class.

  Workaround: There is no workaround.

- CSCua51991

  Symptoms: An invalid SPI message is seen throughout the lifetime of IPsec SA.

  Conditions: This symptom is observed with SVTI-SVTI with a GRE IPv6 configuration. When bringing up 1K sessions, an invalid SPI is seen. There is also inconsistency between the number of child SAs in IKEv2 and the number of IPsec SAs on the same box.

  Workaround: There is no workaround.

- CSCua52289

  Symptoms: CPU hog is seen on the line card due to Const2 IPv6 process.

  Conditions: This symptom occurs with 4 core facing tunnels. Upon FRR cutover, the CPU hog is observed.

  Workaround: There is no workaround.

- CSCua52977

  Symptoms: DHCPv6 solicitations are sent over the air. This should be filtered, as it is normally client->network and not a flood type of traffic.

  Conditions: This symptom applies to any network with clients using IPv6.

  Workaround: There is no workaround.

- CSCua53772

  Symptoms: Router crashes when scheduling a y1731 DMM IP SLA probe to run.

  Conditions: This symptom happens when the probe's target cfm mep is configured under service instance with double tag encapsulation.

  Workaround: There is no workaround.

- CSCua55539

  Symptoms: CE devices ping is failing on SAToP/CESoPSN.

  Conditions: This issue is observed only with ECMP at the core.

  Workaround: There is no workaround.

- CSCua55691

  Symptoms: A Cisco IOS memory leak is observed.

  Conditions: This symptom is seen when unconfiguring/reconfiguring BGP AD VFIs.

Workaround: There is no workaround.

Further Problem Description: This issue is seen during longevity run.

- CSCua56802

  Symptoms: QoS will not work on one of the subinterfaces/EVC.

  Conditions: This symptom occurs when HQoS policy is configured on more than one subinterface/EVC on ES+ and then add flat SG on them.

  Workaround: Remove and reapply SG.

- CSCua57728

  Symptoms: Traffic loss of ~25s is seen upon doing TE FRR Cutover with IPv6 prefixes.

  Conditions: This symptom is observed with four core facing tunnels, and 100,000 IPv6 prefixes. Shut the primary interface and check for the traffic loss.

  Workaround: There is no workaround.

- CSCua58100

  Symptoms: The syslog is flooded with the following traceback message:

  ```
  %SYS-2-NOTQ: unqueue didn't find 7F3D26BDCCD8 in queue
  7F3CA5E4A240 -Process= "RADIUS Proxy", ipl= 0, pid= 223
  -Traceback= 1#e0ee0ce60492fdd11f0b03e0f09dc812  :400000+873623 :400000+2547652
  :400000+20F9217 :400000+6C70C9C :400000+6C69C71 :400000+6C682BC :400000+6C68183
  ```

  Conditions: Occurs under the following conditions:

  - You establish 36k EAPSIM sessions using a RADIUS client on server A.
  - You establish 36k roaming sessions using a RADIUS client on server B.
  - The roaming sessions have the same caller-station-id but use a different IP address than the EAPSIM sessions.

  Workaround: There is no workaround.

- CSCua60395

  Symptoms: When an IPv6 packet is received via EoMPLS pseudowire, the packet is punted to the CPU and sent back on the pseudowire.

  Conditions: This has been identified on a Cisco ME3600X with Cisco IOS Release 15.2(1)S1.

  Workaround:

  Option 1: Configure the xconnect under a interface vlan and configure a (dummy) IP address. Example:

  ```
  interface vlan XXX
  ip address A.B.C.D M.M.M.M
  xconnect N.N.NN <vc-id> encapsulation mpls
  ```

  Option 2: Block IPv6 packets on remote end so that these packets are not sent over pseudowire.

- CSCua64546

  Symptoms: In a scaled setup with IPV4 and IPV6 ACL together (not necessarily on the same interface), IPV4 ACLs may stop working if the IPV6 ACL configured later overwrites the IPv4 ACL results and vice versa.

  Conditions: This symptom is observed with IPV4 and IPV6 ACLs configured on the box.

Workaround: There is no perfect workaround. Reconfiguring the IPV4 ACL can recover the functionality but will affect the IPV6 ACL.

Further Problem Description: Only the IPV4 or IPV6 ACL configuration will work.

- CSCua64700

  Symptoms: The IPsec tunnel state goes to Up-Idle after 4-5 days of the router being up and running.

  Conditions: This symptom is observed if you have low rekey value, as with the rekey, the new SPI gets allocated. This issue is seen with WS-IPSEC-3 and to verify this, check the below counter.

  ```
  show crypto ace spi
  ```

  If there is no decrement in the SPI allocated counter and there is a consistent increment in the counter, the chances are high that you will encounter this issue.

  Once the value reaches 61439, you will encounter this issue.

  ```
  MTCVPNK03#sh cry ace spi
  SPI in use .......................... 0
  Normal SPI allocated ................ 61439
  ```

  Workaround: There is no workaround. You need to reload the box.

- CSCua67532

  Symptoms: IPsec sessions fail to come up.

  Conditions: This symptom occurs when Site-Site crypto configuration using crypto map is applied on SVI, and when no ISAKMP profile is configured under that crypto map.

  Workaround: There is no workaround.

- CSCua67795

  Symptoms: The router does not transmit Y.1731 Delay Measurement Message (DMM) values using QinQ encapsulation.

  Conditions: Occurs with the following configuration:

  - An EFP is configured and applied to a bridge-domain.
  - The EFP is configured with QinQ encapsulation.
  - A Y.1731 Delay Measurement Message (DMM) value is applied.
  - The Y.1731 traffic uses a CoS value other than 0.

  Workaround: There is no workaround.

- CSCua67998

  Symptoms: System crashes.

  Conditions: This symptom occurs after adding or removing a policy-map to a scaled GRE tunnel configuration.

  Workaround: There is no workaround.

- CSCua68243

  Symptoms: IGMP and PIM control packets are not reaching RP. As a result, mac-address table for IGMP snooping entries is not populated.

  Conditions: This symptom can be seen on a Cisco 7600 series router that is running Cisco IOS where we have IGMP and PIM control packets coming in on an SVI only after the condition where the SVI link state went down and came up again. This does not affect routed ports.

  Workaround: Unconfigure and reconfigure the SVI.

- CSCua69657

  Symptoms: Traceback is seen when executing the **show clock detail** command.

  Conditions: This symptom is seen when executing the **show clock detail** command with Cisco IOS interim Release 15.3(0.4)T image.

  Workaround: There is no workaround.

- CSCua70065

  Symptoms: CUBE reloads on testing DO-EO secure video call over CUBE when SDP passthru is enabled.

  Conditions: The symptom is observed when running Cisco IOS interim Release 15.3(0.4)T.

  Workaround: There is no workaround.

- CSCua71038

  Symptoms: Router crash.

  Conditions: The symptom is observed with a Cisco router that is running Cisco IOS Release 15.2(3)T1. The router may crash during the failover test with OCSP and CRL configured.

  Workaround: Configure OCSP or CRL but not both

- CSCua72199

  Symptoms: Unsolicited RAs from the switch is forwarded as mcast RAs over the air to the wireless clients. It should be a unicast packet. CAPWAP packet header from the switch is populated with L2 MGID and not IPv6 RA MGID (L3) and forwarded as multicast over air.

  Conditions: This symptom is seen with Standalone Newton 48 with a couple of APs and a couple of wireless clients with IPv6 enabled. IPv6 unicast routing is enabled on the switch.

  Workaround: There is no workaround.

- CSCua72440

  Symptoms: The REP VLAN load balancing does not happen correctly when two REP edge no-neighbor ports are configured. Traffic does not flow as expected.

  Conditions: This symptom is seen with Cisco IOS Release 15.2(4)S image that is loaded on a Cisco 7600 box. Two REP edge no-neighbor ports along with VLAN Load balancing are configured. The correct VLANs are not blocked/opened on the respective ports.

  Workaround: There is no workaround.

- CSCua78782

  Symptoms: Authentication of EzVPN fails.

  Conditions: The symptom is observed with BR-->ISP-->HQ.

  Workaround: There is no workaround.

- CSCua80204

  Symptoms: EoMPLS remote port shutdown feature does not work.

  Conditions: This symptom is observed if xconnect and a service instance are configured under the same interface.

  Workaround: There is no workaround.

- CSCua83609

  Symptoms: With 10 VRFs, traffic is forwarded through data and default-mdt address. The PEs are connected in a serial fashion, and total number of PEs is over 200. After the number of PEs becomes more than 50, the CPU usage goes high as a result of both software and hardware switching of mVPN control packets like Data-MDT.

  Conditions: This issue has been seen under the following conditions:

  - Cisco ME 3600X is running Cisco IOS Release 15.2(4)S but is not release specific.
  - Multicast stream can be received on any type of interface (L2/L3).

  Traffic is stopped as the CPU hog/crash is seen. Issue can be verified via the following:

  “show processes cpu sorted | e 00”

  Workaround: There is no workaround.

- CSCua84879

  Symptoms: Crash at slaVideoOperationPrint_ios.

  Conditions: The symptom is observed when IPSLA video operations are configured and **show running-config** is issued.

  Workaround: There is no workaround.

- CSCua84923

  Symptoms: Following a misconfiguration on a two-level hierarchical policy with a user-defied queue-limit on a child policy, the UUT fails to attach the QoS policy on the interface even when corrected queueing features are used.

  Conditions: This symptom is observed with the following conditions:

  1. The issue must have the user-defined queue-limit defined.
  2. This error recovery defected is confirmed as a side effect with the c3pl cnh compoent project due to ppcp/cce infrastructure enhancement.

  Workaround: There is no workaround.

- CSCua85837

  Symptoms: Depending on the aces in the redirect-list ACL used, only a subnet of the traffic gets redirected based on ports.

  Conditions: This symptom is observed when the WCCP service has a redirect-list ACL applied which in turn has port-specific aces in them.

  Workaround: Remove the L4 operators from the redirect-list ACL.

- CSCua85934

  Symptoms: A session provisioning failure is seen in the ISG-SCE interface. The deactivate or disconnect request has the message authenticator wrongly calculated.

  Conditions: This symptom is observed with the ISG-SCE interface.

  Workaround: There is no workaround.

- CSCua86310

  Symptoms: When relay is configured with unnumbered interface, it appears the packet is sent out of the loopback interface (instead of the serial interface) to the server, which does not receive the packet.

Conditions: The issue happens only when unnumbered loopback address is used on the relay interface which connects to server. If an IPv6 address is used directly on the interface, it works fine.

Workaround: Use numbered interface instead of unnumbered interface.

- CSCua87944

  Symptoms: In an IPv6 snooping policy, the keyword "prefix-list" has no effect on control packet. The keyword only affects the binding table recovery. In an "ipv6 nd raguard" policy, the limited-broadcast keyword appears though it is deprecated. It should be hidden and is always on.

  Conditions: These symptoms are observed in an IPv6 snooping policy and IPv6 and RA-guard policy.

  Workaround: There is no workaround.

- CSCua88341

  Symptoms: Multicast traffic on P2P GRE tunnel will get dropped.

  Conditions: This symptom usually happens in scenarios like SSO, which is done after VRF deletion or addition. Here the P2P GRE tunnel will be in the VRF.

  Workaround: Do a shut/no shut of the P2P GRE tunnel interface.

- CSCua91104

  Symptoms: ISIS adjacency process shows traceback messaging related to managed timer.

  Conditions: This symptom is seen when configuring isis network point-to-point on LAN interface with isis bfd or isis ipv6 bfd enabled. The traceback does not happen always. It depends on timing.

  Workaround: Disable isis bfd or isis ipv6 bfd before issuing **isis network point-to-point** command. Restore isis bfd or isis ipv6 bfd configuration on LAN interface.

- CSCua93136

  Symptoms: The switch crashes when sending the DHCPv6 packet with "ipv6 snooping" on VLAN configurations.

  Conditions: This symptom occurs when sending the DHCPv6 packet with "ipv6 snooping" configured on VLAN configurations.

  Workaround: There is no workaround.

- CSCua94947

  Symptoms: RP crashes when downloading FreeRadius Framed-IPv6-Route on MLPPP sessions.

  Conditions: This symptom occurs when downloading radius Framed-IPv6-Route.

  Workaround: There is no workaround.

- CSCua98690

  Symptoms: The ES+/ES20/SIP-400 (any card which supports EVC) card may crash due to memory corruption.

  Conditions: This symptom is observed when the MAC ACL is configured on EFP.

  Workaround: There is no workaround.

- CSCua98902

  Symptoms: FIBIDB is not getting initialized.

  Conditions: This symptom is observed when LFA FRR is configured Cisco ME 3800X.

  Workaround: There is no workaround.

- CSCub07382

  Symptoms: NHRP cache entry for the spokes gets deleted on NHRP timer expiry even though there is traffic flowing through the spoke to spoke tunnel.

  Conditions: This symptom is seen with FlexVPN spoke to spoke setup.

  Workaround: Configure the same hold time on both tunnel interface and the virtual-template interface.

- CSCub07673

  Symptoms: IPsec session does not come up for spa-ipsec-2g if ws-ipsec3 is also present. “Volume rekey” is disabled on Zamboni.

  Conditions: This symptom occurs if we have “volume rekey” disabled on Zamboni.

  Workaround: Do not disable the volume rekey on Zamboni.

- CSCub09124

  Symptoms: MDT tunnel is down.

  Conditions: This symptom is seen in MVPN. If the **ip multicast boundary** command on non-current RPF interface blocks the MDT group, it may cause MDT tunnel failure.

  Workaround: Adding the **static join** command under PE loopback interface may work around the problem temporarily.

- CSCub10951

  Symptoms: At RR, for an inter-cluster BE case, there are missing updates.

  Conditions: This symptom is observed with the following conditions:

  1. The following configuration exists at all RRs that are fully meshed: - bgp additional-paths select best-external - nei x advertise best-external
  2. For example, RR5 is the UUT. At UUT, there is:

     - Overall best path via RR1.

     - Best-external (best-internal) path via PE6 (client of RR5): for example, the path is called “ic_path_rr5”.

     - Initially, RR5 advertises “ic_path_rr5” to its nonclient iBGP peers, that is, RR1 and RR3.
  3. At PE6, unconfigure the route so that RR5 no longer has any inter-cluster BE path. RR5 sends the withdrawals to RR1 and RR3 correctly.
  4. At PE6, reconfigure the route so that RR5 will have “ic_path_rr5” as its “best-external (internal) path”. At this point, even though the BGP table at RR5 gets updated correctly, it does not send the updates to RR1 and RR3. They never relearn the route.

  Workaround: Hard/soft clear.

- CSCub15542

  Symptoms: Configuring mpls lsp trace results in IOSD restart.

  Conditions: This symptom occurs when configuring mpls lsp trace results in IOSD restart.

  Workaround: There is no workaround.

- CSCub17985

  Symptoms: A memory leak is seen when IPv6 routes are applied on the per-user sessions.

  Conditions: This symptom is seen if IPv6 routes are downloaded as a part of the subscriber profile. On applying these routes to the sessions, a memory leak is observed.

Workaround: There is no workaround.

- CSCub18997

  Symptoms: A Cisco ME 3800 may crash after the following error message is displayed:

  ```
  %SYS-6-STACKLOW: Stack for process Non-Qos Events Process running low, 0/6000
  ```

  Conditions: This symptom is observed on a Cisco ME 3800 that is running Cisco IOS Release 15.2(2)S1.

  Workaround: There is no workaround.

- CSCub21468

  Symptoms: UDP header is corrupted randomly.

  Conditions: This symptom is observed with the Cisco 7609-S (RSP720-3C-GE) running Cisco IOS Release 12.2(33)SRE5, with the VRF Aware LI feature.

  Workaround: There is no workaround.

- CSCub24079

  Symptoms: TAR bundle does not get downloaded through the **archive** command.

  Conditions: This symptom applies to any conditions.

  Workaround: Untar externally and copy to flash/ucode1 directories.

- CSCub25360

  Symptoms: In a Flexlink switchover scenario, it seems that for some reason, the Cisco ME 3600X switch does not send out a dummy mcast packet for the SVI.

  Conditions: This symptom is observed with a Cisco ME 3600X Flexlink switchover.

  Workaround: There is no workaround.

- CSCub31592

  Symptoms: After the flap of the interface with EVC configured, the box is no longer adding second tag to the traffic. Forwarding is broken. See the following example:

  ```
  service instance 100 ethernet
    encapsulation dot1q 10
    bridge-domain 100
  ```

  Conditions: This symptom is seen with flap of the interface.

  Workaround: There is no workaround.

- CSCub31622

  Symptoms: RSTP BPDUs are not tunneled over xconnect.

  Conditions: This has been observed on Cisco IOS Releases 15.1(02)EY02a, 15.1(02)EY3 and 15.2(2)S1 with below configuration on the Cisco ME3800X:

  ```
  int gix/x
   service instance 100
    encapsulation default
    l2protocol tunnel
    bridge-domain 500

   int vlan 500
   platform rewrite imposition tag push 1 symmetric
  ```

```
 xconnect x.x.x.x 500 encapsulation mpls
```

This may create STP inconsistency and blocked VLANs on CE side.

Workaround: There is no workaround.

- CSCub31902

  Symptoms: Alignment correction tracebacks are seen from within the diag_dump_lc_l2_table() cosmetic issue, which create temporary memory inconsistencies in the function.

  Conditions: This symptom occurs in normal conditions, during bootup time, provided testMacNotification fails.

  Workaround: Disable bootup diagnostics or disable the testMacNotification health monitoring test.

- CSCub32500

  Symptoms: Router crashes in EIGRP due to chunk corruption.

  Conditions: This symptom is seen on EIGRP flaps.

  Workaround: There is no workaround.

- CSCub33877

  Symptoms: During the "issue loadversion" where we are downgrading from Texel (or later) to Yap (v151_1_sg_throttle or earlier), the standby RP keeps reloading due to the out of the sync of configuration.

  Conditions: The issue occurs during ISSU loadversion operation. The newer version of image supports the IPv6 multicast while the older version of image does not.

  Workaround: There is no workaround.

- CSCub35388

  Symptoms: The **port-channel min-links** command is rejected under port-channel.

  Conditions: This symptom is seen when port-channel has vrf configuration.

  Workaround: first configure min-link command and then configure vrf command under port-channel

- CSCub36217

  Symptoms: When the Cisco ME 3800 router is running Cisco IOS Release15.2(4)S software, if EVC maximum MAC security address limit is reached for a service instance, new MAC address is not rejected.

  Conditions: This symptom is observed when EVC MAC security is enabled under a service instance.

  Workaround: There is no workaround.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 1.7/1.3: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:L/AC:L/Au:S/C:N/I:P/A:N/E:U/RL:OF/RC:C No CVE ID has been assigned to this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCub42920

  Symptoms: KS rejects rekey ACK from GM with message (from "debug crypto gdoi ks rekey all"):

  ```
  GDOI:KS REKEY:ERR:(get:0):Hash comparison for rekey ack failed.
  ```

  The keys and policies in the rekey packet are correctly installed by the GM, but the rekey ACK does not get processed by the KS. This leads to rekey retransmissions, GM re-registration and potential disruption of communication.

Conditions: Rekey ACK validation in Cisco IOS Releases 15.2(4)M1 (ISR-G2) and 15.2(4)S/XE 3.7S (Cisco ASR1000) is incompatible with other software releases.

A KS that runs Cisco IOS Releases 15.2(4)M1 or 15.2(4)S/XE 3.7S will only be able to perform successful unicast rekeys with a GM that runs one of those two versions. Likewise, a KS that runs another version will only interoperate with a GM that also runs another version.

Workaround: Use multicast rekeys.

- CSCub46570

  Symptoms: The image cannot be built with an undefined symbol.

  Conditions: This symptom occurs as the commit error triggers the compiling issue.

  Workaround: There is no workaround.

- CSCub47520

  Symptoms: "Match dscp default" matches router initiated ARP packets.

  Conditions: This issue is seen on Cisco 7600 ES+ line cards.

  Workaround: Classify router generated packets using source mac address using a MAC ACL.

- CSCub48262

  Symptoms: Router crashes in ROMMON.

  Conditions: This symptom occurs with RSP processor.

  Workaround: There is no workaround.

- CSCub49291

  Symptoms: Static tunnels between hubs and spokes fail to rebuild.

  Conditions: This symptom occurs when reloading hub on the DMVPN IPv6 setup with DPD on-demand enabled on all spokes.

  Workaround: There is no workaround.

- CSCub54872

  Symptoms: A /32 prefix applied to an interface (e.g. a loopback) is not being treated as connected. This can then prevent Half-Duplex VRFs from operating correctly.

  Conditions: This symptom is seen when the prefix applied to an interface is for a host route (/32 for IPv4 or /128 for IPv6).

  Workaround: Use a shorter prefix.

- CSCub62897

  Symptoms: SVI is not coming up for a long time even though there are active ports in that VLAN.

  Conditions: This issue happens with flexlink + preemption + VLAN load balance configuration.

  Workaround: There is no workaround.

- CSCub67101

  Symptoms: The POS interface line protocol is down with encapsulation PPP in an MPLS setup.

  Conditions: This symptom occurs when configuring encapsulation PPP on both ends of PE1 and CE1, and then configuring xconnect in the customer-facing interface of PE1.

  Workaround: Reconfigure the xconnect settings. Then, the interface will come up in the proper state.

- CSCub73159

  Symptoms: IOSD crash is observed.

Conditions: This symptom is seen when bringing up 8k PPP sessions with QoS and eBGP routes.

Workaround: There is no workaround.

- CSCub73430

  Symptoms: A Cisco router that is running Cisco IOS Release 15.2.(4)S ipBaseK9 feature set crashes when an interface that a QoS policy attached to it comes up.

  Conditions: This symptom occurs on a Cisco router that is running Cisco IOS Release 15.2.(4)S ipBaseK9 feature set.

  Workaround: Use other feature sets.

- CSCub78830

  Symptoms: Traffic matching WCCP service gets black-holed.

  Conditions: This symptom is seen in vrf-wccp scenario and on redirection into MPLS cloud.

  Workaround: There is no workaround.

- CSCub78917

  Symptoms: PIM VRF neighbor is not coming up.

  Conditions: This symptom is seen with MVPN v6 configurations.

  Workaround: Use an earlier image where it was proper.

- CSCub79102

  Symptoms: Router crashes with MVPNV6 setup.

  Conditions: This symptom is seen while unconfiguring VRF. The router crashes.

  Workaround: There is no workaround.

- CSCub92588

  Symptoms: The chopper SPA does not come up.

  Conditions: This symptom is seen when the router reloads.

  Workaround: There is no workaround.

- CSCub98588

  Symptoms: The IPsec session does not comes up for spa-ipsec-2g if you have “volume rekey” disabled.

  Conditions: This symptom is seen if we have “volume rekey” disabled on spa-ipsec-2g.

  Workaround: Do not disable the volume rekey on spa-ipsec-2g.

- CSCub99756

  Symptoms: A Cisco ASR 1000 router that is running Cisco IOS Release 15.2(4)S acting as a GM in a GETVPN deployment starts using the most recent IPSEC SA upon KS rekey instead of using the old key up to 30 seconds of expiration.

  Conditions: This symptom is observed only in Cisco IOS Release 15.2.(4)S.

  Workaround: There is no workaround.

- CSCuc08298

  Symptoms: ISSU between XE 3.7S base version (Cisco IOS Release 15.2(4)S) and Cisco IOS Release 15.2(4)S2 or later releases may not pass in the presence of trifecta modules.

  Conditions: This issue is specific to setups with trifecta modules.

Workaround: In order to make ISSU work with (Cisco IOS Release 15.2(4)S) base release, power down the trifecta module using **no power enable mod** t*rifecta slot(s)* and then carry out the ISSU procedure to releases later than Cisco IOS Release 15.2(04)S2.

- CSCuc11090

  Symptoms: With Cisco ME3600/ME3800 as the encap box in MVPN, if the packet size if greater than the default MTU, packets will not flow out of the box.

  Conditions: This symptom is seen with MVPN configured on Cisco ME3600/ME3800 box. The box should be a core encap box and traffic should be going on the tunnel to hit this situation. Only packets beyond the default MTU will not go out and get dropped.

  Workaround: Send packets of smaller size from the source so that after encaping with the 24 bytes of outer IP of the MDT tunnel does not go beyond the size of egressing interface MTU.

- CSCuc13364

  Symptoms: Egress service policy on EFP is dropping all traffic in egress. Offered rate equals drop rate. Interface output rate is zero, output drop is increasing.

  Conditions: This issue has been observed with Cisco ME36xx that is running Cisco IOS Release 15.2(2)S.

  Workaround: There is no workaround.

- CSCuc14023

  Symptoms: Cisco IOS build failure is due to signature verification.

  Conditions: This symptom is seen with Cisco 7600 build, RSP and SUP image.

  Workaround: There is no workaround.

- CSCuc15548

  Symptoms: Subscriber session on LAC/LNS is stuck in attempting state with “vpdn authen-before-forward” CLI configured and auto-service in the radius-profile.

  Conditions: The key to the issue is CLI “vpdn authen-before-forward” and one auto-service in the user profile in radius.

  Workaround: Configure and apply one policy-map with SESSION-START rule with at least one action.

- CSCuc15656

  Symptoms: REP occasionally fails when a peer device that is running REP on the same segment is reloaded.

  Conditions: This issue is seen when a remote device is reloaded. The REP state machines on both devices can get stuck.

  Workaround: Flap the link of the unit that did not go into the REP wait state. This will bring the REP statemachines at both ends.

Open Caveats—Cisco IOS Release 15.2(4)S

This section describes possibly unexpected behavior by Cisco IOS Release 15.2(4)S. All the caveats listed in this section are open in Cisco IOS Release 15.2(4)S. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCtl86057

  Symptoms: The loading of the standby RP and bulk sync times have increased on the XE3 throttle. Increases in time of up to 20-30% have been seen.

  Conditions: Under higher scale this problem becomes more noticeable.

  Workaround: There is non known workaround at this time. We are still investigating the problem.

- CSCtq24011

  Symptoms: Routers act like if local-proxy-arp is configured and does a proxy-arp even for the systems in the same subnet.

  Conditions: The router receives arp request on an interface while the interface is not fully initialized. The connected routes are not added in the routing table yet. This causes proxy-arp reply and wrong arp entry stuck forever.

  Workaround: **shut/no shut** on victim and offender routers.

- CSCtq56659

  Symptoms: Wrong LC programming with CEM interface.

  Conditions: Issue is seen after the initial configuration of HSPWs.

  Workaround: Soft OIR.

- CSCtr45030

  Symptoms: The SNMP timers process causes the router to exit global configuration mode or prevents the console from entering global configuration mode.

  ```
  c7609#conf t
  ```

  Configuration mode is locked by process “319” user “unknown” from terminal “0”. Please try later.

  ```
  c7609#show proc | in 319

    319 Mwe  9735348          928      21701      42 4412/6000   0 SNMP Timers
  ```

  Or

  ```
    c7609(config)#logging console
  ```

  Config session is locked by process “307”, user will be pushed back to exec mode. Command execution is locked, Please try later.

  ```
    c7609(config)#^Z
  ```

  Conditions: Occurs when you copy and paste large configurations, particularly a large number of VLAN configurations. The issue occurs without any SNMP configurations present.

  Workaround:

  - Option 1 - Disable RMON
  - Option 2 - If configuration is huge. Paste in multiple blocks.

  - Option 3 - Enable debug snmp timers. Paste the required configuration when the timer callbacks have finished executing.

- CSCtr94565

  Symptoms: Sp hung after the router crashes.

  Conditions: Occurs with bgp-pic core and enabled.

  Workaround: Disable the bgp pic.

- CSCts04802

  Symptoms: During vrf transfer, old services are removed but the new service is not applied.

  Conditions: This symptom is observed during a vrf transfer from v1 to v2.

  Workaround: There is no workaround.

- CSCts11715

  Symptoms: After shutting the tunnel, ISAKMP does not turn OFF.

  Conditions: This symptom is observed in a scaled DMVPN setup with more than 1k spokes.

  Workaround: There is no workaround.

- CSCts54641

  Symptoms: Various small/medium/big/VB chunks leak at the following functions:

  __be_snmp_decode_varbind

  __be_snmp_decode_sync_msg

  __be_k_ciscoFlashDeviceEntry_get

  __be_snmp_decode_varbind

  __be_mib_tlv_to_oid

  __be_mib_tlv_to_octet

  __be_snmp_decode_varbind

  Conditions: MIBs are being polled or SSO is done.

  Workaround: There is no workaround.

- CSCtw94737

  Symptoms: Standby supervisor keeps getting power-cycled due to RF request:

  ```
  %OIR-SP-3-PWRCYCLE: Card in module 6, is being power-cycled (RF request)
  ```

  Conditions: Symptom is observed during RPR downgrade from Cisco IOS 15S to Cisco IOS Release 12.2SRE.

  Workaround: Perform downgrade through reload.

- CSCtx15799

  Symptoms: An MTP on a Cisco ASR router sends an “ORC ACK” message through CRC for the channel ID that is just received but does not reply to the ORC for the next channel.

  Conditions: The symptom is observed when there is a very short time lapse between the ORC and CRC, say 1 msec.

  Workaround: There is no workaround.

- CSCtx23593

  Symptoms: Some virtual circuit (VC) information is missing in the Simple Network Management Protocol (SNMP) MIB object cAal5VccEntry from the output of the **snmpwalk** router configuration command. For example, The ATM VCs 4/0.120 exist on the router but are missing in the MIB.

  Conditions: This symptom is observed on a Cisco 7204VXR (NPE-G2) router that is running Cisco IOS Release 12.2(33)SRE5 (c7200p-advipservicesk9-mz.122-33.SRE5.bin) image in customer network. The symptom may also occur in other releases.

  Workaround:

  - Enter the **show atm vc** privileged EXEC command on the same device to obtain a complete list of all the VCs. Or,
  - Do the SNMPWALK suffixing the ifIndex of the interface to get the value. $ snmpwalk -v 2c -c fwwrcmn na-salerno-ar011 .1.3.6.1.2.1.2.2.1.2 | grep "4/0.120" IF-MIB::ifDescr.253 = STRING: ATM4/0.120-atm subif IF-MIB::ifDescr.254 = STRING: ATM4/0.120-aal5 layer

    ```
    $ snmpwalk -v 2c -c fwwrcmn na-salerno-ar011 .1.3.6.1.2.1.2.2.1.2 | grep "4/0.120"

    IF-MIB::ifDescr.253 = STRING: ATM4/0.120-atm subif

    IF-MIB::ifDescr.254 = STRING: ATM4/0.120-aal5 layer


    $  snmpwalk -v 2c -c fwwrcmn na-salerno-ar011 .1.3.6.1.4.1.9.9.66.1.1.1.1.3 | grep
    9.9.66.1.1.1.1.3.254 ===> Got no entry of ifindex here in complete snmpwalk

    $

    $ snmpwalk -v 2c -c fwwrcmn na-salerno-ar011 .1.3.6.1.4.1.9.9.66.1.1.1.1.3.254
    ===> When done the SNMPWALK suffixing the ifindex, then getting the value which
    can be one workaround.

    SNMPv2-SMI::enterprises.9.9.66.1.1.1.1.3.254.200.106 = Counter32: 403633041
    ```

- CSCtx54882

  Symptoms: A Cisco router may crash due to bus error crash at voip_rtp_is_media_service_pak.

  Conditions: This symptom is been observed on a Cisco router that is running Cisco IOS Release 15.1(4)M2.

  Workaround: There is no known workaround.

- CSCtx59669

  Symptoms: Spikes are observed in UDP jitter RTT values for MPLS VPN based operations.

  Conditions: On a Cisco 7600 when there are a large number of packets configured per UDP operation, some packets (~1%) exhibit large RTT delays. This is especially noticeable when BGP is exchanging large number of routes.

  Workaround: There is no workaround.

- CSCtx72906

  Symptoms: Standby gets stuck in cold-bulk state and it does not come up in SSO mode even after few hours.

  Conditions: This symptom is seen with scale QoS configs applied on EVCs/subifs (L2VPN/L3VPN) and scale crypto configs.

  Workaround: There is no workaround.

- CSCty09682

  Symptoms: REP Primary edge fails to take part in REP.

  Conditions: Occurs on reload.

  Workaround: Flap the interface, and it will converge.

- CSCty10693

  Symptoms: Device crashes with what looks like a memory corruption.

  Conditions: Are not known at this time and will update as we have more information.

  Workaround: There is no workaround.

- CSCty22117

  Symptoms: When swapping ip addresses on an ethernet connection between an MWR2941 and a Cisco 7600. OSPF fails to re-establish.

  Conditions: Changing the IP address in the Cisco MWR2900 to the neighbors IP address and then changing the neighbors IP address to what was on the MWR causes the MWR to see a duplicate IP address and never allows the svi to participate in OSPF.

  Tested changing the IP address in the other equipment first and this works fine. Only when the Cisco MWR2900 is changed first do we see this issue.

  Workaround: "Change" the MWR address back to bad address:

  - This causes duplicate address. OSPF timers again expire.
  - Now change back the MWR address to final IP address. We will not have the duplicate address this time, and the OSPF process completes to FULL.

- CSCty31982

  Symptoms: Portchannel is in suspended state, with peer throwing messages that lacp is not enabled on remote node.

  Conditions: This symptom occurs on reload.

  Workaround: Remove/Add untagged service instance which would have l2peer stp,lacp configured.

- CSCty33037

  Symptoms: Out of memory is seen on sender

  Conditions: This symptom is observed on three Telepresence sessions running at the same time for maximum duration (10 minutes).

  Workaround: There is no workaround. Reduce duration or session number.

- CSCty47447

  Symptoms: IPv6 traffic over IPv6 sVTI tunnels gets dropped.

  Conditions: This symptom is seen under the following conditions:

  - Have GRE+IPsec tunnels configured with QoS.
  - Have IPv4 sVTI tunnels configured with QoS.
  - Have IPv6 sVTI tunnels configured.

  With all the above tunnels configured, traffic should flow on all the IPv4 IPsec and VTI tunnels and traffic rate should oversubscribe the QoS policy on them.

  Workaround: There is now workaround.

- CSCty53054

  Symptoms: Tracebacks show up on standby sometimes when **shut/unshut** of the p2mp TE tunnel.

  Conditions: This symptom is seen when a dual RP box **shut/noshut** of the p2mp TE tunnel may generate traceback. There is no functionality impact.

  Workaround: There is no workaround.

- CSCty57137

  Symptoms: SIP SPAs go out of service state in scaled subinterface config (more than 2000 subinterfaces on single GigE port).

  Conditions: While performing ISSU between iso1-rp2 and iso2-rp2 xe3.6 throttle image, after issu runversion, the SIP SPAs go out of service state. Need heavily scaled config. Seen when there are 2000 to 3000 subinterfaces on the single SPA and following limits are exceeded. Overall dual stack VRFs per box: 2800 dual stack limit on interface: 1000.

  Workaround: The issue is not seen in the following scenario:

  1. Before doing a load version from RP0 (initial active), issue the following command: asr1000# show ipv6 route table | inc IPv6.
  2. Note down the number of ipv6 route tables in the system.
  3. Do a load version.
  4. Wait for standby to come up to Standby hot.
  5. Enable standby console from RP0 (active) asr1000#configure terminal Enter configuration commands, one per line. End with CNTL/Z. asr1000(config)# asr1000(config)#redundancy asr1000(config-red)#main-cpu asr1000(config-r-mc)#standby console enable.
  6. Login to standby console and issue the following command asr1000-stby# show ipv6 route table | inc IPv6 Again note down the number of IPv6 route tables in standby. If it is less than the number noted at step2, wait for some time and re-verify till it reaches the number noted in step 2.
  7. Issue issu runversion from RP0 (active)

- CSCty59891

  Symptoms: On the node where **shut/no shut** is issued, traffic does not reach IPsec VSPA which is supposed to get encrypted.

  Conditions: Issue **shut/no shut** on the GRE tunnel protected with IPsec and QoS configured on this IPsec Tunnel.

  Workaround: Remove and attach “tunnel protection ipsec profile”.

- CSCty64216

  Symptoms: On unconfiguring a scaled ACL, a router crash is noted.

  Conditions: This symptom is seen with an ACL having 1000 ACEs or more when unconfigured.

  Workaround: There is no workaround.

- CSCtz06740

  Symptoms: MPLS LSP ping does not work when PE-to-PE TE tunnel is down.

  Conditions: PE-to-PE tunnel is down, and Next hop to PE1 has TE tunnel to remote PE2. PE1 is Cisco ME3600.

  Workaround: There is no workaround.

- CSCtz17175

  Symptoms: Traffic loss for 100 seconds will be seen.

  Condition: When the router with ~32K VCs configured is reloaded.

  Workaround: There is no workaround.

- CSCtz37164

  Symptoms: The requests to the radius server are retransmitted even though the session no longer exists. This causes unnecessary traffic to radius and also radius gets requests for an invalid session.

  Conditions: This issue occurs when the radius server is unreachable and the CPE times out the session

  Workaround: The issue can be seen as per the conditions mentioned above. This can be avoided by making sure that the radius server is always reachable

- CSCtz49200

  Symptoms: OSPF IPv6 control packets are not encrypted/decrypted.

  Conditions: Occurs while configuring the ipv6 ospf authentication.

  Workaround: There is no workaround.

- CSCtz50204

  Symptoms: Crash is seen while applying “vrf ivrf2” on Server.

  Conditions: Crash is seen while applying “vrf ivrf2” on Server.

  Workaround: There is no workaround.

- CSCtz50537

  Symptoms: Deactivation of ipv4 unicast rpf via radius does not work.

  Conditions: Occurs when you configure a user profile in Radius with an AVPair: Cisco-AVPair += “lcp:interface-config=no ip verify unicast source reachable-via rx”.

  No error appears in debugs or logs. The same configuration works in Cisco IOS XE Release 2.x releases but does not work in 3.x releases.

  Workaround: There is no workaround.

- CSCtz62857

  Symptoms: RP crashes with segmentation fault pointing to IP RIB Update process.

  Conditions: This problem is seen if you issue the configuration command: no router bgp during the period between when BGP is first configured and when it completes routing protocol initialization and bulk sync to the standby.

  Workaround: Wait for BGP initialization and bulk sync to complete before issuing “no router bgp”. How long this takes will vary by platform, configuration, and routing table size. On an Cisco ASR 1004 with an RP2 route processor and a typical configuration and routing table size, this takes no longer than 20 minutes.

- CSCtz63438

  Symptoms: In a GETVPN environment, the group member continuously registers to keyserver.

  Conditions: The symptom is observed when the onboard crypto engine is disabled on a Cisco 1900 series platform.

  Workaround: There is no workaround.

- CSCtz69517

  Symptoms: IPv6 VRF data packets are getting punted to CPU.

  Workaround: There is no workaround.

- CSCtz70207

  Symptoms: The device experiences an I/O memory leak in the “Big” buffer pool.

  Conditions: Occurs when you configure NetFlow data export and the device is actively exporting traffic to a collector.

  Workaround: Disable NF/NF data export.

- CSCtz71084

  Symptoms: When prefix from CE is lost, the related route that was advertised as best-external to RR by PE0 does not get withdrawn.

  Conditions:

  ```
  PE0#conf t
  Enter configuration commands, one per line. End with CNTL/Z.
  PE0(config)#router bgp 1
  PE0(config-router)#address-family ipv4 vrf CE2
  PE0(config-router-af)#import path selection all
  PE0(config-router-af)#bgp recursion host
  PE0(config-router-af)#bgp advertise-best-external
  PE0(config-router-af)#end
  ```

  Even though the configs have SOO, it is not necessary for the repro.

  However, the issue is not happening if we shut the interface between PE0-CE2 from either side. Instead, need to do something like the following to stop CE2 to advertise the prefixes:

  ```
  CE2#conf t
  Enter configuration commands, one per line. End with CNTL/Z.
  CE2(config)#router bgp 2
  CE2(config-router)#no network 100.1.1.0 mask 255.255.255.0
  CE2(config-router)#no network 110.1.1.0 mask 255.255.255.0
  CE2(config-router)#no network 120.1.1.0 mask 255.255.255.0
  CE2(config-router)#
  ```

  Workaround: There is no workaround.

- CSCtz87622

  Symptoms: MLDP traffic is dropped for sometime (few min) couple of times after SSO.

  Conditions: Issue is seen soon after performing SSO.

  Workaround: There is no workaround.

- CSCtz90328

  Symptoms: Multicast traffic stops for some time because of CPU Hog on removal of the QoS policy-map from the service instance.

Conditions: Occurs when the Multicast traffic is bursty and is oversubscribing the queue.

Workaround: There is no workaround.

- CSCtz91502

  Symptoms: Nile unicast met shows multiple ReplicationContextQueueEntry, and traffic is flooded to all ports in vlan.

  Conditions: The issue is seen when a access port is in the same vlan as the rep segment. A rep flap is seen.

  Workaround: Clear mac-address table fixes the CQE entries.

- CSCtz92606

  Symptoms: MFR memberlinks - T1 serial intfs created under a CHOC12 controller, do not get decoupled from MFR even after the MFR bundle intf is deleted. And once the MFR bundle interface is reconfigured, the memberlinks does not appear under it.

  Conditions: MFR with memberlinks as T1 serials from CHOC12 sonet controller.

  Workaround: Unconfigure and reconfigure the “encap frame-relay MFRx” under each memberlink after reconfiguring the MFR bundle interface.

- CSCtz97297

  Symptoms: Router takes sporadically up to 5 seconds to forward multicast after IGMP join is received.

  Conditions: None.

  Workaround: Use static IGMP join on egress interface.

- CSCua01641

  Symptoms: The router’s NAS-IP address contained in the RADIUS Accounting-on packet is 0.0.0.0:

```
===
*May 17 14:34:22 JST: RADIUS:  Acct-Session-Id     [44]  10  "00000001"
*May 17 14:34:22 JST: RADIUS:  Acct-Status-Type    [40]  6   Accounting-On
        [7]
*May 17 14:34:22 JST: RADIUS:  NAS-IP-Address      [4]   6   0.0.0.0
         <<======Here!!!
*May 17 14:34:22 JST: RADIUS:  Acct-Delay-Time     [41]  6   0
===
```

  Conditions: Occurs when you restart the router.

  Workaround: There is no workaround.

- CSCua03201

  Symptoms: If the VPN ID of an existing Virtual Forwarding Interface (VFI) is changed on a dual-RP system, and then a stateful switchover (SSO) is performed, the new standby router may repeatedly reload.

  Conditions: This symptom has been observed in Cisco IOS Release 15.2(2)S/ Cisco IOS XE Release 3.6.0S and later.

  Workaround: In order to configure a new VPN ID for a VFI, completely remove the existing VFI and reconfigure it.

- CSCua06629

  Symptoms: The **sh ipv6 mobile pmipv6 mag globals** command does not show any output.

Conditions: The symptom is observed only when domain and MAG configurations are present.

Workaround: If MAG configuration is complete (all requisite access interfaces and peers are configured) then this issue will not be seen.

- CSCua07791

  Symptoms: ISR-G2 running Cisco IOS Release 15.2(2)T or later sees memory leak in CCSIP_SPI_CONTRO process.

  Conditions: The leak is apparent after 3-4 weeks. Process is CCSIP_SPI_CONTRO.

  Workaround: There is no workaround.

- CSCua07927

  Symptoms: MLDP Traffic is dropped for local receivers on a bud node.

  Conditions: Issue is seen on doing SSO (stateful switchover) on Bud node.

  Workaround: **clear ip mroute vrf** *vrf name** for the effected vrfs will resume the MLDP traffic.

- CSCua09764

  Symptoms: SSS Manager intermittently crashes when clearing sessions. This crash has been seen when issuing "clear subscriber session all" with a single L2 session and 600 default sessions.

  Conditions: This crash is difficult to reproduce and occurs more frequently when you have "debug subscriber policy all" enabled while continuously clearing sessions.

  Workaround: There is no workaround.

- CSCua13561

  Symptoms: After upgrading to Cisco IOS Release 15.2(2)S, users cannot get IP address via PPP IPCP from DHCP pool on Cisco ASR. There is no configuration change.

  Conditions: Upgrade from Cisco IOS Release 12.2(33) XNF2 to Cisco IOS Release 15.2(2)S.

  Workaround: There is no workaround.

- CSCua13804

  Symptoms: Router crashes when doing snmp query on ERM- Resource Groups.

  Condition: Crash occurs only when a resource group is configured.

  Work around: There is no workaround.

- CSCua20373

  Symptoms: After SSO, we will see all the GRE tunnels get admin down and it stays down until the security module SSC-600/WS-IPSEC-3 comes up. We see complete traffic loss during this time.

  Conditions: Have Vanilla GRE tunnels configured in the system where HA and IPsec Module SSC-600/WS-IPSEC-3 card is present and issue SSO.

  Workaround: There is no workaround.

- CSCua21238

  Symptoms: IOSD crashes at _ipv6_address_set_tentative.

  Conditions: Occurs while unconfiguring ipv6 subinterfaces.

  Workaround: There is no workaround.

- CSCua23451

  Symptoms: High convergence is seen on Cisco 7600 SUP720 switchover (oir or software cli) in 1 out of 10 readings.

Conditions: Occurs with high convergence on Cisco 7600 SUP720 switchover (oir or software cli) in 1 out of 10 readings.

Workaround: There is no workaround.

- CSCua23570

  Symptoms: IS-IS adjacency remains down on the standby RP while it is up on the active RP. If a switchover occurs this may result in an adjacency flap as the Standby transition to Active.

  Conditions: Occurs when you apply the multi-topology command under the IPv6 address family and the router receives IPv6 prefixes through IS-IS.

  Workaround: There is no workaround.

- CSCua24676

  Symptoms: VRF to global packet's length are corrupted by -1.

  Conditions: Issue is seen when the next-hop in vrf is global and recursive going out labled. Issue is seen from Cisco IOS Release 15.0(1)S3a onwards and not seen on Cisco IOS Release 15.0(1)S2.

  Workaround: Use next hop interface ip instead of recursive next hop.

- CSCua25943

  Symptoms: CPU Hog is seen on the LC with CMFI Background process hogging the CPU.

  Conditions: It is observed when more than 10k IPv6 prefixes are pumped into the router.

  Workaround: There is no workaround.

- CSCua26064

  Symptoms: IPv6 routes in the global routing table take up different adjacency entries.

  Conditions: It is seen when there are 4 core facing tunnels that load balance traffic to these prefixes. "show mls cef ipv6 <prefix> detail" shows the different adjacencies taken by different prefixes.

  Workaround: Have a single tunnel on the core facing side, instead of a load balanced path.

- CSCua26981

  Symptoms: A Cisco ASR router may crash due to a CPU Watchdog upon invocation of "show ip eigrp neighbor detail."

  ```
  CMD: 'sh ip eigrp nei detail'
  <snip>
  ASR1000-WATCHDOG: Process = Exec
  %SCHED-0-WATCHDOG: Scheduler running for a long time, more than the maximum configured
  (120) secs.
  -Traceback= ...
  ```

  Conditions: The Cisco ASR router must be experiencing rapid changes in EIGRP neighborship, such as during a flap. One way to artificially create this scenario is to mismatch the interface MTU.

  Workaround: There is no workaround.

- CSCua27842

  Symptoms: The Cisco ASR 1000 router crashes in Firewall code due to NULL l4_info pointer. Day 1 issue.

  Conditions: This symptom occurs when the Cisco ASR 1000 router acts as the MPLS L3VPN UHP. It crashes because FW/NAT requires the l4_info to be set. To trigger this issue, the following features must be configured:

  1. MPLS L3VPN (PE)

2. Zone Based FW/NAT
3. MPLS & MP-BGP loadbalance configured towards upstream router

Workaround: There is no workaround.

- CSCua27852

  Symptoms: Traffic loss is seen in pure BGP nsr peering environment.

  Conditions: The symptom is seen on Cisco router with Cisco IOS Release 15.2(2)S, and the bgp peerings to CEs and RR are all NSR enabled.

  Workaround: Enable the bgp graceful-restart for RR peering.

- CSCua29001

  Symptoms: ANCP truncated line rate is not seen on standby and the policy application will differ from that on active.

  Conditions: Occurs when **ancp truncate** *value* CLI is enabled and port ups received on BRAS.

  Workaround: There is no workaround.

- CSCua30956

  Symptoms: Network is not reachable behind CEs when primary PW fails and secondary PW takes over.

  Conditions: Primary PW fails. Secondary takes over but network behind CEs are not reachable.

  Workaround: There is no workaround.

- CSCua30963

  Symptoms: DHCP client is not getting a response for DHCPREQUEST message.

  Conditions: DHCP server did not send an ACK to the DHCPREQUEST sent by the client.

  Workaround: There is no workaround.

- CSCua31794

  Symptoms: After reload with the debug image, framed E1 lines are down.

  Conditions: On checking the “show controller SONET”, the default controller framing mode is taken as “crc4”. However before reload the configuration for those E1s were configured as “no-crc4”. Customer configured them on the E1s as “no-crc4” and it started working fine and the “show controller SONET” framing output changed to “no-crc4”. As per running configuration still the configuration is not showing “no-crc4”, as it should show as the default is CRC4. So the current issue is configuring “No-crc4”, it is not showing in running configuration and not saved and after reload it shows again CRC4 and services go down again.

  Workaround: Configure E1s as “no-crc4” and they would be working fine, but such changes are not being saved in configuration, so if reload reoccurs all these services go down again.

- CSCua31934

  Symptoms: Crash seen at __be_address_is_unspecified.

  Conditions: The symptom is observed with the following conditions:

  1. It occurs one out of three times, and it is a timing issue.
  2. DMVPN tunnel setup between Cisco 2901 as spoke and Cisco ASR 1000 as hub.
  3. Pass IPv4 and IPv6 traffic between the hub and the spoke for 5-10 minutes.
  4. It can occur with v6 traffic alone.

5. If you remove the tunnel interface on the ASR and add it again using **conf replace nvram:startup-config** the crash will occur.

Workaround: Use CLI to change configuration instead of the rollback feature.

- CSCua33287

  Symptoms: ES+: L2TPv3 entries are programmed incorrectly after restart.

  Conditions: This symptom is observed when some L2TPv3 sessions are established on ES+ module. After the restart of ES+, some np entries may not program correctly. As the result, ES+ will stop to transmit packets.

  This condition will recover after executing **shut/no shut** on physical interfaces.

  Workaround: There is no workaround.

- CSCua33527

  Symptoms: Traceback seen after second or third switchover:

  ```
  %LFD-SW2-3-SMBADEVENT: Unexpected event CO_WAIT_TIMEOUT for state RUNNING -Traceback=
  7908E9Cz 7909848z 79099CCz 7909B9Cz 78DBF20z 523292Cz 522C1D4z
  ```

  Conditions: The symptom is observed with a quad-sup scenario/setup. This traceback is seen on the new active RP after second switchover onwards.

  Workaround: There is no workaround.

- CSCua34033

  Symptoms: Cisco ME 3800x hangs after boot.

  Conditions: It is possible for an Evaluation Scaled license to be configured on the router and scaled services license configured. EULA acceptance can be ignored when configuring this. When the Cisco ME 3800x is rebooted, the router needs to program itself differently for a scaled license than a base license but it cannot do so without the EULA being accepted so the router issues a prompt on the console port. The router will wait here until a user has responded. However, if a user is not on the console port to see this EULA message, they will not know that it is waiting for an EULA response and so the router will continue to wait.

  This is not seen on purchased licenses as they are not installed unless the EULA is accepted.

  Workaround: When using evaluation licenses, accept the EULA upon configuring a license on the router or only reload the router from a connection to the console port after configuring the router to use an evaluation license.

- CSCua37333

  Symptoms: The router displays an EIGRP Active Route in the routing table.

  Conditions: Occurs on the Cisco ASR 1000 with Cisco IOS Releases 15.1(3)S2 and 15.1(3)S3.

  Workaround: There is no workaround.

- CSCua40273

  Symptoms: The Cisco ASR1000 router crashes when displaying MPLS VPN MIB information.

  Conditions: Occurs on the ASR1000 router with Cisco IOS Release 15.1(2)S.

  Workaround: There is no workaround.

- CSCua41398

  Symptoms: The Cisco SUP720 crashes.

  Conditions: Occurs when you issue the sh clns interface | i ^[A-Z]|Number of active command multiple times via script with following error and decodes:

```
%ALIGN-1-FATAL: Corrupted program counter 00:53:22 EET Tue Jun 5 2012
pc=0x0 , ra=0x411514F4 , sp=0x55A8B080

c7600s72033_rp-adventerprisek9-m.122-33.SRE5.symbols.gz read in
Enter hex value: 0x407F5B70 0x407F612C 0x407E026C 0x42BCA588 0x407EDDFC
0x41A78BB8 0x41A78B9C
0x407F5B70:get_alt_mode(0x407f5b68)+0x8
0x407F612C:get_mode_depth(0x407f6118)+0x14
0x407E026C:parse_cmd(0x407ded18)+0x1554
0x42BCA588:parser_entry(0x42bca360)+0x228
0x407EDDFC:exec(0x407ed344)+0xab8
0x41A78BB8:r4k_process_dispatch(0x41a78b9c)+0x1c
0x41A78B9C:r4k_process_dispatch(0x41a78b9c)+0x0
```

Workaround: There is no workaround.

- CSCua42806

  Symptoms: A Cisco RSP720 crashes after a couple of hours traffic passing though MPLS L2VPN VC.

  Conditions: MPLS L2VPN VC setup, with the Cisco 7600 in the MPLS L3 path to the VC endpoints. This issue is seen after several hours of forwarding traffic.

  Workaround: The crash is not seen if the Cisco 7600 terminates the L2 VC.

- CSCua42860

  Symptoms: The standby SUP module displays an “in progress to standby cold-bulk” message and crashes.

  Conditions: Occurs when you an perform an archive configuration.

  Workaround: There is no workaround.

- CSCua43930

  Symptoms: Checksum value parsed from GRE header is not populating causing the GRE tunnel checksum test case to fail.

  Conditions: The issue is seen on a Cisco ISR G2.

  Workaround: There is no workaround.

- CSCua45114

  Symptoms: Default sessions will not establish when you apply VRF as a service to the default policy. VRF can only be applied to a default session by assigning a VRF on the access-interface. However with dedicated sessions, one cannot apply a VRF on the access-interface and VRF transfer at the same time. Thus if we require VRF transfer on dedicated sessions, we need VRF transfer on lite sessions as well.

  Conditions: Access-side interface is in the default VRF, VRF is applied as a service to the default policy.

  Workaround: There is no workaround.

- CSCua46210

  Symptoms: Packets are not decrypted for specific ezvpn client and ping fails.

  Conditions: Occurs while sending traffic, only first 50 ezvpn clients are reachable.

Workaround: There is no workaround.

- CSCua46304

  Symptoms: Crash is seen at __be_nhrp_group_tunnel_qos_apply.

  Conditions: Occurs when flapping a DMVPN tunnel on the hub in a scale scenario.

  Workaround: There is no workaround.

- CSCua48584

  Symptoms: Cisco ME3600X ARP resolution may fail after flexlink switchover

  Conditions: Occurs on Cisco ME3600X that is running Cisco IOS Releases 15.2S or 15.2(2)S1 with flexlink configured.

  Work around: Shut the active port of the flexlink pair, in other words do a manual switchover through CLI.

- CSCua48807

  Symptoms: Complete traffic loss is observed.

  Conditions: Occurs when having queue-limit and default WRED "random-detect" configured in a class and dynamically modify queue-limit of that class.

  Workaround: There is no workaround.

- CSCua49803

  Symptoms: Ingress PE in mvpnv6 setup crashes.

  Conditions: Issue is seen on performing SSO with mvpnv6 sm and ssm traffic for 50 vrfs.

  Workaround: There is no workaround.

- CSCua52289

  Symptoms: CPU Hog is seen on the LC, due to Const2 IPv6 process.

  Conditions: Have 4 core facing tunnels. Upon FRR cutover, observing hog.

  Workaround: There is no workaround.

- CSCua52439

  Symptoms: MLD reports are not received on ES+.

  Conditions: On sending MLD joins on ES+ the reports are not received on the router.

  Workaround: There is no workaround.

- CSCua57585

  Symptoms: CPU utilization increases with XE33 builds.

  Conditions: Occurs when a device forwards traffic on PPPoE connections.

  Workaround: There is no workaround.

- CSCua57728

  Symptoms: Observing traffic loss of ~25s upon doing TE FRR Cutover with IPv6 prefixes.

  Conditions: Have 4 core facing tunnels, 100k IPv6 prefixes. Shut the primary interface and check for the traffic loss.

  Workaround: There is no workaround.

- CSCua57883

  Symptoms: UDLD flaps are reported over the BR Interface when L2TP configuration is done over the 6500.

  Conditions: No known Trigger of the issue. But when this issue is seen it caused the MST to recalculate which eventually lead to the BFD to flap for ISIS and thus causing the network outage.

  Workaround: There is no workaround.

- CSCua58100

  Symptoms: The syslog is flooded with the following traceback message:

  ```
  %SYS-2-NOTQ: unqueue didn't find 7F3D26BDCCD8 in queue 7F3CA5E4A240 -Process= "RADIUS
  Proxy", ipl= 0, pid= 223
  -Traceback= 1#e0ee0ce60492fdd11f0b03e0f09dc812 :400000+873623 :400000+2547652
  :400000+20F9217 :400000+6C70C9C :400000+6C69C71 :400000+6C682BC :400000+6C68183
  ```

  Conditions: Occurs under the following conditions:

  – You establish 36k EAPSIM sessions using a RADIUS client on server A.

  – You establish 36k roaming sessions using a RADIUS client on server B.

  – The roaming sessions have the same caller-station-id but use a different IP address than the EAPSIM sessions.

  Workaround: There is no workaround.

- CSCua60395

  Symptoms: When a IPv6 packet is received via EoMPLS pseudowire, the packet is punted to the CPU and sent pack on the pseudowire.

  Conditions: This has been identified on a Cisco ME3600x with Cisco IOS Release 15.2(1)S1.

  Workaround:

  Option 1: Configure the xconnect under a interface vlan and configure a (dummy) IP address. Example: interface vlan XXX ip address A.B.C.D M.M.M.M xconnect N.N.NN <vc-id> encapsulation mpls

  Option 2: Block IPv6 packets on remote end, so that these packets are not send over pseudowire.

- CSCua61201

  Symptoms: Unexpected reload with BFD configured is seen.

  Conditions: Occurs when a device is configured with BFD it may experience unexpected reloads.

  Workaround: There is no workaround.

- CSCua61814

  Symptoms: Overhead accounting configuration is changed on XE37 image.

  Conditions:

  XE34: overhead accounting configure at parent only

  XE35: overhead accounting configure at parent only

  XE37: overhead accounting need to be configured on both parent and child policy

  Workaround: There is no workaround.

- CSCua63182

  Symptoms: Incorrect minimum bandwidth is displayed when a 0k received.

  Conditions: Different behavior in Cisco ASR code when Min BW of 0 Kbit is received.

```
2.6.2 uses 10 Gbps as Min BW in case Min BW = 0 received
3.4.3 uses 1 Kbit as Min BW in case Min BW = 0 received
```

Workaround: There is no workaround.

- CSCua64546

  Symptoms: In scaled setup with IPV4 and IPV6 ACL together (not necessarily on same interface), IPV4 ACLs may stop working if IPV6 ACL configured later overwrites the ipv4 acl results and vice versa.

  Conditions: Occurs when IPV4 and IPV6 ACLs are configured on the box.

  Workaround: Not perfect workaround, reconfiguring the IPV4 ACL can recover the functionality but will affect the IPV6 ACL.

  Further Problem Description: Only IPV4 or IPV6 ACL configuration will work.

- CSCua64676

  Symptoms: MVPNv4 traffic is not flowing properly from remote PE to UUT.

  Conditions: With Agilent traffic on, after removal/addition of MDT configs for the MVRFs configured on the UUT, MVPNv4 traffic is not flowing properly from remote PE to UUT.

  Workaround: There is no workaround.

- CSCua64700

  Symptoms: IPSec Tunnel States goes to Up-Idle after 4-5 days of router up and running.

  Conditions: If you have low rekey value, the chances of hitting this issue is high, as with the rekey the new spi gets allocated. Seen with WS-IPSEC-3 and to verify this, check the below counter show crypto ace spi.

  If no decrement in spi allocated counter and there the consistent increment in counter, the chances are high, you will hit this issue.

  Once the value reaches to 61439, you will hit this issue.

  ```
  MTCVPNK03#sh cry ace spi
  SPI in use .......................... 0
  Normal SPI allocated ................ 61439
  ```

  Workaround: There is no workaround.

- CSCua76281

  Symptoms: Crash of RSP720-3C-GE @ vc_qos_change is seen.

  Conditions: Device crashes unexpectedly. Last function processed was vc_qos_change.

  Workaround: There is no workaround.

- CSCua80204

  Symptoms: **service instance 1 ethernet myevc** command is not accepted

  Conditions: Occurs if the interface is already attached with xconnect.

  Workaround: There is no workaround.

- CSCua81608

  Symptoms:

  While running 4RURP1 ISSU sub package forwarding run with all feature from XE352/XE36->latest mcp_dev,iosd crashes and router reloads again and again in final ISSU upgrade.

Conditions: Occurs when applying the running config attached in the ddts. Perform an ISSU. Router crashes.

Workaround: There is no workaround.

- CSCua81998

  Symptoms: Doing ISSU RV in Cisco 7600 box with ES40 LC may sometimes cause crash in ES40 LC.

  Conditions: ISSU RV XE3.7 or XE3.8 to XE3.6.1

  Workaround: There is no workaround.

- CSCua84147

  Symptoms: Router crashes during "sh run | format" CLI execution

  Conditions: This crash is seen only during "sh run | format" execution. All other CLI executions are fine.

  Workaround: Avoid executing "sh run | format". Instead "sh run" can be executed.

- CSCua84860

  Symptoms: The device cannot ping a device in a separate VRF.

  Conditions: Occurs when the device is configured as an ISG subscriber and is in a different VRF than the target IP address.

  Workaround: Configure an ACL that permits the IP address range and configure the log keyword.

- CSCua85239

  Symptoms: Flapping BGP sessions are seen with change route-map after/before mpls-ip or mtu be configured:

```
*Jun  3 18:20:20.792 UTC: %TCP-6-BADAUTH: Invalid MD5 digest from 6.6.6.5(179) to
2.2.2.5(17744) tableid - 0

*Jun  3 18:20:30.488 UTC: %TCP-6-BADAUTH: Invalid MD5 digest from 6.6.6.5(179) to
2.2.2.5(17744) tableid - 0

*Jun  3 18:20:36.451 UTC: %BGP-5-ADJCHANGE: neighbor 6.6.6.5 Down BGP Notification
sent

*Jun  3 18:20:36.451 UTC: %BGP-3-NOTIFICATION: sent to neighbor 6.6.6.5 4/0 (hold time
expired) 0 bytes

*Jun  3 18:20:36.569 UTC: %BGP_SESSION-5-ADJCHANGE: neighbor 6.6.6.5 VPNv4 Unicast
topology base removed from session  BGP Notification sent

*Jun  3 18:20:40.184 UTC: %TCP-6-BADAUTH: Invalid MD5 digest from 6.6.6.5(179) to
2.2.2.5(17744) tableid - 0

*Jun  3 18:20:44.619 UTC: %BGP-5-ADJCHANGE: neighbor 6.6.6.5 Up

*Jun  3 18:20:49.926 UTC: %TCP-6-BADAUTH: Invalid MD5 digest from 6.6.6.5(179) to
2.2.2.5(17744) tableid - 0

*Jun  3 18:20:59.604 UTC: %TCP-6-BADAUTH: Invalid MD5 digest from 6.6.6.5(179) to
2.2.2.5(17744) tableid - 0
```

  Conditions: The issue is seen between two BGP peers with matching MD5 passwords configured and can be triggered by:

  1. Removing and re-adding "route-map" with "mpls-ip" configuration for the BGP peering on one side of the peering.

     ```
     conf t

     router bgp A
     ```

```
address-family vpnv4
(no) neighbor x.x.x.x route-map SET-MED out
(no) neighbor y.y.y.y route-map SET-MED out

conf t
interface GigabitEthernet1/2/2
(no) mtu 2000
```

or

2. Removing and re-adding "route-map" with "mtu" configuration for the BGP peering on one side of the peering.

```
conf t
router bgp A
address-family vpnv4
(no) neighbor x.x.x.x route-map SET-MED out
(no) neighbor y.y.y.y route-map SET-MED out

conf t
interface GigabitEthernet1/2/2
(no) mpls ip
```

3. Peering Down and MD5 error do not always occur. Only happens one or two times within 100 tested of (1) and (2).

Workaround: There is no workaround.

- CSCua88341

  Symptoms: Multicast traffic on P2P GRE tunnel will get dropped.

  Conditions: It usually happens in scenarios like SSO is done after vrf del/add. Here the P2P GRE tunnel will be in the VRF.

  Workaround: **shut/no shut** of the P2P GRE tunnel interface.

- CSCua91473

  Symptoms: crypto_kmi_add_data_to_pyld memory leak is seen at IPSEC key engine process.

  Conditions: IPSEC key engine holding memory keeps increasing.

  Workaround: There is no workaround.

- CSCua92557

  Symptoms: The active FTP data channel sourced from the outside may not work as expected. Other protocol inspections that expect pinhole or door for connections initiated from the outside may be affected as well.

  Conditions: This symptom was first identified on the Cisco ASR router running Cisco IOS Release 15.1(3)S3 with VASI+VRF+PAT+FW. This issue is seen when the FTP client is on the inside and the active FTP server is on the outside.

  Workaround: Static NAT will work.

- CSCua94947

  Symptoms: RP crashes when downloading Freeradius Framed-IPv6-Route on MLPPP sessions.

  Conditions: Occurs when downloading radius Framed-IPv6-Route.

  Workaround: There is no workaround.

- CSCua98690

  Symptoms: ES+ Card may crash due to memory corruption.

  Conditions: Occurs when MAC ACL is configured on EFP.

  Workaround: There is no workaround.

- CSCub01238

  Symptoms: Hardware appeared to be incorrectly programmed on ES card.

  Conditions: TE tunnel with FRR.

  Workaround: Once the control plane and data plane get out of sync, the only way to resolve is to tear down the tunnel's LSP.

- CSCub02618

  Symptoms: Cisco 7600 router configured with VFI with RSP720 processor may crash with memory related issues.

  Conditions: Multiple Config/unconfig and SSO.

  Workaround: There is no workaround.

- CSCub02709

  Symptoms: Router crash indicates memory allocation failure.

  Conditions: Occurs when loading router bgp process config with scaled ipv4 and ipv6 address-family neighbors.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.2(4)S

All the caveats listed in this section are resolved in Cisco IOS Release 15.2(4)S. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCej11786

  Symptoms: A Cisco 2600 router reloads when a clear counter is performed on the router. This crash is reproducible only after making a number of calls first.

  Conditions: This symptom has been observed on a Cisco 2600 router.

  Workaround: There is no workaround.

- CSCtj93356

  Symptoms: Batch suspending from platform causes the MFIB on line card to go into reloading state.

  Conditions: This symptom occurs when MFIB on line card goes into reloading state and then finally to purge state after removal/addition of MVRFs is done followed by a line card reset.

  Workaround: There is no workaround.

- CSCtl01184

  Symptoms: Sometimes an EVC that is configured on ES+ sends frames out with CFI bit set in the VLAN tag.

  Conditions: This symptom is observed on EVCs that are configured on ES+.

  Workaround: There is no workaround.

- CSCtl18571

  Symptoms: On a Cisco 7600 series router with etherchannels configured, the **show etherchannel load-balance module** *x* command shows VLAN included even though the excluded VLAN has been configured globally using the **port-channel load-balance** *algorithm* **exclude vlan** command.

  Conditions: This symptom occurs when the system is operating in pfc3c or pfc3cxl mode with CFC and DFC card without per module load-balance.

  Workaround: This is an issue with the **show** command. The algorithm itself is not affected. The load-balancing algorithm is applied correctly as configured globally.

- CSCtr36083

  Symptoms: IKE SAs are not cleared. Ping fails over the IPsec tunnel.

  Conditions: This symptom occurs when SAs are cleared by using the **clear crypto session local** *address* command.

  Workaround: There is no workaround.

- CSCtr93412

  Symptoms: Crash seen on mwheel process.

  Conditions: The symptom is observed with GETVPN multicast followed by **clear crypto gdo**.

  Workaround: There is no workaround.

- CSCts00341

  Symptoms: When executing a CLI that requires domain-name lookup such as **ntp server** *server.domain.com*, the command fails with the following message on the console:

  ```
  ASR1k(config)#ntp server server.domain.com         <<<    DNS is not resolved
  with dual RPs on ASR1k
  Translating "server.domain.com "...domain server (10.1.1.1) [OK]

  %ERROR: Standby doesn't support this command              ^
  % Invalid input detected at '^' marker.

  ASR1k(config)#do sh run | i ntp
  ASR1k(config)#
  ```

  Conditions: This symptom occurs on a redundant RP chassis operating in SSO mode.

  Workaround: Instead of using *hostname* in the command, specify the IP address of the host.

- CSCts12499

  Symptoms: SPA firmware crash at one bay leads to SPA crash in another bay.

  Conditions: This symptom is observed when “test crash cema” is executed from the SPA console. leading to the SPA in the other bay to reload. Also, the crashinfo is not present in the RP disk.

  Workaround: There is no workaround.

- CSCts44393

  Symptoms: A Cisco ASR 1000 crashes.

  Conditions: The symptom is more likely to occur when a large number of VRFs are repeatedly configured and deleted.

  Workaround: There is no workaround.

- CSCts68626

  Symptoms: PPPoE discovery packets causes packet drop.

  Conditions: The symptom is observed when you bring up a PPPoE session and then clear the session.

  Workaround: There is no workaround.

- CSCtt26692

  Symptoms: Router crashes due to memory corruption. In the crashinfo you may see:

  ```
  %SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header, chunk xxxxxxx data
  xxxxxxxx chunkmagic xxxxxxxx chunk_freemagic EF4321CD -
  Process= "CCSIP_SPI_CONTROL", ipl= 0, pid= 374
  chunk_diagnose, code = 1
  chunk name is MallocLite
  ```

  Conditions: Router is configured for SIP. When a translation-rule is configured to translate a number to one with more digits, the router may crash when the translation takes effect, such as when a call is forwarded.

  Workaround: Configuring “no memory lite” configurations can be used as a workaround in some cases (depending on the length of the phone numbers), but will cause the router to use more memory. If the translation-profile is configured to translate forwarded calls, then avoid or disable the option to forward the call.

- CSCtt35379

  Symptoms: BGP Processing Enhancements.

- CSCtt45654

  Symptoms: In a DVTI IPSec + NAT-t scaling case, when doing session flapping continually, several Virtual-Access interfaces are “protocol down” and are not deleted.

  Conditions: This symptom can be observed in a DVTI IPSec + NAT-t scenario when session flapping is done in the spoke side.

  Workaround: There is no workaround.

- CSCtt70133

  Symptoms: The RP resets with FlexVPN configuration.

  Conditions: This symptom is observed when using the **clear crypto session** command on the console.

  Workaround: There is no workaround.

- CSCtt94440

  Symptoms: The Cisco ASR 1000 series router RP may reload.

  Conditions: This symptom is observed when an etoken is in use and the **show crypto eli all** command is issued.

Workaround: Avoid using the **show crypto eli all** command. However, you can use the **show crypto eli** command.

- CSCtu01601

  Symptoms: A Cisco ASR1000 series router may crash while executing the **write memory** command.

  Conditions: This issue may be triggered when the memory in the router is low.

  Workaround: There is no workaround.

- CSCtu14409

  Symptoms: The "Insufficient bandwidth 2015 kbps for bandwidth guarantee" error message is displayed when configuring a policy map with "priority level xxx" and then updating it with "police cir xxx".

  Conditions: This symptom occurs when the priority is configured without a specific rate. This issue is only seen with a Cisco ASR 1000 series router.

  Workaround: Configure police before priority.

- CSCtu23195

  Symptoms: SNMP ifIndex for serial interfaces (PA -4T/8T) becomes inactive after PA OIR.

  Conditions: The symptom is observed with a PA OIR.

  Workaround: Unconfigure and reconfigure the channel-groups of the controller and reload the router.

- CSCtu40028

  Symptoms: The SCHED process crashes.

  Conditions: The issue occurs after initiating TFTP copy.

  Workaround: There is no workaround.

- CSCtu43120

  Symptoms: Service accounting start is not sent for L2TP sessions.

  Conditions: This symptom is observed with L2TP.

  Workaround: There is no workaround.

- CSCtv28434

  Symptoms: GDOI cannot start negative GM re-register timer and prints out traceback at func crypto_gdoi_start_re_register_timer().

  Conditions: The symptom is observed with both IP (v4/v6) GDOI crypto maps configured on the dual-stack interface and GMs re-registration triggered.

  Workaround: Do not trigger GMs to re-register.

- CSCtv36812

  Symptoms: Incorrect crashInfo file name is displayed during crash.

  Conditions: The symptom is observed whenever a crash occurs.

  Workaround: There is no workaround.

- CSCtw46229

  Symptoms: Small buffer leak. The PPP LCP configuration requests are not freed.

  Conditions: The symptom is observed with PPP negotiations and the session involving PPPoA.

Workaround: Ensure all your PPP connections stay stable.

- CSCtw50952

  Symptoms: A Cisco ASR series router crashes due to memory exhaustion after issuing the **clear ip ospf**. This symptom was not observed before issuing this command.

  ```
  ACC-CDC-NET-Pri#sh mem stat
                   Head    Total(b)     Used(b)     Free(b)   Lowest(b)
  Largest(b)
   Processor   30097008   1740862372   279628560   1461233812   1460477804
   1453167736
   lsmpi_io   97DD61D0     6295088     6294120         968         968
     968
  ```

  Conditions: This symptom is observed upon executing the **clear ip ospf** causing tunnel interfaces to flap.

  Workaround: There is no workaround.

- CSCtw53121

  Symptoms: ES+ goes into major state occasionally on reload or SSO.

  Conditions: This issue is seen in the Cisco 7600 router with 40 gig ES+ line card that is running Cisco IOS Release 15.2(2)S.

  Workaround: There is no workaround.

- CSCtw55401

  Symptoms: The SPA-1XCHSTM1/OC3 card goes to out of service after SSO followed by OIR.

  Conditions: This issue is seen with the SPA-1XCHSTM1/OC3 card with Cisco 7600- SIP-200 combination.

  Workaround: There is no workaround.

- CSCtw55424

  Symptoms: SSH with "vrf" in command line for IPv6 addr/host is not working. For example: **ssh -l** *username* **-vrf** *vrfname ipv6 add/host*.

  Conditions: The symptom is observed when **ip ssh source-interface** is not defined and the user specifies the VRF by command line (e.g.: **ssh -l** *username* **-vrf** *vrfname ipv6 add/host*).

  Workaround: Use **ip ssh source-interface** *interface-name* and connect with **ssh -l** *username (IPv4/IPv6)(addr/host)*.

- CSCtw62310

  Symptoms: The **cells** keyword is added to "random-detect" whenever a policy-map is removed from an interface/map-class via "no service- policy".

  Conditions: The symptom is observed when removing the policy-map from map-class.

  Workaround: There is no workaround.

  Further Problem Description: The CLI is technically valid if it has been manually configured as "cells" prior to the removal. The issue is that the template policy is being changed automatically to "cells" whenever the removal happens, regardless of what the original configuration was, and that is not the expected behavior.

- CSCtw70298

  Symptoms: A router crashes after the router boots up with scaled configuration and L2/L3 Distributed EtherChannel (DEC) or port-channel.

  Conditions: This symptom occurs only if there are more than two or more DFCs (ES+ and other equivalents) and with L2/L3 DEC configured such that one of the DFCs takes much longer to come up than the other.

  Workaround: There is no workaround.

- CSCtw73530

  Symptoms: Unable to delete metadata sessions.

  Conditions: This symptom is observed when more than 100 metadata sessions are created.

  Workaround: Disable metadata and then enable it. Note that this will remove all the flows.

- CSCtw79171

  Symptoms: Platform asserts at adjmgr_l2_create.

  Conditions: This symptom occurs with excessive flapping of a link.

  Workaround: There is no workaround.

- CSCtx05726

  Symptoms: When creating a bulk number of traffic engineering tunnel interfaces on the router with option **tunnel mpls traffic-eng exp-bundle master**, the standby route processor crashes.

  Conditions: This symptom is seen with a specific set of configurations which has creation of a large number of tunnel interfaces (scale number 1000) followed by creation of large number of master tunnels (scale number 1000). Copying such a configuration to the router causes this crash on the standby processor.

  The tunnel interfaces which are created at the beginning of the configuration are added as members to the master tunnels in the later part of the configuration. During this phase of creation of the master tunnels and adding member tunnels, these tunnel interfaces go through a cycle of “create-delete-create”. When such a configuration is being synced to the standby route processor along with the resulting create-delete events, the standby processor crashes.

  This point where crash happens is random and can happen during configuration of any of the master tunnels.

  Workaround: There is no workaround. Once the standby reboots after the crash, the configurations on the active are synced to the standby and this sync does not cause any crash. Crash is only during the initial copy of the configurations to the router.

- CSCtx06813

  Symptoms: Installation fails, “rwid type l2ckt” error messages appear, and the VC may fail to come up on Quad-Sup router only. Though this error may appear for multiple other reasons, this bug is specific to Cisco Catalyst 6000 Quad-Sup SSO only.

  Conditions: The symptom is observed in a scaled scenario, doing second switchover on Quad-Sup router.

  Workaround: There is no workaround.

- CSCtx11598

  Symptoms: A router reload causes a Cisco Shared Port Adapter (SPA) failure with the following error message:

  ```
  % CWAN_SPA-3-FAILURE: SPA-2CHT3-CE-ATM[2/2]: SPA failure
  ```

This failure can cause the SPA to go to one of the following states:

- none
- standby reset
- down

This failure leads to unexpected system reload.

Conditions: This symptom is observed during router reload for 15-20 times.

Workaround: Ensure that all of the library shared objects are loaded at the time of the SPA initialization.

- CSCtx32527

  Symptoms: The **show crypto session** command reveals the flexVPN GRE tunnel is in a DOWN state instead of DOWN-negotiating.

  Conditions: The symptom is observed with "ip address negotiated" configured on the GRE tunnel interface (with tunnel protection). The tunnel is unable to reach the gateway initially.

  Workaround: Configure an IP address on the tunnel interface instead of "ip address negotiated".

- CSCtx35064

  Symptoms: Traffic remains on blackholed path until holddown timer expires for PfR monitored traffic class. Unreachables are seen on path, but no reroute occurs until holddown expires.

  Conditions: This symptom is seen under the following conditions:

  - MC reroutes traffic-class out a particular path (BR/external interface) due to OOP condition on the primary path.
  - Shortly after enforcement occurs, an impairment on the new primary path occurs causing blackhole.
  - PfR MC does not declare OOP on the new primary path and attempt to find a new path until Holddown timer expires. Causes traffic loss.

  Workaround: Reduce the holddown timer to 90 seconds (minimum value) to minimize impact.

- CSCtx36095

  Symptoms: A traceback is seen after applying DMLP configurations while doing a line card reload.

  Conditions: This symptom occurs during a line card reload.

  Workaround: There is no workaround.

- CSCtx38121

  Symptoms: IPv6 traffic is not passing through the interface attached with service policy matching IPv6 traffic using IPv6 ACL.

  Conditions: This symptom is observed when attaching a service policy matching IPv6 traffic that is configured using ipv6 access-list on EFP of an interface, which will lead to a traffic drop.

  Workaround: There is no workaround.

- CSCtx47213

  Symptoms: The following symptoms are observed:

  1. Session flap when iBGP local-as is being used on RRs.
  2. Replace-as knob is not working in iBGP local-as case.

Conditions:

1. The session will flap when iBGP local-as is used on the RR client and RR sends an update.
2. Replace-as knob even used is ignored and prefixes are appended with local-as.

Workaround: Do not use iBGP local-as.

- CSCtx57073

  Symptoms: A Cisco router may crash with the following error:

  ```
  "Segmentation fault(11), Process = Metadata HA"
  ```

  Conditions: This symptom is observed while upgrading the router from Cisco IOS XE Release 3.6 to mcp dev.

  Workaround: The required changes have been made with this DDTS to prevent the crash.

- CSCtx62138

  Symptoms: Standby resets continuously due to Notification timer that Expired for RF Client: Cat6k QoS Manager.

  Conditions: This symptom is observed on a Cisco 7600 HA loaded with scale QoS and GRE + IPsec configurations.

  Workaround: There is no workaround.

- CSCtx66046

  Symptoms: The Standby RP crashes with a traceback listing db_free_check.

  Conditions: This symptom occurs when OSPF NSR is configured. A tunnel is used and is unnumbered with the address coming from a loopback interface. A network statement includes the address of the loopback interface. This issue is seen when removing the address from the loopback interface.

  Workaround: Before removing the address, remove the network statement which covers he address of the loopback interface.

- CSCtx67474

  Symptoms: Update message is sent with an empty NLRI when the message consists of 2byte aspath in ASPATH attribute and 4byte value aggregate attribute.

  Conditions: This can happen when there is a mix of 2byte and 4byte attributes in the update message and the message is sent from a 2byte peer and there is a 4byte aggregator attribute.

  Workaround: Move all the 2byte AS peers to a separate update-group using a non-impacting outbound policy like “advertisement-interval”.

- CSCtx73612

  Symptoms: A Cisco ASR 1000 may reload while reading IPsec MIBs via SNMP and write a crashfile.

  Conditions: The symptom is observed on a Cisco ASR 1000 that is running Cisco IOS Release 15.1(1)S1.

  Workaround: Do not poll or trap IPsec information via SNMP.

- CSCtx77501

  Symptoms: Traffic is dropped at decap side of PE box.

  Conditions: This symptom occurs with SSO at decap side of MVPN set-up, DFC core-facing, 6748 access facing.

  Workaround: Do a switchover.

- CSCtx77750

  Symptoms: Crosstalk may be heard by PSTN callers when a call is placed on hold and Music on Hold (MMOH) is enabled.

  Conditions: CUCM is configured to do Multicast MoH.

  Workaround:

  1. Disable H.323 Multicast MoH functionality in IOS or use SIP Multicast MoH.
  2. Use Unicast MoH.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4.3/4.1:

  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:P/I:N/A:N/E:F/RL:ND/RC:C

  CVE ID CVE-2012-1361 has been assigned to document this issue.

  Additional information on Cisco’s security vulnerability policy can be found at the following URL:

  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtx79462

  Symptoms: OSPF neighborship does not get established.

  Conditions: This symptom is observed when Enabling PFC on a multilink bundle in SIP-400. The OSPF neighborship does not get established.

  Workaround: There is no workaround. Disable PFC to bring up the OSPF neighborship.

  Further Problem Description: The OSPF hello packets get dropped by the peer end because the IP header is corrupted.

- CSCtx82775

  Symptoms: Calls on the Cisco ASR 1000 series router seem to be hung for days.

  Conditions: The symptom is observed when MTP is invoked for calls.

  Workaround: Reload the router or perform a no sccp/sccp.

- CSCtx92802

  Symptoms: IP fragmented traffic destined for crypto tunnel is dropped.

  Conditions: The symptom is observed under the following conditions:

  - Cisco IOS Release 15.0(1)M7 on a Cisco 1841.
  - VRF enabled.
  - CEF enabled.
  - VPN tunnel.

  Workaround: Disable VFR or CEF.

- CSCtx95840

  Symptoms: A Cisco voice gateway may unexpectedly reload.

  Conditions: The symptom is observed on a Cisco voice gateway running SIP protocol. In this case the issue was when sipSPIUfreeOneCCB() returns, the leftover event is still being processed after CCB is released from sipSPIUfreeOneCCB(). Based on sipSPIStartRemoveTransTimer(ccb), CCB should have been released later by a background timer.

  Workaround: There is no workaround.

- CSCty01237

  Symptoms: The router logs show:

  ```
  <timestamp> %OER_BR-5-NOTICE: Prefix Learning STARTED
  CMD: 'show run' <timestamp>
  ```

  This is followed by the router crashing.

  Conditions: This issue is seen under the following conditions:

  1. Configure PfR with a learn-list using a prefix-list as a filter and enable learn.
  2. Use a configuration tool, script or NMS that periodically executes **show run** on the MC over HTTP or some other means.

  Workaround 1: If you use PfR learn-list feature, do not execute **show run** periodically.

  Workaround 2: If you use a monitoring tool that executes **show run** periodically, avoid using a learn-list configuration in PfR.

- CSCty03745

  Symptoms: BGP sends an update using the incorrect next-hop for the L2VPN VPLS address-family, when the IPv4 default route is used, or an IPv4 route to certain destination exists. Specifically, a route to 0.x.x.x exists. For this condition to occur, the next-hop of that default route or certain IGP/static route is used to send a BGP update for the L2VPN VPLS address-family.

  Conditions: This symptom occurs when the IPv4 default route exists, that is:

  ```
  ip route 0.0.0.0 0.0.0.0 <next-hop>.
  ```

  Or a certain static/IGP route exists: For example:

  ```
  ip route 0.0.253.0 255.255.255.0 <next-hop>.
  ```

  Workaround 1: Configure next-hop-self for BGP neighbors under the L2VPN VPLS address-family. address-family. For example:

  ```
  router bgp 65000
    address-family l2vpn vpls
     neighbor 10.10.10.10 next-hop-self
  ```

  Workaround 2: Remove the default route or the static/IGP route from the IPv4 routing table.

- CSCty05092

  Symptoms: EIGRP advertises the connected route of an interface which is shut down.

  Conditions: This symptom is observed under the following conditions:

  - Configure EIGRP on an interface.
  - Configure an IP address with a supernet mask on the above interface.
  - Shut the interface. You will find that EIGRP still advertises the connected route of the above interface which is shut down.

  Workaround 1: Remove and add INTERFACE VLAN xx.

  Workaround 2: Clear ip eigrp topology x.x.x.x/y.

- CSCty08070

  Symptoms: Router may print error message and traceback similar to the following example:

  ```
  %SCHED-STBY-3-THRASHING: Process thrashing on watched
  boolean 'OSPFv3 Router
  boolean'. -Process= "OSPFv3R-10/4/2", ipl= 5, pid= 830router ospf
  ```

```
-Traceback= 7235C3Cz 7235F1Cz 6A5F7A8z 6A6168Cz 50DA290z 50D3B44zv
```

Conditions: The symptom is observed when the affected OSPFv3 router is configured, but the process does not run because it has no router-id configured. Further, an area command is configured, for example “area X stub”.

Workaround: Configure “router-id” so the process can run.

- CSCty16620

  Symptoms: Backup pseudowire in SVIEoMPLS does not come up after reloading the router.

  Conditions: This symptom is seen under the following conditions:

  1. Remote PE on the backup PW does not support pseudowire status TLV.
  2. The “no status TLV” is not configured in pw-class used in the PW, which does not support pseudowire status TLV.

  Workarounds:

  Proactive workaround: Configure “no status TLV” into the pw-class used if the remote side does not support status TLV.

  Reactive workaround: Reprovision the backup pseudowire after reload.

- CSCty17288

  Symptoms: MIB walk returns looping OID.

  Conditions: The symptom is observed when a media mon policy is configured.

  Workaround: Walk around CiscoMgmt.9999.

- CSCty23747

  Symptoms: MAC address withdrawal messages are not being sent.

  Conditions: This symptom is seen with flapping REP ports on UPE.

  Workaround: There is no workaround.

- CSCty24606

  Symptoms: Under certain circumstances, the Cisco ASR 1000 series router’s ASR CUBE can exhibit stale call legs on the new active after switchover even though media inactivity is configured properly.

  Conditions: This symptom is observed during High Availability and box to box redundancy, and after a failover condition. Some call legs stay in an active state even though no media is flowing on the new active. The call legs can not be removed manually unless by a manual software restart of the whole chassis. The call legs do not impact normal call processing.

  Workaround: There is no workaround.

- CSCty29230

  Symptoms: CMFIB entries are not being programmed on the SP and DFCs. Mroute shows both Accept and OILS, ip mfib output also shows Accept interface and Forwarding interface, but CMFIB entries are not programmed.

  Conditions: Cisco 7600 running a Cisco IOS Release 15.1(3)S throttle.

  Workaround: There is no workaround.

- CSCty30886

  Symptoms: A standby RP reloads.

Conditions: This symptom is observed when bringing up PPPoE sessions with configured invalid local IP address pool under virtual-template profile and "aaa authorization network default group radius" on the box with no radius present. No IP address is assigned to PPPoE Client.

Workaround: There is no workaround.

- CSCty32463

  Symptoms: When you boot an ASR-1002-X or an ASR-1001 in dual IOSd mode (SSO), the standby process comes up and SSO gets executed but the configuration is unable to sync up between the two processes:

```
%REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a standby insertion
(raw-event=PEER_FOUND(4))
%REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a standby insertion
(raw-event=PEER_REDUNDANCY_STATE_CHANGE(5))

%LICENSE-3-BULK_SYNC_FAILED: License bulk sync operation Priority Sync for
feature adventerprise 1.0 failed on standby rc=Remote tty failed
%ISSU-3-INCOMPATIBLE_PEER_UID: Setting image (X86_64_LINUX_IOSD-UNIVERSALK9-
M),
version (15.2(20120222:153818)156) on peer uid (49) as incompatible
Config Sync: Bulk-sync failure due to Servicing Incompatibility. Please check
full list of mismatched commands via:
  show redundancy config-sync failures mcl

Config Sync: Starting lines from MCL file:
crypto pki certificate chain root-tank.com
 ! <submode> "crypto-ca-cert-chain"

Cannot finish user input data read from fd 17
%RF-5-RF_TERMINAL_STATE: Terminal state reached for (SSO)
kp_perf1>
```

  When this part of the configuration is removed, the issue is not seen:

```
crypto pki certificate chain root-tank.com
! <submode> "crypto-ca-cert-chain"
- ^C
! </submode> "crypto-ca-cert-chain"
```

  Conditions: The position of the ^C is causing the issue.

  Workaround: The starting "^C" should be placed at the same line as "certificate ca". For example:

```
certificate ca ^C
44AFB080D6A327BA893039862EF8406B
 ......
quit^C
```

- CSCty32728

  Symptoms: CPU hog is seen when MVPN configuration is replaced with another using the **configure replace** command.

Conditions: This symptom is observed on a stable MVPN network when replacing the configuration with dual-home receiver/source configuration once the router comes up with the tunnel.

Workaround: There is no workaround.

- CSCty32851

  Symptoms: A Cisco router may unexpectedly reload due to software forced crash exception when changing the encapsulation on a serial interface to "multilink ppp".

  Conditions: The symptom is observed when the interface is configured with a VRF.

  Workaround: Shut down the interface before making the encap configuration change.

- CSCty34020

  Symptoms: A Cisco 7201 router's GigabitEthernet0/3 port may randomly stop forwarding traffic.

  Conditions: This only occurs on Gig0/3 and possibly Fa0/0 as they both are based on different hardware separate from the first three built-in gig ports.

  Workaround: Use ports Gig0/0-Gig 0/2.

- CSCty34200

  Symptoms: In MVPN scale environment, a crash is observed after "no ip multicast-routing". A memory leak is observed after changing data MDT address.

  Conditions: This symptom is seen in MVPN scale scenario.

  Workaround: There is no workaround.

- CSCty35134

  Symptoms: Data traffic out of REP EdgeNoNeighbor fails to flow.

  Conditions: This symptom is observed when MST runs on the node when "rep stcn stp" is configured. If the MST puts this port to BLK then REP EdgeNN stops forwarding traffic.

  Workaround: When having "rep stcn stp" configured on the rep port, we should not have a topology such that MST puts this port to blocking.

- CSCty43587

  Symptoms: Crash observed with memory corruption similar to the following:

  ```
  %SYS-2-FREEFREE: Attempted to free unassigned memory at XXXXXXXX, alloc XXXXXXXX,
  dealloc XXXXXXXX
  ```

  Conditions: The symptom is observed when SIP is configured on the router or SIP traffic is flowing through it.

  Workaround: There is no workaround.

- CSCty48870

  Symptoms: Router crash due to a bus error.

  Conditions: This has been observed in router that is running Cisco IOS Release 15.2(2)T and 15.2(3)T with NBAR enabled on a crypto-enabled interface. NBAR can be enabled through NAT, QoS, or NBAR protocol discovery.

  Workaround: Using **no ip nat service nbar** will help where NBAR is enabled through NAT.

- CSCty49656

  Symptoms: A crash is observed when executing the **no ip routing** command.

  Conditions: This symptom is observed under the following conditions:

  1. Use a Cisco IOS image that has fix for CSCtg94470.

2. Configure OSPF.
3. Enable multicast.
4. Create several (>6000) routes in the network to be learned by OSPF.
5. Wait for OSPF to learn all the (>6000) routes from the network.

Finally, executing the **no ip routing** command may crash the box.

Workaround: There is no workaround.

- CSCty51088

  Symptoms: On a Cisco ME 3600X or Cisco ME 3800X, when traffic for a group (S2,G) is sent to an interface that is already acting as the source for another group (S1,G), it does not receive any traffic since no (S2,G) entry is formed.

  Conditions: This symptom is observed when the receiver interface is already a source interface for another multicast stream.

  Workaround: There is no workaround.

- CSCty53243

  Symptoms: Video call fails in the latest mcp_dev image asr1000rp2-adventerprisek9.BLD_MCP_DEV_LATEST_20120303_065105_2.bin. This image has the uc_infra version: uc_infra@(mt_152_4)1.0.13. Note that video call works fine with the previous mcp_dev image asr1000rp2-adventerprisek9.BLD_MCP_DEV_LATEST_20120219_084446_2.bin.

  Conditions: This symptom is observed when CUBE changes the video port to “0” in 200 OK sent to the UAC.

  Workaround: There is no workaround.

- CSCty54319

  Symptoms: OSPF and protocols using 224.0.0.x will not work btw CE-CE over a VLAN.

  Conditions: This symptom occurs when IGMP snooping is disabled.

  Workaround: Toggle IGMP snooping two times.

- CSCty55449

  Symptoms: The device crashes after registering an Embedded Event Manager TCL policy.

  Conditions: If the policy uses the multiple event feature and the trigger portion is registered without curly braces (“{}”), then the device will crash. For example, this policy will trigger a crash:

  ```
  ::cisco::eem::event_register_syslog tag 1 pattern " pattern1"
  ::cisco::eem::event_register_syslog tag 2 pattern " pattern2"
  ::cisco::eem::trigger
  ::cisco::eem::correlate event 1 or event 2

  namespace import ::cisco::eem::*
  namespace import ::cisco::lib::*

  action_syslog priority crit msg " triggered "
  ```

  Note how “::cisco::eem::trigger” is not followed by an opening curly brace.

  Workaround: Ensure that the trigger portion (i.e.: the correlate statement) is enclosed within curly braces. Given the example above, the proper syntax is:

```
::cisco::eem::event_register_syslog tag 1 pattern " pattern1"
::cisco::eem::event_register_syslog tag 2 pattern " pattern2"
::cisco::eem::trigger {
    ::cisco::eem::correlate event 1 or event 2
}

namespace import ::cisco::eem::*
namespace import ::cisco::lib::*

action_syslog priority crit msg " triggered "
```

- CSCty58241

  Symptoms: The following symptoms are observed:

  Symptom 1. You may receive the following error when you enable radius debugs:

  RADIUS: Response for non-existent request ident

  Symptom 2. The radius alias functionality may not work.

  Conditions:

  For symptom 1: You move from the alias-based configuration to non-alias based configuration and you remove the host first and alias next. In the new configuration if one of the alias becomes the primary host address this will lead to symptom 1.

  For symptom 2: If the reply comes from the alias IP address the functionality may not work.

  Workarounds:

  For symptom 1: - Reload the router; or - Unconfigure the alias first before unconfiguring the host.

  For symptom 2: - Do not use the alias on the NAS.

- CSCty58992

  Symptoms: One-way audio is observed after transfer to a SIP POTS Phone.

  Conditions: This symptom is observed under the following conditions:

  - Cluster is in v6 mode.
  - A call is made from Phone1 to Phone2, and then Phone2 transfers the call to Phone3(SIP POTS), which is when the issue occurs.

  Workaround: There is no workaround.

- CSCty63868

  Symptoms: CUBE crashes at sipSPICheckHeaderSupport.

  Conditions: CUBE crashes while running the codenomicon suite.

  Workaround: There is no workaround.

- CSCty64721

  Symptoms: Improper memory allocation by CTI process crashes the CME.

  Conditions: The CTI front end process is using up huge memory causing the CME to crash eventually. When the crash occurs:

```
Processor Pool Total:  140331892 Used:  140150164 Free:     181728
      I/O Pool Total:   27262976 Used:    5508816 Free:   21754160
```

  Workaround: There is no workaround.

- CSCty68348

  Symptoms: If the OSPF v2 process is configured with the **nsr** command for OSPF nonstop routing, (seen after shutdown/no shutdown of the OSPF process), the neighbor is seen on standby RP as FULL/DROTHER, although the expected state is FULL/DR or FULL/BDR. As a result, after switchover, routes pointing to the FULL/DROTHER neighbor may not be installed into RIB.

  Conditions: This symptom is observed under the following conditions:

  - The OSPF router is configured for “nsr”.
  - Shutdown/no shutdown of the OSPF process.

  Workaround: Flapping of the neighbor will fix the issue.

- CSCty68402

  Symptoms: NTT model 4 configurations are not taking effect.

  Conditions: This symptom occurs under the following conditions:

```
policy-map sub-interface-account
 class prec1
  police cir 4000000 conform-action transmit  exceed-action drop
  account
 class prec2
  police cir 3500000 conform-action transmit  exceed-action drop
  account
 class prec3
  account
 class class-default fragment prec4
  bandwidth remaining ratio 1
  account

policy-map main-interface
 class prec1
  priority level 1
  queue-limit 86 packets
 class prec2
  priority level 2
  queue-limit 78 packets
 class prec3
 bandwidth remaining ratio 1
  random-detect
  queue-limit 70 packets
  class prec4 service-fragment prec4
  shape average 200000
  bandwidth remaining ratio 1
  queue-limit 62 packets
 class class-default
  queue-limit 80 packets
```

  Workaround: There is no workaround.

- CSCty71843

  Symptoms: Tracebacks observed at lfd_sm_start and lfd_sm_handle_event_state_stopped APIs during router bootup.

  Conditions: The symptom is observed with L2VPN (Xconnect with MPLS encapsulation) functionality on a Cisco 1941 router (acting as edge) running Cisco IOS interim Release 15.2(3.3)T. This is observed when a router is reloaded with the L2VPN configurations.

  Workaround: There is no workaround.

- CSCty73817

  Symptoms: In large-scale PPPoE sessions with QoS, the Standby RP might reboot continuously (until the workaround is applied) after switchover. This issue is seen when the QoS Policy Accounting feature is used. When the issue occurs, the Active RP remains operational and the Standby RP reboots with the following message:

  ```
  %PLATFORM-6-EVENT_LOG: 43 3145575308: *Mar 16 13:47:23.482: %QOS-6-RELOAD: Index
  addition failed, reloading self
  ```

  Conditions: This symptom occurs when all the following conditions are met:

  1. There is a large amount of sessions.
  2. The QoS Policy Accounting feature is used.
  3. Switchover is done.

  Workaround: Bring down sessions before switchover. For example, shut down the physical interfaces that the sessions go through, or issue the Cisco IOS command **clear pppoe all**.

- CSCty76106

  Symptoms: Crash is seen after two days of soaking with traffic.

  Conditions: This symptom occurs with node acting as ConPE with multiple services like REP, MST, L3VPN, L2VPN, constant frequent polling of SNMP, RCMD, full scale of routes and bidirectional traffic.

  Workaround: There is no workaround.

- CSCty78435

  Symptoms: L3VPN prefixes that need to recurse to a GRE tunnel using an inbound route-map cannot be selectively recursed using route-map policies. All prefixes NH recurse to a GRE tunnel configured in an encapsulation profile.

  Conditions: This symptom occurs when an inbound route-map is used to recurse L3VPN NH to a GRE tunnel. Prefixes are received as part of the same update message and no other inbound policy change is done.

  Workaround: Configure additional inbound policy changes such as a community change and remove it prior to sending it out.

- CSCty80553

  Symptoms: Multicast router crashes.

  Conditions: The symptom is observed when multicast traffic is routed through an IPsec tunnel and multicast packets are big causing fragmentation.

  Workaround: Make sure that multicast packet sizes do not exceed tunnel transport MTU.

- CSCty81700

  Symptoms: When a remote PE reloads in MVPN network, it causes a memory leak.

Conditions: This symptom occurs when core interface flap or remote PE node reloads causing a small amount of memory leak. If the node stays up experiencing a lot of core interface/remote PE outages, it can run out of memory and fail to establish PIM neighborship with remote PEs.

Workaround: There is no workaround. As a proactive measure, user can periodically (depending on n/w outages) run the **show memory debug leak chunk** command and reload the node, if there are a lot of memory leaks reported by this command.

- CSCty83357

  Symptoms: ACL denied packets are getting punted to host queue, leading to flaps in routing protocols.

  Conditions: This symptom occurs when ACL is configured with src IP match, and packets are being denied by the ACL. The packets are punted to the CPU.

  Workaround: There is no workaround.

- CSCty83520

  Symptoms: IP Phone -- CUCM --- H323 -- 3845 - PSTN:

  1. A call is originated from the IP phone to a PSTN number and it gets connected.
  2. The IP phone puts the call on hold.
  3. The CUCM instructs GW to listen to the Multicast MoH stream.
  4. The Cisco IOS Gateway sends the RTCP packet to Multicast MoH.

  Conditions: This symptom is observed when the H.323 Gateway is configured and the Multicast MoH and MoH stream is sent across an IP Multicast network.

  Workaround 1: Disable the H.323 Multicast MoH functionality in Cisco IOS.

  Workaround 2: Use Unicast MoH.

- CSCty84989

  Symptoms: IKEv2 pushed routes are not installed in the IPv6 inner VRF routing table.

  Conditions: This symptom occurs when using IKEv2 on pure IPV6 tunnels with tunnel protection IPsec and a VRF on the tunnel.

  Workaround: There is no workaround.

- CSCty85926

  Symptoms: VC (VPLS/EoMPLS) will stay down with the following in the **show mpls l2 vc detail** command:

  Signaling protocol: LDP, peer unknown

  Conditions: This symptom will only happen if you have LDP GR configured. Do a SSO switchover and try configuring the VC after the switchover is complete.

  Workaround: There is no workaround. Reload the switch.

- CSCty86111

  Symptoms: The Cisco ISR G2 router crashes after “no ccm-manager fallback-mgcp” is configured.

  Conditions: This symptom is observed with Cisco ISR G2 router.

  Workaround: There is no workaround.

- CSCty90223

  Symptoms: A crash occurs at nhrp_nhs_recovery_co_destroy during setup and configuration.

Conditions: This symptom is observed under the following conditions:

1. Add and remove the ip nhrp configuration over the tunnel interface on the spoke multiple times.
2. Do shut/no shut on the tunnel interface.
3. Rapidly change IPv6 addresses over the tunnel interface on the spoke side and on the hub side multiple times.
4. Replace the original (correct) IPv6 addresses on both the spoke and the hub.
5. Wait for the registration timer to start.

The crash, while not consistently observed, is seen fairly often with the same steps.

Workaround: There is no known workaround.

- CSCty90293

  Processing improvements for GREv6 over IPv6 currently requires IP CEFv6 to be disabled,

  Workaround: Use "tunnel protection" instead,

- CSCty91955

  Symptoms: L2-switched traffic loss within a BridgeDomain routed traffic via an SVI experiences no loss.

  Conditions: This symptom occurs with BridgeDomain that has both tagged and untagged EVCs. Issue should not happen with like-to-like scenario.

  Workaround: Make sure there is like-to-like (tagged-to-tagged or untagged-to- untagged) communication.

- CSCty94289

  Symptoms: The drop rate is nearly 1 Mbps with priority configuration.

  Conditions: This symptom is observed when traffic received in the MSFC router class-default is the same as on the other end of the MSFC2 router.

  Workaround: Unconfigure the priority and configure the bandwidth, and then check for the offered rate in both the routers. This issue is only seen with the Cisco 7600 series routers (since the issue is with the Flexwan line cards). The issue is seen with a priority configuration and does not show up when the priority is unconfigured, so there is no workaround as such for this issue otherwise.

- CSCty96049

  Cisco IOS Software contains a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. An attacker could exploit this vulnerability by sending a single DHCP packet to or through an affected device, causing the device to reload.

  Cisco has released free software updates that address this vulnerability. A workaround that mitigates this vulnerability is available. This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-dhcp

- CSCty96052

  Symptoms: A Cisco router may unexpectedly reload due to Bus error or SegV exception when the BGP scanner process runs. The BGP scanner process walks the BGP table to update any data structures and walks the routing table for route redistribution purposes.

  Conditions: It is an extreme corner case/timing issue. Has been observed only once on release image.

  Workaround: Disabling NHT will prevent the issue, but it is not recommended.

- CSCty96579

  Symptoms: Under periods of transient interface congestion, an MPLS-TP network may experience unnecessary traffic switchovers or longer than expected restoration times.

  Conditions: This symptom is observed during periods of transient interface congestion. Behavior will be caused by loss of vital OAM packets (e.g. AIS/LDI, LKR). Lack of a classification mechanism for these packets prevents from protecting them with a QoS policy.

  Workaround: There is no workaround.

- CSCty97784

  Symptoms: The router crashes.

  Conditions: This symptom is observed when NBAR is enabled, that is, "match protocol" actions in the QoS configuration, or "ip nbar protocol-discovery" on an interface or NAT is enabled and "ip nat service nbar" has not been disabled.

  Workaround: There is no workaround.

- CSCty99331

  Symptoms: CPU hog messages are seen on the console.

  Conditions: This symptom is seen when applying huge rmap with more than 6k sequences on an interface.

  Workaround: There is no workaround.

- CSCty99711

  Symptoms: SIP-400 crash may be observed due to illegal memory access.

  Conditions: This symptom is observed with Cisco IOS Release 12.2(33)SRE4 when SIP-400 has PPPoE session scale.

  Workaround: There is no workaround.

- CSCty99874

  Symptom: Ingress policing is done on the EVC which does not have QoS policy.

  Conditions: This symptom is observed when one EVC has a QoS policy, and another does not. The QoS policy shows effect on the other EVC also.

  Workaround: Attach a dummy policy to the other EVC. Or attach and detach a policy on the other EVC.

- CSCtz01361

  Symptoms: Traffic gets black holed when TE auto-backup is enabled on midpoint router and FFR is configured on the P2MP TE tunnel head end.

  Conditions: This symptom is seen when enabling FRR on the head end with auto- backup already configured on the box.

  Workaround: Remove auto-backup configuration from the midpoint router.

- CSCtz02182

  Symptoms: Tracebacks are seen on a flexVPN hub.

  Conditions: The symptom is observed when adding a virtual-template interface type tunnel.

  Workaround: There is no workaround.

- CSCtz02622

  Symptoms: FlexVPN spoke crashed while passing spoke to spoke traffic.

Conditions: Passing traffic from spoke to spoke or clearing IKE SA on the spoke.

Workaround: There is no workaround.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.1/5:

https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:M/C:N/I:N/A:C/E:F/RL:OF/RC:C

CVE ID CVE-2012-3893 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtz04090

  Symptoms: In a VRRP/HSRP setup, traffic from particular hosts is getting dropped. Ping from the host to any device through the VRRP routers fails.

  Conditions: This symptom is usually seen after a VRRP/HSRP switchover. The packet drops because of some packet loop that is created between the routers running VRRP/HSRP.

  Workaround: A clear of the MAC table on the new VRRP master usually restores the setup to working conditions.

- CSCtz06611

  Symptoms: IPSec tunnel states are UP-IDLE because of broadcast packets that are punted to the CPU. The mac-address of VPN-SPA is not learned properly.

  Conditions: This symptom is a timing issue. You may see it first time or need to try multiple times. This symptom is seen with crypto map plus vrf configuration.

  1. Reload the router with above configuration: the mac-address changes to all FF.
  2. Default the configuration of VLAN (where crypto map and engine is applied), then configure it again with old configuration. Now the mac-address will show all FF.
  3. Create the vlan. Do a **no shutdown**. Attach vrf. Then add crypto map to it.

  Workarounds: For the steps mentioned in condition section above, below are the workarounds respectively.

  Workaround 1: Remove and add "ip vrf forwarding" and then remove and add the **crypto engine** command.

  Workaround 2: Remove and add the **crypto engine** command.

  Workaround 3: Do a **shut/no shut** on the VLAN interface.

- CSCtz08037

  Symptoms: The router fails to pass any traffic after receiving the "%OCE-3-OCE_FWD_STATE_HANDLE: Limit of oce forward state handle allocation reached; maximum allowable number is 50000" error message.

  Conditions: This symptom is observed MPLS L2VPN is configured with EoMPLSoGRE with IPSec encryption on top of the VTI tunnel with IPSec encryption (double encryption).

  Workaround: Reload the router.

- CSCtz08719

  Symptoms: With split horizon, traffic does not flow on all BDs.

  Conditions: This symptom is observed when traffic does not flow on all BDs.

  Workaround: There is no workaround.

- CSCtz08746

  Symptoms: On the 12in1 Serial SPA with hardware version lower than 2.0, an upgrade using "test upgrade" with the latest Cisco 7600 FPD bundles results in the SPA FPD device being downgraded from version 1.2 to 1.1. Subsequently, both auto and manual upgrades fail to bring the SPA FPD version back to 1.2. The SPA goes to the OutOfServ or FpdUpReqd state.

  Conditions: This issue is seen only with the older SPA hardware (hardware version lower than 2.0) when it is plugged into a SIP200 or SIP400 on the Cisco 7600 platform.

  Workaround: Use the latest SPA hardware (hardware version 2.0 or above).

- CSCtz12714

  Symptoms: A Cisco router configured for voice functions may crash.

  Conditions: The exact conditions to trigger the crash are unknown at this time.

  Workaround: There is no workaround.

- CSCtz13451

  Symptoms: A Cisco ME 3800X and Cisco ME 3600X switch may experience CPU HOG errors and then a watchdog crash or memory corruption.

  Conditions: This symptom is observed when running many of the **show platform mpls handle** commands. The switch may crash.

```
SW#sh platform mpls handle 262836664 ?
  BD_HANDLE              bd/el3idc_vlan handle
  L2VPN_L2_HANDLE        l2 tunnel intf handle
  L2VPN_PW_BIND_DATA     pw bind data
  LFIB_TABLE             LFIB TABLE handle
  PORT_HANDLE            port/met handle
  RW_HANDLE              Rewrite handle
  SW_OBJ_ADJACENCY       oce type SW_OBJ_ADJACENCY
  SW_OBJ_ATOM_DISP       oce type SW_OBJ_ATOM_DISP
  SW_OBJ_ATOM_IMP        oce type SW_OBJ_ATOM_IMP
  SW_OBJ_DEAGGREGATE     oce type SW_OBJ_DEAGGREGATE
  SW_OBJ_EGRESS_LABEL    oce type SW_OBJ_LABEL
 SW_OBJ_EOS_CHOICE      oce type SW_OBJ_EOS_CHOICE
  SW_OBJ_FIB_ENTRY       oce type SW_OBJ_FIB_ENTRY
  SW_OBJ_FRR             oce type SW_OBJ_FRR
  SW_OBJ_GLOBAL_INFO     oce type SW_OBJ_GLOBAL_INFO
  SW_OBJ_ILLEGAL         oce type SW_OBJ_ILLEGAL
  SW_OBJ_IPV4_FIB_TABLE  oce type SW_OBJ_IPV4_FIB_TABLE
  SW_OBJ_IPV6_FIB_TABLE  oce type SW_OBJ_IPV6_FIB_TABLE
  SW_OBJ_LABEL_ENTRY     oce type SW_OBJ_LABEL_ENTRY
  SW_OBJ_LABEL_TABLE     oce type SW_OBJ_LABEL_TABLE
  SW_OBJ_LOADBALANCE     oce type SW_OBJ_LOADBALANCE
  SW_OBJ_RECEIVE         oce type SW_OBJ_RECEIVE
```

  Workaround: Do not run the commands as they are for development use.

- CSCtz13818

  Symptoms: In a rare situation when route-map (export-map) is updated, IOS is not sending refreshed updates to the peer.

  Conditions: The symptom is observed when route-map (export-map) is configured under VRF and the route-map is updated with a new route-target. Then the IOS does not send refreshed updates with modified route-targets.

  Workaround 1: Refresh the updated route-target to use **clear ip route vrf** *vrf-name net mask*.

  Workaround 2: Hard clear the BGP session with the peer.

- CSCtz14634

  Symptoms: Negative "maximum reservable bandwidth" and "priority" values are seen on the opaque-lsa for Bundle-Ether[2*10GE]interface.

  Conditions: This symptom is observed on the Bundle-Ether[2*10GE]interface.

  Workaround: There is no workaround. The error is only in the way the values are displayed by **show** commands. The correct bandwidth values are sent in the opaque LSA, and this error has no operational effect.

- CSCtz14980

  Symptoms: When you perform the RP switch, the standby RP (original active one) will keep rebooting.

  Conditions: The symptom is observed when you have "crypto map GETVPN_MAP gdoi fail-close" configured and image is Cisco IOS XE Release 3.6 or 3.7.

  Workaround: There is no workaround.

- CSCtz15211

  Symptoms: The ISM card does not encrypt packets through a double encrypted tunnel.

  Conditions: This symptom is observed with ISR g2 with the ISM module and crypto configured for GRE over IPsec packets to be encrypted through a VTI (double encryption).

  Workaround: Use onboard encryption.

- CSCtz16622

  Symptoms: A Cisco ME 3600X acts as a label disposition Edge-LSR when receiving MPLS packets with Checksum 0xFFFF that will continue to drop with Ipv4HeaderErr and Ipv4ChecksumError at nile.

  Conditions: This symptom is seen with label pop action at the Edge-LSR.

  Workaround: There is no workaround.

- CSCtz22112

  Symptoms: A VXML gateway may crash while parsing through an HTTP packet that contains the "HttpOnly" field:

  ```
  //324809//HTTPC:/httpc_cookie_parse: * cookie_tag=' HttpOnly'
  //324809//HTTPC:/httpc_cookie_parse: ignore unknown attribute: HttpOnly
  ```

  ```
  Unexpected exception to CPU: vector D, PC = 0x41357F8
  ```

  Note: The above log was captured with "debug http client all" enabled to generate additional debugging output relevant to HTTP packet handling.

  Conditions: The symptom is observed when an HTTP packet with the "HttpOnly" field set is received.

Workaround: There is no workaround.

- CSCtz23433

  Symptoms: ISG shell maps with policer on egress child default-class fail.

  Conditions: This symptom is seen with shell map with policer or shaper on child default-class.

  Workaround: There is no workaround.

- CSCtz24047

  Symptoms: Free process memory is being depleted slowly on line cards in the presence of the DLFIoATM feature configured on a PA-A6-OC3 (enhanced Flexwan). Finally memory allocation failures are observed. Use the **show memory proc stat history** command to display the history of free process memory.

  Conditions: Slow Proc Memory depletion is observed on 7600-ES+ cards when installed on a Cisco 7600 router that has DLFIoATM configured on a PA-A6-OC3 hosted on an enhanced Flexwan module.

  Workaround: There is no workaround.

- CSCtz25953

  Symptoms: "LFD CORRUPT PKT" error message is dumped and certain length packets are getting dropped.

  Conditions: The symptom is observed with a one-hop TE tunnel on a TE headend. IP packets with 256 or multiples of 512 byte length are getting dropped with the above error message.

  Workaround: There is no workaround.

- CSCtz26188

  Symptoms: Packet loss is observed on platforms in certain deployments having a large number of prefixes routing traffic onto a TE tunnel.

  Conditions: If the Configured value of the cleanup timer is 60 secs, then packets might be lost on the platforms where the forwarding updates take longer.

  Workaround: Configure the value of the cleanup timer to 300secs.

  mpls traffic-eng reoptimize timers delay cleanup 300

- CSCtz27782

  Symptoms: A crash is observed on defaulting service instance with OFM on EVC BD configured.

  Conditions: This symptom occurs when interface is in OAM RLB slave mode.

  Workaround: There is no workaround.

- CSCtz30983

  Symptoms: Crash on ES+ line card upon issuing the "show hw-module slot X tech- support" or "show platform hardware version" command.

  Conditions: This symptom occurs on an ES+ line card.

  Workaround: Do not issue the **show hw-module slot X tech-support** or **show platform hardware version** command on an ES line card unless explicitly mentioned by Cisco.

- CSCtz31888

  Symptoms: After state change of one of the L3 uplink interfaces, STP cost of BPDU PW increases from 200 to 2M, which can lead to blocking state in STP for this PW.

  Conditions: This symptom occurs with state change of one of the uplink L3 interfaces.

Workaround: Increase the cost of access ring to more then 2M to avoid blocking of the BPDU PW.

- CSCtz32521

  Symptoms: In interop scenarios between Cisco CPT and Cisco ASR 9000 platforms, in order to support transport switchover requirement for 50 msec, it would require Cisco ASR 9000 or PI code to allow configuration or negotiation of minimal interval timer to 2.

  Conditions: This symptom occurs in interop scenarios between Cisco CPT and Cisco ASR 9000 platform. In order to support transport switchover requirement for 50 msec, it would require Cisco ASR 9000 or PI code to allow configuration or negotiation of minimal interval timer to 2.

  Workaround: There is no workaround.

- CSCtz33536

  Symptoms: SIP KPML subscription fails with:

  ```
  ?xml version="1.0" encoding="UTF-8"?><kpml-response version="1.0" code="533"
  text="Multiple Subscriptions on a Dialog Not Supported"/
  ```

  This happens on a CUBE when the call is transferred on CUCM.

  Conditions: The symptom is observed with SIP to SIP CUBE running Cisco IOS Release 15.1(3)T2.

  Workaround: Use a different DTMF method.

- CSCtz35061

  Symptoms: Flexlink switchover causes VLAN to not be allowed in trunk link.

  Conditions: This issue is related to flexlink switchover caused by instantaneous link flapping.

  Workaround: There is no workaround.

- CSCtz35467

  Symptoms: QoS policy-map gets detached from interface on line protocol down-- >up transition happens on reload, admin shut/no shut and interface flap as well.

  Conditions: This symptom is observed when QoS policy-map is applied at interface and more than one child has “priority + police cir percent x” configured.

  Workaround: To be preventive use “police cir <absolute>” instead of “police cir percent x”. To be reactive use EEM applet/script.

  Further Problem Description: There is no error message in the syslog, only on console. It seems that line protocol UP can be used as the trigger action for EEM.

- CSCtz37863

  Symptoms: IPCP is not in an open state and it does not seem to be calling the This-Layer-Down (TLD) vector.

  Conditions: The symptom is observed if IPv4 saving is enabled and IPCP negotiation failed because of a TermReq received from peer.

  Workaround: There is no workaround.

- CSCtz38119

  Symptom: The router does not complete a MAC address flush on the receiving side of a VPLS pseudowire.

  Conditions: Occurs when the router receives a layer 2 MAC withdrawal over a VPLS pseudowire.

  Workaround: There is no workaround.

- CSCtz40435

  Symptoms: The L4 port-range security ACL does not work on EVC.

  Conditions: This symptom is seen when security ACL containing L4 port range operation that is applied on EVC. The behavior is not as expected. The same works on physical interface.

  Workaround: Add support for L4 port range operation similar to the case of applying it on physical interface.

  PSIRT Evaluation: The Cisco PSIRT has evaluated this issue and does not meet the criteria for PSIRT ownership or involvement. This issue will be addressed via normal resolution channels.

  If you believe that there is new information that would cause a change in the severity of this issue, please contact psirt@cisco.com for another evaluation.

  Additional information on Cisco's security vulnerability policy can be found at the following URL:

  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtz40621

  Symptoms: Router crash observed.

  Conditions: The symptom is observed when GetVPN GM tries to register to keyserver and keyserver issues a rekey simultaneously.

  Workaround: There is no workaround.

- CSCtz41048

  Symptoms: The **trace mpls ipv4** command is unsuccessful.

  Conditions: The symptom is observed with the **trace mpls ipv4** command.

  Workaround: There is no workaround.

- CSCtz45057

  Symptoms: High CPU is seen on a Cisco ME 3800X switch.

  Conditions: This symptom occurs when loop of OTNIFMIB causes CPU Hog/Crash on a Cisco ME 3800X switch during pulling from PPM.

  Workaround: Disable OTNIFMIB while pulling from PPM, which is not supported or required on Cisco ME 3800X and ME 3600X switches.

- CSCtz45487

  Symptoms: REP flaps when modifying allows VLANs on REP enabled trunk.

  Conditions: This symptom is seen under the following conditions:

  - "vlan dot1q tag native" must be configured globally.
  - Issue does not occur when native VLAN is 1 on REP trunk.
  - Issue is seen on Cisco IOS Releases 15.2(2)S, 15.1(2)EY2a and earlier Cisco IOS 15.1(2)S releases.
  - Issue is not seen on Cisco IOS Release 12.2(52)EY4 and earlier Cisco IOS 12.2(52)EY releases.

  Workaround:

  - Remove "vlan dot1q tag native" global configuration.
  - Change to native VLAN 1 on the REP enabled trunks.
  - Change to Cisco IOS Release 12.2(52)EY.

- CSCtz45901

  Symptoms: The **show runn** or **format xml** output for an ATM interface is not displayed in the correct order.

  Conditions: The symptom is observed if there are multiple subinterfaces for an ATM interface and PVC is configured under these.

  Workaround: There is no workaround.

- CSCtz46300

  Symptoms: Traffic is not classified under the QoS ACLs having port matching using range (inclusive range), lt (less than), and gt (greater than) operators.

  Conditions: This symptom is seen with IPv4 and IPv6 with L4 port ranger operations using range, lt, and gt, which do not work with QoS ACLs on Cisco ME 3600 and Cisco ME3800 switches.

  Workaround: There is no workaround.

- CSCtz47873

  Symptoms: The command **show crypto ikev2 client flex** does not work as expected.

  Conditions: The symptom is observed with a client/server flexVPN setup.

  Workaround: Execute either **show crypto IKEv2 sa** or **show crypto session detail**.

- CSCtz48615

  Symptoms: AES encryption may cause high CPU utilization at crypto engine process.

  Conditions: The symptom is observed with AES encryption configuration in ISAKMP policy. The issue is seen only when one of the negotiating routers is a non-Cisco device where the key size attribute is not sent in ISAKMP proposal.

  Workaround: Remove ISAKMP policy with AES encryption.

- CSCtz54823

  Symptoms: Configuration is getting locked on chopper SPA.

  Conditions: This symptom happens as follows:

  1. Shut down the controller of the SPA.
  2. Reload will bring the SPA in the locked state.

  Workaround: There is no workaround. Erase start up and reload the system to get back to configuration mode.

- CSCtz59429

  Symptoms: Packets do not match a flow with the attribute “application category voice-video”.

  Conditions: This symptom occurs when a flow with the attribute “application category voice-video” is matched for the same attribute.

  Workaround: There is no workaround.

- CSCtz62680

  Symptoms: “DFC WAN Line Card Software Element Not Found - QOS: TCAM Class ID” errors appear along with BADCHUNKFREEMAGIC errors, leading to an ES20 crash.

  Conditions: When service policies less than 128 kb are added or removed.

  Workaround: There is no workaround.

- CSCtz66770

  Symptoms: When under ATM PVC (SPA-4XOC3-ATM or v2) with MUX encapsulation and OAM enabled, L3 policy-map is applied and PVC goes down.

  Conditions: This symptom occurs when policy-map sets DSCP (to 7) for default- class, and it affects OAM communication.

  Workaround: Use aal5snap encapsulation.

- CSCtz67403

  Symptoms: A Cisco ME 3600 switch as core switch is dropping all BPDU coming in QnQ tunnel.

  Conditions: This symptom occurs on a Cisco ME 3600 switch that is the core, and the Cisco ME 3400 switches are edge switches.

  Workaround: There is no workaround.

- CSCtz67726

  Symptoms:

  1. Single probe ID is not permitted on the **ip sla group schedule...** command. For example: **ip sla group schedule** *group id* **schedule-period 5 start now** gives following error messages:

     ```
     %Group Scheduler: probe list wrong syntax
     ```

     ```
     %Group schedule string of probe ID's incorrect
     ```

  2. Entering the same probe ID under **ip sla group schedule** in the format of “id,id” is accepted but it will display on the running configuration as just single probe ID. For example: **ip sla group schedule** *group* **id,id schedule-period 5 start now**. The running configuration will show **ip sla group schedule** *group* **id schedule-period 5 start now**.

  Conditions: Observed if using single probe ID under **ip sla group schedule...** command.

  Workaround: Use the command **ip sla schedule** for single probe ID.

- CSCtz72044

  Symptoms: EzVPN client router is failing to renew ISAKMP security association, causing the tunnel to go down.

  Conditions: The issue is timing-dependent, therefore the problem is not systematic.

  Workaround: There is no workaround.

- CSCtz72390

  Symptoms: The name mangling functionality is broken. Authorization fails with the “IKEv2:AAA group author request failed” debug message.

  Conditions: This symptom is observed with Cisco IOS Release 15.2(3)T.

  Workaround: There is no workaround.

- CSCtz72615

  Symptoms: All interfaces on a Cisco 7600-SIP-200 are down after Cisco IOS downgrade.

  Conditions: This symptom is observed on Cisco 7600 series routers.

  Workaround: There is no workaround.

- CSCtz73157

  Symptoms: CUBE sends 0.0.0.0 when 9971 has video enabled for hold/resume/conference from PSTN caller. CUBE sends correct IP address when 9971 has video disabled for hold/resume/conference from PSTN caller.

Conditions: The symptom is observed with the following conditions:

- Cisco IOS Release 15.2(2)T1.
- Current phone load sip99719.2.4-19.
- Current CUCM version: 8.5.1.13900-5.
- MCS7825I4-K9-CMD2A.
- On the SIP trunk, the box "Retry Video Call as Audio" was checked.

For the calls with video disabled, the CUBE is sending the 200OK with the C=IN ipX x.x.x.x address.

```
Sent:
SIP/2.0 200 OK
Via: SIP/2.0/TCP x.x.x.x:5060;branch=z9hG4bK7322e28fb58f2
From: "name"
<sip:2127153896@x.x.x.x>;tag=1171271~17954349-bc2a-4081-adb4-34491012bb45-24984725
To: <sip:16464831236@x.x.x.x>;tag=D99A474-A1A
Date: Tue, 24 Apr 2012 18:26:17 GMT
Call-ID: f9e43000-f961f049-61593-a28050a@x.x.x.x
CSeq: 101 INVITE
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE,
NOTIFY, INFO, REGISTER
Allow-Events: telephone-event
Remote-Party-ID: <sip:16464831236@x.x.x.x>;party=called;screen=no;privacy=off
Contact: <sip:16464831236@x.x.x.x:5060;transport=tcp>
Supported: replaces
Supported: sdp-anat
Server: Cisco-SIPGateway/IOS-15.2.2.T1
Supported: timer
Content-Type: application/sdp
Content-Disposition: session;handling=required
Content-Length: 241

v=0
o=CiscoSystemsSIP-GW-UserAgent 9798 5431 IN IPX x.x.x.x
s=SIP Call
c=IN IPX x.x.x.x
t=0 0
m=audio 25014 RTP/AVP 0 101
c=IN IPX x.x.x.x
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
```

For the calls with video enabled, the CUBE is not sending the IP address correctly, as seen here:

```
Sent:
SIP/2.0 200 OK
```

```
Via: SIP/2.0/TCP x.x.x.x:5060;branch=z9hG4bK734ab4c88ccb9
From: "name"
<sip:2127153896@x.x.x.x>;tag=1171897~17954349-bc2a-4081-adb4-34491012bb45-24984949
To: <sip:16464831236@x.x.x.x>;tag=DA1D53C-2232
Date: Tue, 24 Apr 2012 18:35:25 GMT
Call-ID: 39f7e280-f961f262-616f4-a28050a@x.x.x.x
CSeq: 102 INVITE
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE,
NOTIFY, INFO, REGISTER
Allow-Events: telephone-event
Remote-Party-ID: <sip:16464831236@x.x.x.x>;party=called;screen=no;privacy=off
Contact: <sip:16464831236@x.x.x.x:5060;transport=tcp>
Supported: replaces
Supported: sdp-anat
Server: Cisco-SIPGateway/IOS-15.2.2.T1
Supported: timer
Content-Type: application/sdp
Content-Length: 278

v=0
o=CiscoSystemsSIP-GW-UserAgent 144 2583 IN IPX x.x.x.x
s=SIP Call
c=IN IPX 0.0.0.0
t=0 0
m=audio 16654 RTP/AVP 0 101
c=IN IPX 0.0.0.0
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
m=video 0 RTP/AVP 126
c=IN IPX 10.5.40.14
```

Workaround: Disable video from CUCM phone page under the 9971.

- CSCtz74189

  Symptoms: Occasionally the system hangs at bootup with the following signature in the bootlogs. The system will not respond to break character keys.

  ```
  Configuring Freq Synthesizer 2^M
  Synthesizer PLL 2 locked successfully^M
  Configuring Freq Synthesizer 3^M
  Synthesizer PLL 3 locked successfully^M
  Configuring Freq Synthesizer 4^M
  Synthesizer PLL 4 locked successfully^M
  TDM Processor has been configured in iter(1)^M <<<<<<<<<<<< HANG
  ```

  Conditions: This symptom occurs in normal reload conditions, or on a next reload of the software after a system power cycle.

Workaround: Requires a system power cycle.

- CSCtz74685

  Symptoms: A router crash is observed on Y1731 DM.

  Conditions: This symptom is seen when starting 1DM session.

  Workaround: There is no workaround.

- CSCtz75228

  Symptoms: On a power cycle or a reload condition, the system may stall occasionally after the following console logs are printed.

```
<snip
Finished memctrl.h, apply WinHMS Errata...
Initialize Winpath
Initializing interrupt controller
Initialization of Winpath Complete
loading program at addr: 0xE2C00000, size: 0x0007A648
Enable the MIPS Core0
Before minimon_init() call... <<<<<<<<<<<HANG
-----  minimon 1st 64 bytes ------
C00BD108:
```

  Conditions: This symptom may happen during a system reload.

  Workaround: A power cycle is required, and the subsequent reload may not be impacted.

- CSCtz75380

  Symptoms: A Cisco ASR 1000 series router sends malformed radius packets during retransmission or failover to a secondary radius server, e.g.: Cisco CAR.

  ISG log if secondary radius server is installed in the network:

```
Radius-Server Log:
13:23:01.011: P78: Packet received from 10.0.0.1
13:23:01.011: P78: Packet successfully added
13:23:01.011: P78: Parse Failed: Invalid length field - 63739 is greater than 288
13:23:01.011: Log: Packet from 10.0.0.1: parse failed <unknown user>
13:23:01.011: P78: Rejecting Request: packet failed to parse
13:23:01.011: P78: Trace of Access-Reject packet
13:23:01.011: P78:    identifier = 40
13:23:01.011: P78:    length = 21
13:23:01.011: P78:    reqauth = 23:<snip....>
13:23:01.011: P78: Sending response to 10.0.0.1
13:23:01.011: Log: Request from 10.0.0.1: User <unknown user> rejected
(MalformedRequest).
13:23:01.011: P78: Packet successfully removed
```

  Conditions: The issue can occur during retransmission of radius access requests or if radius packets are sent to a secondary radius server.

  Workaround: There is no workaround.

- CSCtz76650

  Symptoms: In phase 2 IPv6 DMVPN deployment, traffic for IPv6 hosts behind spokes goes via the hub.

  Conditions: This symptom is observed in IPv6 DMVPN network when using phase 2 configuration and routing protocols with link-local nexthop.

  Workaround: Do not use link-local nexthop routing, instead use unicast nexthops (e.g.: BGP as the routing protocol).

- CSCtz77171

  Symptoms: Subscriber drops are not reported in mod4 accounting.

  Conditions: This symptom is observed on checking policy-map interface for account QoS statistics on a port-channel subinterface.

  Workaround: There is no workaround.

- CSCtz78194

  Symptoms: A Cisco ASR 1000 that is running Cisco IOS XE Release 3.6 or Cisco IOS Release 15.2(2)S crashes when negotiating multi-SA DVTI in an IPsec key engine process.

  Conditions: The symptom is observed with the Cisco ASR configured to receive DVTI multi-SA in aggressive mode and hitting an ISAKMP profile of a length above 31.

  Workaround: Shorten the ISAKMP profile name to less than 31.

- CSCtz80643

  Symptoms: A PPPoE client's host address is installed in the LNS's VRF routing table with the **ip vrf receive** *vrf name* command supplied either via RADIUS or in a Virtual-Template, but is not installed by CEF as attached. It is instead installed by CEF as receive, which is incorrect.

  Conditions: This symptom is observed only when the Virtual-access interface is configured with the **ip vrf receive** *vrf name* command via the Virtual-Template or RADIUS profile.

  Workaround: There is no workaround.

- CSCtz83311

  Symptoms: In the bootlog, the following strings may be observed:

  ```
  "MCB timeout"
  ```

  Occasionally these messages also are followed by a GigE port link down for any of the ports Gig 0/1-Gig 0/8. A **shut/no shut** may not recover the link down condition.

  Conditions: This symptom happens during a system reload. It may also happen if a **media-type** command is issued to the first eight GigE ports.

  Workaround: Do not configure "media-type rj45" for the first eight ports either at bootup time or configurations if you are using an image that does not have this fix.

- CSCtz85907

  Symptoms: A Cisco 7600 should have an MVPNv4 configuration and the system replication mode as egress. Now if "address-family ipv6" is configured under the VRF definition, MVPN traffic might be affected.

  Conditions: SREx and RLSx releases.

  Workaround: Use ingress replication.

- CSCtz86024

  Symptoms: There is a long delay in joining mcast stream with Cisco IOS 15S releases that are running on RP.

  Conditions: This symptom is seen when there is no (*,G) on the box, and the first packet for the stream creates this entry.

  Workaround: With static joins we can make sure that entry is present in mroute table.

- CSCtz86747

  Symptoms: Router crashes upon removing all the class-maps from policy-map.

  Conditions: This symptom is observed when a route crashes while removing all user defined class-maps with live traffic.

  Workaround: Shut the interface first before removing class-map.

- CSCtz86763

  Symptoms: Sessions remain partially created, and memory is consumed and not returned.

  Conditions: This symptom occurs when sessions are churned and reset before they reach active state.

  Workaround: There is no workaround.

- CSCtz88289

  Symptoms: It is observed that in a Cisco ME 3600-24CX unit, which is subjected to 100 consecutive image reloads, there is a system bootup hang in this area. The system stalls indefinitely and does not respond to console keystrokes like break keys.

  ```
  <bootup snip>

   I2C Bus Initialization begins
   Margining CPU and Nile board Voltages
   Control FPGA Initialization begins  <<<<System  Hang here
  ```

  Conditions: This symptom may happen during a system bootup.

  Workaround: A powercycle is required, and the next reload may not hit the above condition.

- CSCtz89608

  Symptoms: A router that is operating in an ISG environment experiences a crash due to memory corruption.

  Conditions: This symptom occurs within the SSS context.

  Workaround: There is no workaround.

- CSCtz90154

  Symptoms: Rapid getVPN re-registration by GM when IPsec failure occurs during initial registration. Multiple ISAKMP SAs created and deleted per second.

  Conditions: The symptom is observed on a Cisco ASR 1000 that is running Cisco IOS Release 15.2(1)S or Release 15.2(1)S2 as a GM.

  Workaround: There is no workaround.

- CSCtz90909

  Symptoms: A router crashes while giving the **no l2 vfi** *vfi-name* **point-to-point** command.

  Conditions: This symptom occurs while unconfiguring l2 vfi. The router crashes.

  Workaround: There is no workaround.

- CSCtz94188

  Symptoms: With AdvancedMetroIPAccess evaluation license and with TDM permanent license xconnect under CEM, ckts are not shown and are not configurable.

  Conditions: This symptom occurs under regular configuration steps.

  Workaround: There is no workaround.

- CSCtz96342

  Symptoms: Inconsistency in scaled feature license name between Cisco IOS Releases 12.2(52)EY*/15.1(2)EY* and Cisco IOS Release 15.2(2)S:

  Cisco IOS Releases 12.2(52)EY*/15.1(2)EY* - ScaledServices

  Cisco IOS Release 15.2(2)S - ScaledMetroAggrServices

  Conditions: This symptom occurs with an upgrade from Cisco IOS Releases 12.2 (52)EY*/15.1(2)EY* to Cisco IOS Release 15.2(2)S release, which could impact the scalability feature in below ways:

  - If user already had permanent license before upgrade, it will now downgrade to Eval license.
  - New license for installing ScaledMetroAggrServices cannot be generated as the license tool does not support this feature name.

  Workaround: Upgrade to Cisco IOS Release 15.2(2)S1.

- CSCtz97244

  Symptoms: IPSLA Video Operation with VRF support sees no packets received at responder.

  Conditions: This symptom occurs when no emulate CLI is specified with the input interface.

  Workaround: Use the emulate CLI to specify the input interface that has access to the VRF.

- CSCtz97755

  Symptoms: ES card crash and alignment tracebacks on SP are seen.

  Conditions: This symptom is observed with IPv6 unicast and multicast traffic up and running. Unconfiguring IPv6 unicast-routing will lead to this issue.

  Workaround: There is no workaround.

- CSCua01375

  Symptoms: Certificate validation fails when CRL is not retrieved.

  Conditions: This symptom occurs when the router is configured to use a VRF.

  Workaround: Use certificate map to revoke certificates or publish CRL to an HTTP server and configure “CDP override” to fetch the CRL.

- CSCua10377

  Symptoms: A Cisco router with Circuit Emulation SPA may suffer an SPA crash.

  Conditions: This symptom occurs when the CE T1 circuit is configured by the end user for AT&T FDL, and the end user transmits FDL messages requesting 4- hour or 24-hour performance statistics.

  Workaround: There is no workaround. If possible, contact the end user and have them reconfigure their device for ANSI FDL.

- CSCua16786

  Symptoms: When a Cisco 7600 router is placed as a mid-hop-router between the first hop router (FHR) and rendezvous point (RP), with P2P GRE tunnel interface as the FHR facing interface, then PIM-registration might not get completed. The unicast PIM-registration packet might get dropped at the Cisco 7600 router.

  Conditions: This symptom is seen in Cisco IOS Release 12.2(33)SRE6 and RLSx releases.

  Workaround: Delete and create the FHR facing p2p tunnel interface at Cisco 7600 router, which is acting as mid-hop-rtr.

- CSCua17746

  Symptoms: IKEv2 with RSA-Sig as auth session will fail.

  Conditions: The symptom is observed with:

  - IKEv2 + RSA-Sig auth + ISM VPN; or
  - IKEv2 + RSA-Sig auth + 7200 with VSA.

  Workaround: Disable ISM VPN or VSA or do not use IKEv2 RSA-Sig as auth.

- CSCua22599

  Symptoms: MCB timeout error message is seen on console. Ports 7 and 8 do not come up.

  Conditions: This symptom is seen when combo ports come up with media-type.

  Workaround: There is no workaround.

- CSCua30259

  Symptoms: EVC egress traffic does not flow. The frames are dropped by Selene.

  Conditions: This symptom occurs when SPAN is configured on service instance.

  Workaround: There is no workaround.

Caveats for Cisco IOS Release 15.2(2)S

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats, and only select severity 3 caveats are included in this section.

In this section, the following information is provided for each caveat:

- Symptoms—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.

Note If you have an account on Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com and go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl. (If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)

This section consists of the following subsections:

Open Caveats—Cisco IOS Release 15.2(2)S2

This section describes possibly unexpected behavior by Cisco IOS Release 15.2(2)S2. All the caveats listed in this section are open in Cisco IOS Release 15.2(2)S2. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCty54695

  Symptoms: RRI routes are missing when IPsec SA is up after peer IP change.

  Conditions: This symptom is observed under the following conditions:

  - Cisco ASR 1002 router running Cisco IOS XE Release 3.4.2S.
  - Dynamic crypto map with RRI.
  - Peer changes the IP address frequently.

  Workaround: Clear the crypto session with the peer.

Resolved Caveats—Cisco IOS Release 15.2(2)S2

Cisco IOS Release 15.2(2)S2 is a rebuild release for Cisco IOS Release 15.2(2)S. The caveats in this section are resolved in Cisco IOS Release 15.2(2)S2 but may be open in previous Cisco IOS releases.

- CSCsi46463

  Symptoms: A VRF-aware Name Server may not source its addresses from a VRF interface but, instead, from global interface that is connected to the Name Server.

  Conditions: This symptom is observed on a Cisco router that functions as a Name Server and that has the VRF-Aware DNS feature enabled.

  Workaround: Ping the Name Server from a CE router.

- CSCtg47129

  The Cisco IOS Software implementation of the virtual routing and forwarding (VRF) aware network address translation (NAT) feature contains a vulnerability when translating IP packets that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are not available.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-nat

  Note: The March 27, 2013, Cisco IOS Software Security Advisory bundled publication includes seven Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the March 2013 bundled publication.

  Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar13.html

- CSCtj93356

  Symptoms: Batch suspending from platform causes the MFIB on the line card to go into reloading state.

  Conditions: This symptom occurs when MFIB on the line card goes into reloading state and then finally to purge state after removal/addition of MVRFs is done followed by a line card reset.

  Workaround: There is no workaround.

- CSCtr42806

  Symptoms: The following error message can be seen sometimes, when standby or a line card is coming UP:

  ```
  %TID_HA-3-ISSU_ERR: TABLEID-ISSU-RP: FAILED: Negotiation start:
  ISSU_RC_CLIENT_ENTITY_DOES_NOT_EXIST_IN_PEER
  ```

  Conditions: This symptom occurs occasionally at standby/line card bootup.

  Workaround: There is no workaround.

- CSCts55778

  Symptoms: This is a problem involving two SAF forwarders, where one is running EIGRP rel8/Service-Routing rel1 and the other is running EIGRP dev9/Service-Routing dev2. The capabilities-manager, a client of the service-routing infrastructure, will advertise two services. When forwarders are peering with the same release image, the services propagate between the forwarders without any problems. But, when you run rel8/rel1 on one forwarder, and dev9/dev2 on the other forwarder, a third service appears in the topology table and the SR database that was not advertised. Note: The problem cannot be recreated if both forwarders are running an Cisco IOS XE Release 3.4S or and Cisco IOS XE Release 3.5S image.

Conditions: This symptom occurs if two SAF forwarders peer with each other, where one SAF forwarder is running EIGRP SAF rel9 or above and the other SAF forwarder is running EIGRP SAF rel8 or below.

Workaround: Make sure each SAF forwarder is running EIGRP rel8 or below, or rel9 or above.

- CSCtt26692

  Symptoms: The router crashes due to memory corruption. In the crashinfo, you may see:

  ```
  %SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header, chunk xxxxxxx data
  xxxxxxxx chunkmagic xxxxxxxx chunk_freemagic EF4321CD -
  Process= "CCSIP_SPI_CONTROL", ipl= 0, pid= 374
  chunk_diagnose, code = 1
  chunk name is MallocLite
  ```

  Conditions: This symptom is observed when the router is configured for SIP. When a translation-rule is configured to translate a number to one with more digits, the router may crash when the translation takes effect, such as when a call is forwarded.

  Workaround: Configuring “no memory lite” configurations can be used as a workaround in some cases (depending on the length of the phone numbers), but will cause the router to use more memory. If the translation-profile is configured to translate forwarded calls, then avoid or disable the option to forward the call.

- CSCtt34646

  Symptoms: IOMd crashes on the HA system.

  Conditions: This symptom occurs during normal reload, sometimes when standby shuts down completely and before coming up.

  Workaround: There is no workaround.

- CSCtu01601

  Symptoms: A Cisco ASR1000 series router may crash while executing the **write memory** command.

  Conditions: This issue may be triggered when the memory in the router is low.

  Workaround: There is no workaround.

- CSCtu36446

  Symptoms: The following error messages are displayed for the performance test with >20 CPS using the Cisco Radclient callsPerSecond Tool:

  ```
  Nov 10 12:56:32.953 EDT: %FMANRP_ESS-4-SESSCNT: ESS Provision Lterm Session:
  Unsupported peer_segtype= (0x15) Nov 10 12:56:32.955 EDT: %FMANRP_ESS-4-WRNPARAM_U:
  Get Lterm Peer ESS Segtype: Unsupported Peer SEGTYPE= (21) Nov 10 12:56:32.956 EDT:
  %FMANRP_ESS-4-WRNEVENT2: Ignoring Invalid ESS Segment: ESS segment/signature (0x0 /
  0x0) Nov 10 12:56:32.957 EDT: %SW_MGR-3-CM_ERROR_CLASS: Connection Manager Error:
  Class ADJ: - unable to unbind segment 2. Nov 10 12:56:32.958 EDT: %SW_MGR-3-CM_ERROR:
  Connection Manager Error - unprovision segment failed [ADJ:Lterm:43232] - hardware
  platform error.
  ```

  Conditions: This symptom is observed with high-scale, iEdge sessions.

  Workaround: There is no workaround.

- CSCtv36812

  Symptoms: An incorrect crashInfo file name is displayed during a crash.

  Conditions: This symptom is observed whenever a crash occurs.

  Workaround: There is no workaround.

- CSCtw53121

  Symptoms: ES+ goes into major state occasionally on reload or SSO.

  Conditions: This symptom is observed with the Cisco 7600 router with a 40 gig ES+ line card that is running Cisco IOS Release 15.2(2)S.

  Workaround: There is no workaround.

- CSCtw68089

  Symptoms: The routing event detector is not present on Integrated Services Routers such as the Cisco 2800 series.

  Conditions: This symptom occurs for all releases on generation one Cisco ISR routers running Cisco IOS Release 15.2(2)T.

  Workaround: There is no workaround.

- CSCtw70298

  Symptoms: A router crashes after the router boots up with scaled configuration and L2/L3 Distributed EtherChannel (DEC) or port-channel.

  Conditions: This symptom occurs only if there are more than two or more DFCs (ES+ and other equivalents) and with L2/L3 DEC configured such that one of the DFCs takes much longer to come up than the other.

  Workaround: There is no workaround.

- CSCtw98200

  Symptoms: Sessions do not come up while configuring RIP commands that affect the virtual-template interface.

  Conditions: This symptom is observed if a Cisco ASR1000 series router is configured as LNS.

  RIP is configured with the **timers basic** *5 20 20 25* command. Also, every interface matching the network statements is automatically configured using the **ip rip advertise** *5* command. These interfaces include the loopback and virtual-template interfaces too.

  On a Cisco ASR1000 series router, this configuration causes the creation of full VAIs which are not supported. Hence, the sessions do not come up. On Cisco ISR 7200 routers, VA subinterfaces can be created.

  Workaround: Unconfigure the **timers rip** command.

- CSCtx06813

  Symptoms: Installation fails, “rwid type l2ckt” error messages appear, and the VC may fail to come up on Quad-Sup router only. Though this error may appear for multiple other reasons, this bug is specific to Cisco Catalyst 6000 Quad-Sup SSO only.

  Conditions: This symptom is observed in a scaled scenario, doing second switchover on Quad-Sup router.

  Workaround: There is no workaround.

- CSCtx11598

  Symptoms: A router reload causes a Cisco Shared Port Adapter (SPA) failure with the following error message:

  ```
  % CWAN_SPA-3-FAILURE: SPA-2CHT3-CE-ATM[2/2]: SPA failure
  ```

  This failure can cause the SPA to go to one of the following states:

  - none

  - standby reset
  - down

  This failure leads to unexpected system reload.

  Conditions: This symptom is observed during router reload for 15-20 times.

  Workaround: Ensure that all of the library shared objects are loaded at the time of the SPA initialization.

- CSCtx23014

  Symptoms: HSRP hellos cannot be sourced from certain IPs.

  Conditions: This symptom is observed when HSRP hellos cannot be sourced for an IP address with a standby IP address in the same subnet and both are configured in the global VRF. For example:

```
Router(config)#interface Ethernet0/0
Router(config-if)# ip address 192.168.68.13 255.255.252.0
Router(config-if)# standby 68 ip 192.168.70.1
Router(config-if)# standby 68 priority 120
Router(config-if)# standby 68 preempt
Router(config-if)# arp timeout 300
```

  Workaround: Use an IP from the subnet for the SVI interface in the same VRF.

- CSCtx42751

  Symptoms: The following error message is displayed:

```
 %TRANSCEIVER-3-INIT_FAILURE: SIP2/0: Detected for transceiver module in
TenGigabitEthernet2/0/0, module disabled %LINK-3-UPDOWN: SIP2/0: Interface
 TenGigabitEthernet2/0/0, changed state to down
```

  Conditions: This symptom is observed with the XFP-10GLR-OC192SR transceiver.

  Workaround: Configure “service unsupported-transceiver”.

- CSCtx48753

  Symptoms: Higher memory usage with PPP sessions than seen in Cisco IOS XE Release 3.4/3.5.

  Conditions: This symptom is observed with configurations with PPP sessions. These will see up to 10% higher IOS memory usage than in previous images.

  Workaround: There is no workaround.

- CSCtx54882

  Symptoms: A Cisco router may crash due to Bus error crash at voip_rtp_is_media_service_pak .

  Conditions: This symptom has been observed on a Cisco router running Cisco IOS Release 15.1(4)M2

  Workaround: There is no known workaround.

- CSCtx66011

  A vulnerability in the Internet Key Exchange (IKE) protocol of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a memory leak that could lead to a device reload.

  The vulnerability is due to incorrect handling of malformed IKE packets by the affected software. An attacker could exploit this vulnerability by sending crafted IKE packets to a device configured with features that leverage IKE version 1 (IKEv1).

Although IKEv1 is automatically enabled on a Cisco IOS Software and Cisco IOS XE Software when IKEv1 or IKE version 2 (IKEv2) is configured, the vulnerability can be triggered only by sending a malformed IKEv1 packet.

In specific conditions, normal IKEv1 packets can also cause an affected release of Cisco IOS Software to leak memory.

Only IKEv1 is affected by this vulnerability.

An exploit could cause Cisco IOS Software not to release allocated memory, causing a memory leak. A sustained attack may result in a device reload.

Cisco has released free software updates that address this vulnerability. There are no workarounds to mitigate this vulnerability.

This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130925-ike

Note: The September 25, 2013, Cisco IOS Software Security Advisory bundled publication includes eight Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the September 2013 bundled publication.

Individual publication links are in “Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication” at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep13.html

- CSCtx66030

  Symptoms: A Cisco router handling SIP registrations/unregistrations may unexpectedly reload. This symptom is observed on the following devices:

  – SIP-CME

  – SIP-SRST GW

  – CUBE

  Conditions: This symptom is observed when the number of SIP registrations/unregistrations handled is more than 320.

  Workaround: Limit the number of registrations/unregistrations to less than 320.

- CSCtx66046

  Symptoms: The Standby RP crashes with a traceback listing db_free_check.

  Conditions: This symptom occurs when OSPF NSR is configured. A tunnel is used and is unnumbered with the address coming from a loopback interface. A network statement includes the address of the loopback interface. This issue is seen when removing the address from the loopback interface.

  Workaround: Before removing the address, remove the network statement which covers he address of the loopback interface.

- CSCtx66804

  Symptoms: The configuration “ppp lcp delay 0” does not work and a router does not initiate CONFREQ.

  Conditions: This symptom is observed with the following conditions:

  – “ppp lcp delay 0” is configured.

  – The symptom can be seen on Cisco IOS Release 15.0(1)M5.

Workaround: Set delay timer without 0.

- CSCtx77501

  Symptoms: Traffic is dropped at the decap side of the PE box.

  Conditions: This symptom occurs with SSO at the decap side of an MVPN setup, DFC core-facing, 6748 access-facing.

  Workaround: Do a switchover.

- CSCtx79462

  Symptoms: OSPF neighborship does not get established.

  Conditions: This symptom is observed when enabling PFC on a multilink bundle in SIP-400. The OSPF neighborship does not get established.

  Workaround: There is no workaround. Disable PFC to bring up the OSPF neighborship.

  Further Problem Description: The OSPF hello packets get dropped by the peer end because the IP header is corrupted.

- CSCtx95840

  Symptoms: A Cisco voice gateway may unexpectedly reload.

  Conditions: This symptom is observed on a Cisco voice gateway running SIP protocol. In this case, the issue was when sipSPIUfreeOneCCB() returns, the leftover event is still being processed after CCB is released from sipSPIUfreeOneCCB(). Based on sipSPIStartRemoveTransTimer(ccb), CCB should have been released later by a background timer.

  Workaround: There is no workaround.

- CSCty01237

  Symptoms: The router logs show:

  ```
  <timestamp> %OER_BR-5-NOTICE: Prefix Learning STARTED
  CMD: 'show run' <timestamp>
  ```

  This is followed by the router crashing.

  Conditions: This symptom is observed under the following conditions:

  1. Configure PfR with a learn-list using a prefix-list as a filter and enable learn.
  2. Use a configuration tool, script or NMS that periodically executes **show run** on the MC over HTTP or some other means.

  Workaround 1: If you use the PfR learn-list feature, do not execute **show run** periodically.

  Workaround 2: If you use a monitoring tool that executes **show run** periodically, avoid using a learn-list configuration in PfR.

- CSCty03745

  Symptoms: BGP sends an update using the incorrect next-hop for the L2VPN VPLS address-family, when the IPv4 default route is used, or an IPv4 route to certain destination exists. Specifically, a route to 0.x.x.x exists. For this condition to occur, the next-hop of that default route or certain IGP/static route is used to send a BGP update for the L2VPN VPLS address-family.

  Conditions: This symptom occurs when the IPv4 default route exists, that is:

  ```
  ip route 0.0.0.0 0.0.0.0 <next-hop>.
  ```

  Or a certain static/IGP route exists: For example:

  ```
   ip route 0.0.253.0 255.255.255.0 <next-hop>.
  ```

Workaround 1: Configure next-hop-self for BGP neighbors under the L2VPN VPLS address-family. For example:

```
router bgp 65000
 address-family l2vpn vpls
  neighbor 10.10.10.10 next-hop-self
```

Workaround 2: Remove the default route or the static/IGP route from the IPv4 routing table.

- CSCty05092

  Symptoms: EIGRP advertises the connected route of an interface which is shut down.

  Conditions: This symptom is observed under the following conditions:

  1. Configure EIGRP on an interface.
  2. Configure an IP address with a supernet mask on the above interface.
  3. Shut the interface. You will find that EIGRP still advertises the connected route of the above interface which is shut down.

  Workaround 1: Remove and add INTERFACE VLAN xx.

  Workaround 2: Clear ip eigrp topology x.x.x.x/y.

- CSCty10285

  Symptoms: WCCP redirection does not happen with a Cisco ASR 1000 router running Cisco IOS XE Release 3.5 RP1.

  Conditions: This symptom occurs when GetVPN is used.

  Workaround: There is no workaround.

- CSCty22840

  Symptoms: A router can crash due to a Watchdog timeout on the NTP process as it fails to unpeer from an NTP peer that had already been removed. In addition, the following error might be seen in the system log:

  ```
  NTP Core (ERROR): peer struct for X.X.X.X not in association table
  ```

  Conditions: This symptom is observed when active changes occur in NTP, that is, new peers or servers are added at boot time as part of the existing configuration or during normal operation as part of a new configuration.

  Workaround: Configure NTP to use the ACL with the **ntp access-group peer** command to explicitly define which hosts can function as an NTP peer.

- CSCty24143

  Symptoms: The router does not pass IPv6 OSPF traffic.

  Conditions: This symptom occurs when the router passes traffic at the full line rate of a link.

  Workaround: Reduce the traffic rate by 10%.

- CSCty29230

  Symptoms: CMFIB entries are not being programmed on the SP and DFCs. Mroute shows both Accept and OILS, **ip mfib** output also shows Accept interface and Forwarding interface, but CMFIB entries are not programmed.

  Conditions: This symptom is observed with a Cisco 7600 router running a Cisco IOS Release 15.1(3)S throttle.

  Workaround: There is no workaround.

- CSCty38305

  Symptoms: The **xconnect vfi vpls** command gets rejected.

  Conditions: This symptom occurs while configuring "xconnect vfi vpls" under the interface VLAN. The error message "command rejected" is received.

  Workaround: There is no workaround.

- CSCty41336

  Symptoms: Forward-alarm ais does not work on CESoPSN circuits.

  Conditions: This symptom occurs when you create SAToP and CESoPSN circuits and configure "forward-alarm ais".

  Workaround: There is no workaround.

- CSCty43587

  Symptoms: A crash is observed with memory corruption similar to the following:

  ```
  %SYS-2-FREEFREE: Attempted to free unassigned memory at XXXXXXXX, alloc XXXXXXXX,
  dealloc XXXXXXXX
  ```

  Conditions: This symptom is observed when SIP is configured on the router or SIP traffic is flowing through it.

  Workaround: There is no workaround.

- CSCty47231

  Symptoms: Traffic drops on removing the port-shaper.

  Conditions: This symptom is observed only when the policymap attach/detach is coupled with a link up/down. This issue is not seen on normal attach/detach. There are no issues with reload and policymap attached/detached.

  Workaround: Default the egress interface, and reconfigure; traffic recovers.

- CSCty51172

  Symptoms: The MAC address learned on L2 DEC on 7600-ES+40G3CXL is not installed as the primary entry on all the member interfaces, if the ingress traffic is on the nonhashed interface for that EFP.

  Conditions: This symptom occurs when Layer 2 distributed Etherchannel traffic is learned on a hashed interface first and then moved to a nonhashed interface.

  Workaround: Do not use Layer 2 distributed Etherchannel.

- CSCty53243

  Symptoms: Video call fails in the latest mcp_dev image asr1000rp2-adventerprisek9.BLD_MCP_DEV_LATEST_20120303_065105_2.bin. This image has the uc_infra version: uc_infra@(mt_152_4)1.0.13. Note that video call works fine with the previous mcp_dev image asr1000rp2-adventerprisek9.BLD_MCP_DEV_LATEST_20120219_084446_2.bin.

  Conditions: This symptom is observed when CUBE changes the video port to "0" in 200 OK sent to the UAC.

  Workaround: There is no workaround.

- CSCty53923

  Symptoms: Broadcast traffic flows over the Standby Spoke VC and then gets punted.

Conditions: This symptom is observed when the nPE is the Cisco ME 3600X switch or the Cisco ME 3800X switch and the Standby Spoke VC terminates on it.

Workaround: There is no workaround.

- CSCty55449

  Symptoms: The device crashes after registering an Embedded Event Manager TCL policy.

  Conditions: If the policy uses the multiple event feature and the trigger portion is registered without curly braces ("{}"), then the device will crash. For example, this policy will trigger a crash:

```
::cisco::eem::event_register_syslog tag 1 pattern " pattern1"
::cisco::eem::event_register_syslog tag 2 pattern " pattern2"
::cisco::eem::trigger
::cisco::eem::correlate event 1 or event 2

namespace import ::cisco::eem::*
namespace import ::cisco::lib::*

action_syslog priority crit msg " triggered "
```

  Note how "::cisco::eem::trigger" is not followed by an opening curly brace.

  Workaround: Ensure that the trigger portion (that is, the correlate statement) is enclosed within curly braces. Given the example above, the proper syntax is:

```
::cisco::eem::event_register_syslog tag 1 pattern " pattern1"
::cisco::eem::event_register_syslog tag 2 pattern " pattern2"
::cisco::eem::trigger {
  ::cisco::eem::correlate event 1 or event 2
}

namespace import ::cisco::eem::*
namespace import ::cisco::lib::*

action_syslog priority crit msg " triggered "
```

- CSCty58992

  Symptoms: One-way audio is observed after transfer to a SIP POTS Phone.

  Conditions: This symptom is observed under the following conditions:

  - Cluster is in v6 mode.
  - A call is made from Phone1 to Phone2, and then Phone2 transfers the call to Phone3(SIP POTS), which is when the issue occurs.

  Workaround: There is no workaround.

- CSCty64216

  Symptoms: On unconfiguring a scaled ACL, the router crashes.

  Conditions: This symptom is observed when an ACL having 1000 ACEs or more is unconfigured.

  Workaround: There is no workaround.

- CSCty66871

  Symptoms: The router stops forwarding traffic across one or more EoMPLS virtual circuits (VCs). Conditions: This symptom cccurs when you perform a shut/no shutdown on the MPLS TE tunnel carrying the VC.

  Workaround: Issue the clear xconnect command on the VC.

- CSCty68348

  Symptoms: If the OSPF v2 process is configured with the **nsr** command for OSPF nonstop routing, (seen after shutdown/no shutdown of the OSPF process), the neighbor is seen on standby RP as FULL/DROTHER, although the expected state is FULL/DR or FULL/BDR. As a result, after switchover, routes pointing to the FULL/DROTHER neighbor may not be installed into RIB.

  Conditions: This symptom is observed under the following conditions:

  - The OSPF router is configured for “nsr”.
  - Shutdown/no shutdown of the OSPF process.

  Workaround: Flapping of the neighbor will fix the issue.

- CSCty77582

  Symptoms: Traffic does not get classified in a DSCP-based class map for EVC in SW Eompls.

  Conditions: This symptom is observed when a policy map is applied to EVC in SW Eompls, and DSCP-based classification does not work.

  Workaround: There is no workaround.

- CSCty78435

  Symptoms: L3VPN prefixes that need to recurse to a GRE tunnel using an inbound route-map cannot be selectively recursed using route-map policies. All prefixes NH recurse to a GRE tunnel configured in an encapsulation profile.

  Conditions: This symptom occurs when an inbound route-map is used to recurse L3VPN NH to a GRE tunnel. Prefixes are received as part of the same update message and no other inbound policy change is done.

  Workaround: Configure additional inbound policy changes such as a community change and remove it prior to sending it out.

- CSCty79896

  Symptoms: Traffic drop is seen with 6rd tunnels having two ECMP paths to the core. Upon sending traffic with both ECMP paths (Gi4/14 and Gi4/5) active, traffic drops are seen as packets are software-switched and punted to RP. This issue is not seen with only one path active.

  The following steps summarize the issue:

  1. Both Gi4/14 and Gi4/5 should be unshut. Traffic flows through 4/14 but drops are seen.
  2. Frames are sent from Ixia - 4548658.

```
PE1#
PE1#sh interface counters | i 4/14
 Port        OutOctets        OutUcastPkts     OutMcastPkts    OutBcastPkts
Gi4/14      70829             999              6
 0
Gi4/14      19303273          229956          6
0           >>>>>>>>>>>. Only 229956 are sent out of 4548658

PE1#sh interface counters | i 4/5
Gi4/5       77143              1083           9                 0
Gi4/5       76176              1074           7                 0

PE1#sh int tu10 stat
Tunnel10
   Switching path    Pkts In    Chars In    Pkts Out    Chars Out
      Processor      0          0           0            0
    Route cache      0          0           228961       15111426
     >>>>>>>>>>>> Software switched
```

```
Distributed cache    0          0           0            0
       Total         0          0           228961       15111426
```

Conditions: This symptom is triggered when there are ECMP paths for the 6rd tunnels.

Workaround: You can recover by unconfiguring the ECMP paths and having a single path.

- CSCty86111

  Symptoms: The Cisco ISR G2 router crashes after “no ccm-manager fallback-mgcp” is configured.

  Conditions: This symptom is observed with Cisco ISR G2 router.

  Workaround: There is no workaround.

- CSCty89224

  Symptoms: A Cisco IOS router may crash under certain circumstances when receiving an MVPNv6 update.

  Conditions: This symptom is observed when receiving an MVPNv6 update.

  Workaround: There is no workaround.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.8/5.6: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:S/C:N/I:N/A:C/E:F/RL:OF/RC:C

  CVE ID CVE-2012-3895 has been assigned to document this issue. Additional information on Cisco’s security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCty96052

  Symptoms: A Cisco router may unexpectedly reload due to Bus error or SegV exception when the BGP scanner process runs. The BGP scanner process walks the BGP table to update any data structures and walks the routing table for route redistribution purposes.

  Conditions: This symptom is an extreme corner case/timing issue. This issue has been observed only once on a release image.

  Workaround: Disabling NHT will prevent the issue, but it is not recommended.

- CSCty96953

  Symptoms: The router drops traffic on an MLPPP bundle.

  Conditions: This symptom occurs after you perform a shutdown/no shutdown on an MLPPP bundle while the router is passing traffic.

  Workaround: Perform an OIR the interface module.

- CSCty99874

  Symptoms: Ingress policing is done on the EVC which does not have QoS policy.

  Conditions: This symptom is observed when one EVC has a QoS policy, and another does not. The QoS policy shows effect on the other EVC also.

  Workaround: Attach a dummy policy to the other EVC. Or attach and detach a policy on the other EVC.

- CSCtz00430

  Symptoms: The static route is removed from the routing table.

  Conditions: This symptom is observed when pulling out and replacing a connection to the management interface.

Workaround 1: Default the management interface and reconfigure IP.

Workaround 2: Do a shut and no shut on the management interface through the CLI.

- CSCtz03559

  Symptoms: MVPN is seen on the Cisco ME 3600X and ME 3800X switches.

  Conditions: This symptom is observed as currently, there are two SDM templates present in the Cisco ME 3600X and ME 3800X switches. Both templates do not support MVPN. A new SDM template is needed on the license “AdvancedMetroIPAccess” to support the MVPN.

  Workaround: MVPN cannot be used without the new SDM template.

- CSCtz06611

  Symptoms: IPsec tunnel states are UP-IDLE because of broadcast packets that are punted to the CPU. The mac-address of VPN-SPA is not learned properly.

  Conditions: This symptom is a timing issue. You may see it the first time or need to try multiple times. This symptom is seen with the crypto map plus vrf configuration.

  1. Reload the router with above configuration: the mac-address changes to all FF.
  2. Default the configuration of VLAN (where crypto map and engine is applied), then configure it again with old configuration. Now the mac-address will show all FF. 3. Create the vlan. Do a **no shutdown**. Attach vrf. Then add crypto map to it.

  Workarounds: For the steps mentioned in condition section above, below are the workarounds respectively.

  Workaround 1: Remove and add “ip vrf forwarding” and then remove and add the **crypto engine** command.

  Workaround 2: Remove and add the **crypto engine** command. Workaround 3: Do a **shut/no shut** on the VLAN interface.

- CSCtz08719

  Symptoms: With split horizon, traffic does not flow on all BDs.

  Conditions: This symptom is observed when traffic does not flow on all BDs.

  Workaround: There is no workaround.

- CSCtz08746

  Symptoms: On the 12in1 Serial SPA with hardware version lower than 2.0, an upgrade using “test upgrade” with the latest Cisco 7600 FPD bundles results in the SPA FPD device being downgraded from version 1.2 to 1.1. Subsequently, both auto and manual upgrades fail to bring the SPA FPD version back to 1.2. The SPA goes to the OutOfServ or FpdUpReqd state.

  Conditions: This symptom is observed only with the older SPA hardware (hardware version lower than 2.0) when it is plugged into a SIP200 or SIP400 on the Cisco 7600 platform.

  Workaround: Use the latest SPA hardware (hardware version 2.0 or above).

- CSCtz11876

  Symptoms: The **show ethernet cfm maintenance-points local** command output shows type BD and ID 0 after MTU is changed on the interface that has a service instance with xconnect. This issue is also seen if the backup peer is changed under xconnect.

  Conditions: This symptom is observed when Ethernet CFM MEP is configured on an xconnect service instance.

  Workaround: Remove MEP and reapply.

- CSCtz12525

  Symptoms: Accounting stop is sent without Acct-Input-Packets Acct-Output-Packets Acct-Input-Octets Acct-Output-Octets when service stop is performed.

  Conditions: This symptom is observed when service stop is issued for the prepaid service.

  Workaround: There is no workaround.

- CSCtz13465

  Symptoms: High CPU is seen on Enhanced FlexWAN module due to interrupts with traffic.

  Conditions: This symptom is observed with an interface with a policy installed.

  Workaround: There is no workaround.

- CSCtz13818

  Symptoms: In a rare situation when route-map (export-map) is updated, IOS is not sending refreshed updates to the peer.

  Conditions: This symptom is observed when route-map (export-map) is configured under VRF and the route-map is updated with a new route-target. Then the IOS does not send refreshed updates with modified route-targets.

  Workaround 1: Refresh the updated route-target to use **clear ip route vrf** *vrf-name net mask*.

  Workaround 2: Hard clear the BGP session with the peer.

- CSCtz24047

  Symptoms: Free process memory is being depleted slowly on linecards in the presence of the DLFIoATM feature configured on a PA-A6-OC3 (enhanced Flexwan). Finally memory allocation failures are observed. Use the show memory proc stat history command to display the history of free process memory.

  Conditions: This symptom occurs when Slow Proc Memory depletion is observed on 7600-ES+ cards when installed on a Cisco 7600 router that has DLFIoATM configured on a PA-A6-OC3 hosted on an enhanced Flexwan module.

  Workaround: There is no workaround.

- CSCtz25953

  Symptoms: The "LFD CORRUPT PKT" error message is dumped and certain length packets are getting dropped.

  Conditions: This symptom is observed with a one-hop TE tunnel on a TE headend. IP packets with 256 or multiples of 512 byte length are getting dropped with the above error message.

  Workaround: There is no workaround.

- CSCtz26188

  Symptoms: Packet loss is observed on platforms in certain deployments having a large number of prefixes routing traffic onto a TE tunnel.

  Conditions: This symptom occurs if the configured value of the cleanup timer is 60 seconds, then packets might be lost on the platforms where the forwarding updates take longer.

  Workaround: Configure the value of the cleanup timer to 300 seconds.

  ```
  mpls traffic-eng reoptimize timers delay cleanup 300
  ```

- CSCtz26658

  Symptoms: The Cisco ASR 1000 router acts as GET VPN GM. Small UDP fragments (21 to 25 bytes, IP header included) coming in through IPsec are dropped.

  Conditions: This symptom occurs when the Cisco ASR 1000 router acts as GET VPN GM and TBAR is enabled for the group.

  Workaround: There is no workaround. Disabling TBAR is not recommended as a workaround due to the operational impact of the change on a live GET VPN network.

- CSCtz30983

  Symptoms: Crash on ES+ line card upon issuing the **show hw-module slot X tech- support** or **show platform hardware version** command. This is similar to CSCti78408 but not to CSCti78408.

  Conditions: This symptom occurs on an ES+ line card.

  Workaround: Do not issue the **show hw-module slot X tech- support** or **show platform hardware version** command on an ES line card unless explicitly mentioned by Cisco.

- CSCtz35061

  Symptoms: Flexlink switchover causes VLAN to not be allowed in trunk link.

  Conditions: This symptom is related to flexlink switchover caused by instantaneous link flapping.

  Workaround: There is no workaround.

- CSCtz37863

  Symptoms: IPCP is not in an open state and it does not seem to be calling the This-Layer-Down (TLD) vector.

  Conditions: This symptom is observed if IPv4 saving is enabled and IPCP negotiation failed because of a TermReq received from peer.

  Workaround: There is no workaround.

- CSCtz38558

  Symptoms: The following traceback may be seen on a Cisco ASR 1000 router when processing some IPv6 packets:

  ```
  Apr 18 17:20:27.554: %IOSXE-3-PLATFORM: F1: cpp_cp: QFP:0.0 Thread:132
  TS:00000176080579214858 %INFRA-3-INVALID_GPM_ACCESS: Invalid GPM Load at 800268cd HAL
  start 3fc0 HAL end 413f INFRA start 409e INFRA 4140 NET 340d0
  -Traceback=1#002b3a75f6cabf53c25612ed4553871e 804b0d63 804b1204
  8046c212 80020708 800268cd 80026cd0 80435955 806509bb
  Apr 18 17:20:27.554: %IOSXE-3-PLATFORM: F1: cpp_cp: QFP:0.0 Thread:132
  TS:00000176080579433103 %INFRA-3-INVALID_GPM_ACCESS_INFO: 80026cd0
  0002fdb0 0002fdd4 0002fdd0 00000002 00000001 00000001 0003413f
  00000001 00000000 00000000 00001000 93b9bac0 8ba80000 fffffffd 00201000 Apr 18
  17:20:27.554: %IOSXE-3-PLATFORM: F1: cpp_cp: QFP:0.0 Thread:132
  TS:00000176080579587035 %INFRA-3-INVALID_GPM_ACCESS_DATA: e188f4a8aa3ef3a0
   205e84e72c9f6761 4486ffd3c38d7e12 b0c71bf4a146b4ba 8e786f7e673d2e56
  9308160a565df75c 952e4a0fe2ef327c 1cff673d2be0f8bf
  48248a1e150a1ce9 e1386aed768ad28c e6d23cd54b68619e c49866ce95863bf6
  c99d8c7d5a2e4a8a c99d8c7d5a2e4a8a c99d8c7d5a2e4a8a
  c99d8c7d5a2e4a8a c99d8c7d5a2e4a8a c99d8c7d5a2e4a8a c99d8c7d5a2e4a8a
  c99d8c7d5a2e4a8a 8553c53af0e4f16e
  ```

  Conditions: This symptom occurs when the IPv6 packet is malformed.

  Workaround: There is no workaround.

  Additional Information: The packet will be dropped.

- CSCtz41048

  Symptoms: The **trace mpls ipv4** command is unsuccessful.

  Conditions: This symptom is observed with the **trace mpls ipv4** command.

  Workaround: There is no workaround.

- CSCtz46300

  Symptoms: Traffic is not classified under the QoS ACLs having port matching using range (inclusive range), lt (less than), and gt (greater than) operators.

  Conditions: This symptom is seen with IPv4 and IPv6 with L4 port ranger operations using range, lt, and gt, which do not work with QoS ACLs on Cisco ME 3600 and Cisco ME3800 switches.

  Workaround: There is no workaround.

- CSCtz46399

  Symptoms: VLAN RAM is not programmed with the correct VPN number for a few VRFs.

```
Eagle2-es20-dfc4#sh mls vlan-ram 1182
1182 TYCHO Vlan RAM
Key: * => Set, - => Clear

vlan    nf-vpn mpls mc-base siteid stats rpf vpn-num bgp-grp l2-metro
rpf-pbr-ovr
-------+-----+-------+-----+-----------+------+-----+---+-----------+----------+------
----+-----------
1182    -       -       *      0        0       -       -     0           0
        -          *
```

  Conditions: This symptom is observed with the OIR of the ES-20 line card with scaled MVPNv6 configuration and 50 VRFs configured.

  Workaround: There is no workaround.

- CSCtz47309

  Symptoms: When using smart defaults in FlexVPN, the mode transport may be sent from initiator even if “tunnel” is configured.

  Conditions: This symptom was first seen on a Cisco ASR router running Cisco IOS Release 15.2(2)S and a Cisco ISR router running Cisco IOS Release 15.2(3)T. It is seen with FlexVPN.

  Workaround: Use smart defaults on both sides on of the tunnel.

- CSCtz52844

  Symptoms: Excessive memory is being held by SG DPM process.

  Conditions: This symptom has been observed on a Cisco 10000 router running Cisco IOS Release 12.2(33)SB10 when some users send many duplicate DHCP discover messages.

  Workaround: Clear the sessions intermittently.

- CSCtz59041

  Symptoms: After router reload, the agent succeeds but with the following errors:

```
*Apr 26 11:22:42.455 IST: %DHCP_SNOOPING-6-AGENT_OPERATION_SUCCEEDED: DHCP snooping
database Read succeeded.
*Apr 26 11:22:42.455 IST: %DHCP_SNOOPING-6-VLAN_NOT_SUPPORTED: Vlan not supported. 150
bindings ignored
```

Conditions: This symptom occurs when some LCs such as ES+ take more time to come up compared to others. If there are SVIs on these on which snooping is enabled, some bindings might get dropped after router reload.

Workaround: Force a retry using the **renew** command.

- CSCtz61153

  Symptoms: The Cisco ASR 903 router does not establish BFD neighbors over port-channel 16.

  Conditions: This symptom occurs when you configure BFD on port-channel 16 between two Cisco ASR 903 routers.

  Workaround: Configure BFD on port-channels 1-15.

- CSCtz61274

  Symptoms: BFD sessions remain DOWN post peer node reload.

  Conditions: This symptom occurs when BFD RX gets impacted post reload of the peer node as it fails to do a proper lookup on the GAL label. This issue is seen intermittently.

  Workaround: There is no workaround.

- CSCtz62680

  Symptoms: “DFC WAN Line Card Software Element Not Found - QOS: TCAM Class ID” errors appear along with BADCHUNKFREEMAGIC errors, leading to an ES20 crash.

  Conditions: This symptom occurs when service policies less than 128 kb are added or removed.

  Workaround: There is no workaround.

- CSCtz63974

  Symptoms: Mcast T/F forwarding fails for some EVCs with Trunk EFP’s Encapsulation change.

  Conditions: This symptom is observed under the following conditions:

  1. Configure Trunk EVCs with the range of allowed VLANS.
  2. Initiate Mcast traffic to allowed BDIs.
  3. While Multicast data traffic is on, change the Encapsulation definition to add/delete few VLANs and check the replication.

  Workaround: There is no workaround.

- CSCtz66284

  Symptoms: IOMD crash may be seen.

  Conditions: This symptom is observed when bringing up the interfaces on an HA system.

  Workaround: There is no workaround.

- CSCtz66770

  Symptoms: When under ATM PVC (SPA-4XOC3-ATM or v2) with MUX encapsulation and OAM enabled, L3 policy-map is applied and PVC goes down.

  Conditions: This symptom occurs when policy-map sets DSCP (to 7) for default- class, and it affects OAM communication.

  Workaround: Use aal5snap encapsulation.

- CSCtz67785

  Symptoms: The Cisco ASR 1000 router may experience a CPP crash.

Conditions: This symptom occurs when the router is configured for Session Border Controller (SBC). During periods of high traffic, FP reports a lot of media up events to RP, which can crash FP.

Workaround: If "ip nbar protocol-discovery" is enabled, it may exacerbate the crashes. Removing it may help provide some stability.

- CSCtz71940

  Symptoms: The Present Active crashes on issuing the SSO CLI.

  Conditions: This symptom occurs when performing switchover on the HA system.

  Workaround: There is no workaround. The Present Active (new standby) comes up fine again even after it crashes. There is no functionality impact.

- CSCtz72390

  Symptoms: The name mangling functionality is broken. Authorization fails with the "IKEv2:AAA group author request failed" debug message.

  Conditions: This symptom is observed with Cisco IOS Release 15.2(3)T.

  Workaround: There is no workaround.

- CSCtz72615

  Symptoms: All interfaces on a Cisco 7600-SIP-200 are down after Cisco IOS downgrade.

  Conditions: This symptom is observed on Cisco 7600 series routers.

  Workaround: There is no workaround.

- CSCtz73836

  Symptoms: The router crashes.

  Conditions: This symptom is observed when the router is running NHRP.

  Workaround: There is no workaround.

- CSCtz74229

  Symptoms: The rate at which ARP requests are triggered by traffic being sent to a destination in which the ARP is not resolved is very low.

  Conditions: This symptom occurs when traffic is being sent to multiple destinations in which the ARP is not resolved.

  Workaround: There is no workaround.

- CSCtz74685

  Symptoms: A router crash is observed on Y1731 DM.

  Conditions: This symptom is seen when starting 1DM session.

  Workaround: There is no workaround.

- CSCtz75641

  Symptoms: The router drops traffic over a port-channel.

  Conditions: This symptom occurs when you perform the following sequence of events:

  - Configure and bundle gi0/0/0 into a port-channel.
  - Remove gi0/0/0 from port-channel.
  - Another link (it may be gi0/0/0 if it is added back or any other interface) bundles to the port-channel

  Workaround: Reload the router.

- CSCtz77171

  Symptoms: Subscriber drops are not reported in mod4 accounting.

  Conditions: This symptom is observed on checking policy-map interface for account QoS statistics on a port-channel subinterface.

  Workaround: There is no workaround.

- CSCtz78194

  Symptoms: A Cisco ASR 1000 that is running Cisco IOS XE Release 3.6 or Cisco IOS Release 15.2(2)S crashes when negotiating multi-SA DVTI in an IPsec key engine process.

  Conditions: This symptom is observed with the Cisco ASR configured to receive DVTI multi-SA in aggressive mode and hitting an ISAKMP profile of a length above 31.

  Workaround: Shorten the ISAKMP profile name to less than 31.

- CSCtz79488

  Symptoms: Multicast replication fails for some of the EFPs post removal/recreation of BDIs.

  Conditions: This symptom is observed under the following conditions:

  1. There are 255 EVCs on a single port, attached to 255 BDIS (1:1).
  2. Configure the policy map on each EVC.
  3. Initiate Multicast data traffic to a single Multicast group.
  4. Remove some of the BDIS and recreate with Multicast data traffic on. Replication fails post recreation of BDIS.

  Workaround: Perform shut/no shut on the 255 EVCs configured interface.

- CSCtz80643

  Symptoms: A PPPoE client's host address is installed in the LNS's VRF routing table with the **ip vrf receive** *vrf name* command supplied either via RADIUS or in a Virtual-Template, but is not installed by CEF as attached. It is instead installed by CEF as receive, which is incorrect.

  Conditions: This symptom is observed only when the Virtual-access interface is configured with the **ip vrf receive** *vrf name* command via the Virtual-Template or RADIUS profile.

  Workaround: There is no workaround.

- CSCtz82232

  Symptoms: The following error message is displayed:

  IOSXE_INFRA-6-PROCPATH_CLIENT_HOG: on reload, traffic fails post Reload

  Conditions: This symptom is observed under the following conditions:

  - Multicast data traffic to a single Multicast group with 255 OIFs. - 255 EVCs on single port with a policy map on each EVC. - All 255 BDIS send IGMPv3 SSM joins to a single Multicast group. - Reload the box and observe the Hog messages.

  Workaround: There is no workaround.

- CSCtz82265

  Symptoms: IOSd crash is seen on the Cisco ASR 903 router while reloading all IMs continuously on the setup.

  Conditions: This symptom is observed with MPLS-TP configurations and 510 BFD sessions.

  Workaround: There is no workaround.

- CSCtz82711

  Symptoms: Datapath session would

  Conditions: This symptom is observed when SGSN sends echo req before PDP_CREATE_REQ.

  Workaround: There is no workaround.

- CSCtz85907

  Symptoms: A Cisco 7600 should have an MVPNv4 configuration and the system replication mode as egress. Now, if "address-family ipv6" is configured under the VRF definition, MVPN traffic might be affected.

  Conditions: SREx and RLSx releases.

  Workaround: Use ingress replication.

- CSCtz86024

  Symptoms: There is a long delay in joining mcast stream with Cisco IOS 15S releases that are running on RP.

  Conditions: This symptom is observed when there is no (*,G) on the box, and the first packet for the stream creates this entry.

  Workaround: With static joins we can make sure that entry is present in mroute table.

- CSCtz86763

  Symptoms: Sessions remain partially created, and memory is consumed and not returned.

  Conditions: This symptom occurs when sessions are churned and reset before they reach active state.

  Workaround: There is no workaround.

- CSCtz89485

  Symptoms: NAT traffic passes through the new standby router following HSRP switchover.

  Conditions: This symptom is observed with HA NAT (NAT with HSRP) mappings with inside global addresses that overlap a subnet owned by a router interface.

  Workaround:

  1. Force a HSRP switchover so that the initial standby router takes activity.
  2. Remove and readd HSRP NAT mappings on the newly active router.
  3. Force a HSRP swtichover back to the initial active router.

- CSCtz90154

  Symptoms: Rapid getVPN re-registration by GM when IPsec failure occurs during initial registration. Multiple ISAKMP SAs created and deleted per second.

  Conditions: This symptom is observed on a Cisco ASR 1000 router that is running Cisco IOS Release 15.2(1)S or Cisco IOS Release 15.2(1)S2 as a GM.

  Workaround: There is no workaround.

- CSCtz93922

  Symptoms: An xconnect virtual circuit may be down on one peer while it is up on the remote peer. The output of the **show mpls l2 transport vc detailed** command indicates that it is in the LruRrd state and that the last status it received from the remote peer is pw-tx-fault.

  Conditions: This symptom has been observed when both the attachment circuit and core-facing interfaces are on the same module and that module is reset using the **hw-module module** *module* **reset** command, and the remote peer is running Cisco IOS Release 15.2(02)S or later releases.

Workaround: Do **shutdown** followed by **no shutdown** on the attachment circuit.

- CSCtz95745

  Symptoms: BGP PIC core is broken on shutting an ECMP path towards the BGP next-hop. When one ECMP path is shut, traffic drop is seen for 4-5 seconds and full traffic is recovered after some time.

  Conditions: This symptom occurs when there are uneven number of paths towards two or more BGP next-hops and one path is shut.

  Workaround: Do a shut/no shut on the interface.

- CSCtz97755

  Symptoms: ES card crash and alignment tracebacks on SP are seen.

  Conditions: This symptom is observed with IPv6 unicast and multicast traffic up and running. Unconfiguring IPv6 unicast-routing will lead to this issue.

  Workaround: There is no workaround.

- CSCtz99916

  Symptoms: The Cisco 3945 router does not respond to a reinvite from CVP.

  Conditions: This symptom occurs when call legs are not handled in a proper IWF container.

  Workaround: There is no workaround.

- CSCua04085

  Symptoms: Port-channel member links show as UP when port-channel is admin down.

  Conditions: This symptom is only a display issue.

  Workaround: There is no workaround.

- CSCua07228

  Symptoms: Locally generated traffic is not encrypted when crypto map is applied to the LISP interface.

  Conditions: This symptom occurs when GET VPN or static crypto map is configured on the LISP interface to encrypt traffic between LISP E-IDs.

  Workaround: There is no workaround.

- CSCua08027

  Symptoms: Tracebacks appear on a Cisco ASR router when LI is used with SNMP-based TAP. This issue is seen with Cisco IOS XE Release 3.5S.

  Conditions: This symptom occurs when SNMP-based LI is used with routers running Cisco IOS XE Release 3.5S or later releases.

  Workaround: There is no workaround.

- CSCua08471

  Symptoms: Traffic may go to a wrong destination post switchover on the Cisco ASR 903 router.

  Conditions: This symptom is observed with the VPLS over MPLS-TP scenario. This is an extremely rare scenario, and is seen in less than once out of 50 attempts. The hardware entry corresponding to the VC/TP label is wrongly programmed.

  Workaround: Reconfigure the affected VC post switchover.

- CSCua10377

  Symptoms: A Cisco router with Circuit Emulation SPA may suffer an SPA crash.

  Conditions: This symptom occurs when the CE T1 circuit is configured by the end user for AT&T FDL, and the end user transmits FDL messages requesting 4- hour or 24-hour performance statistics.

  Workaround: There is no workaround. If possible, contact the end user and have them reconfigure their device for ANSI FDL.

- CSCua13418

  Symptoms: RP-Announce packets are being replicated across all the tunnel interfaces and the count of replication is equal to the number of tunnel interfaces. For example, if there are 3 tunnel interfaces, then each tunnel should forward 1 RP-Announce packet each minute (with the default timer configured). However, in this case, each tunnel is forwarding 3 RP-Announce packets across each tunnel interface. This issue is not specific to the number of interfaces. It can happen with any number of tunnel interfaces.

  Conditions: This symptom is observed when filter-autorp is configured with the **ip multicast boundary** command. This issue is seen on the Cisco 3725 router too, where the incoming packets are being replicated because of the **filter-autorp** command.

  Workaround: Removing filter-autorp resolves the issue. However, you need to remove the **pim** and **boundary** commands first and then reapply the pim and boundary list without the **filter-autorp** keyword. Also, doing this might lead to redesigning of the topology to meet specific requirements.

  ```
  int Tun X no ip pim sparse-dense mode no ip multicast boundary XXXXXX filter-autorp
  int TuX ip pim sparse-dense mode ip multicast boundary XXXXXX
  ```

- CSCua16046

  Symptoms: Some packets are dropped when multiple streams are merging on the Cisco ME3600X and ME3800X switches. Sometimes, packet drops are seen with a single stream as well.

  Conditions: This symptom is observed with smaller size packets such as 64-512 bytes.

  Workaround: The workaround depends on the release. With some release, “no ip igmp snooping” will resolve the issue.

- CSCua16786

  Symptoms: When a Cisco 7600 router is placed as a mid-hop-router between the first hop router (FHR) and rendezvous point (RP), with P2P GRE tunnel interface as the FHR facing interface, then PIM-registration might not get completed. The unicast PIM-registration packet might get dropped at the Cisco 7600 router.

  Conditions: This symptom is seen in Cisco IOS Release 12.2(33)SRE6 and RLSx releases.

  Workaround: Delete and create the FHR facing p2p tunnel interface at Cisco 7600 router, which is acting as mid-hop-rtr.

- CSCua18051

  Symptoms: The Cisco ASR 903 router sends duplicated Multicast packets with RPF changes.

  Conditions: This symptom is observed under the following conditions:

  1. Initially, no costs are configured.
  2. Configure OSPF cost to the link to change the RPF path.
  3. Post RPF change, the Cisco ASR 903 router egresses duplicated packets.

  Workaround: There is no workaround.

- CSCua19425

  Symptoms: RP crashes at the far end, pointing to Watchdog Process BGP.

  Conditions: This symptom is observed when doing an FP reload at the near end. This issue is seen with EBGP sessions with BFD configured between near end and far end routers.

  Workaround: There is no workaround.

- CSCua22599

  Symptoms: MCB timeout error message is seen on console. Ports 7 and 8 do not come up.

  Conditions: This symptom is seen when combo ports come up with media-type.

  Workaround: There is no workaround.

- CSCua22755

  Symptoms: The ACL missed blocked ARP reply packets. As a result, the I/F could not learn ARP.

  Conditions: This symptom is observed when the port has 254 BDI I/F, and those 254 BDI I/F have the same ACL. Some of the VLANs ACL blocked ARP reply.

  Workaround: There is no workaround.

- CSCua23997

  Symptoms: Continuous ESP crash is seen after dropping packets due to unsupported OCE.

  Conditions: This symptom is observed when OCE is unsupported.

  Workaround: There is no workaround.

- CSCua25671

  Symptoms: After adding the source interface in RSPAN, there is huge flooding to all trunks allowing RSPAN VLAN starts, even if there is no traffic on the RSPAN source interface.

  Conditions: This symptom is observed under the following conditions:

  1. The router has a RSPAN source session.
  2. The source interface being added to the RSPAN source session is on ES+.
  3. Any of the ES+ modules in the system has an interface on the RSPAN VLAN (that is, at least one of the interfaces on an ES+ module carries RSPAN replicated traffic).
  4. The online diagnostic tests, TestFabricCh0Health and TestFabricCh1Health, are enabled on the ES+ module which has 2 and 3 mentioned above.

  Workaround 1: Disable the online diagnostic tests, TestFabricCh0Health and TestFabricCh1Health, on the ES+ module which has the RSPAN source.

  Workaround 2: If you have to use an interface on the ES+ module as a SPAN source, make sure that no other interface on any of the ES+ modules in the system is in the RSPAN VLAN. If you have to use an interface on the ES+ module to carry RSPAN replicated traffic, make sure that no other interface on any of the ES+ modules in the system is being monitored as an RSPAN source.

- CSCua25748

  Symptoms: The PW receive counter does not work.

  Conditions: This symptom is observed only with the ES+ card. This issue is not seen always due to timing events.

  Workaround: Flap VC again, and check if the counter works. If it does not work, reconfigure the VC.

- CSCua26487

  Symptoms: SNMP loops at OID 1.3.6.1.4.1.9.9.645.1.2.1.1.1, and as a result, SNMP walk fails.

  Conditions: This symptom is observed only on the SNMP getbulk request on 1.3.6.1.4.1.9.9.645.1.2.1.1.1.

  Workaround: Exclude the MIB table from SNMP walk using SNMP view. See the below configurations.

  ```
  snmp-server view <view name> iso included
  snmp-server view <view name> ceeSubInterfaceTable excluded
  snmp-server community <community> view <view name>nterfaceTable excluded
  snmp-server community <community> view <view name>
  ```

- CSCua27842

  Symptoms: The Cisco ASR 1000 router crashes in Firewall code due to NULL l4_info pointer. Day 1 issue.

  Conditions: This symptom occurs when the Cisco ASR 1000 router acts as the MPLS L3VPN UHP. It crashes because FW/NAT requires the l4_info to be set. To trigger this issue, the following features must be configured:

  1. MPLS L3VPN (PE).
  2. Zone-Based FW/NAT.
  3. MPLS & MP-BGP loadbalance configured towards the upstream router.

  Workaround: There is no workaround.

- CSCua30259

  Symptoms: EVC egress traffic does not flow. The frames are dropped by Selene.

  Conditions: This symptom occurs when SPAN is configured on service instance.

  Workaround: There is no workaround.

- CSCua31794

  Symptoms: After reload with the debug image, framed E1 lines are down.

  Conditions: This symptom occurs when checking “show controller SONET”. The default controller framing mode is taken as “crc4”. However, before reload, the configuration for those E1s were configured as “no-crc4”. When configured on the E1s as “no-crc4”, it works fine, and the “show controller SONET” framing output changes to “no-crc4”. As per the running configuration, the configuration does not “no-crc4”, as the default is CRC4. When configuring “no-crc4”, it does not show in the running configuration and is not saved. After reload, it again shows CRC4 and services go down again.

  Workaround: Configure E1s as “no-crc4” and they will work fine, but such changes are not being saved in the configuration. If reload reoccurs, all these services go down again.

- CSCua33287

  Symptoms: ES+: L2TPv3 entries are programmed incorrectly after restart.

  Conditions: This symptom is observed when some L2TPv3 sessions are established on ES+ module. After the restart of ES+, some np entries may not program correctly. As the result, ES+ will stop to transmit packets.

  This condition will recover after executing **shut/no shut** on physical interfaces.

  Workaround: There is no workaround.

- CSCua33527

  Symptoms: Traceback seen after second or third switchover:

  ```
  %LFD-SW2-3-SMBADEVENT: Unexpected event CO_WAIT_TIMEOUT for state RUNNING -Traceback=
  7908E9Cz 7909848z 79099CCz 7909B9Cz 78DBF20z 523292Cz 522C1D4z
  ```

  Conditions: This symptom is observed with a quad-sup scenario/setup. This traceback is seen on the new active RP after second switchover onwards.

  Workaround: There is no workaround.

- CSCua34638

  Symptoms: A crash is seen on RP2, when the **show platform software shell command package** command is issued.

  Conditions: This symptom is observed when the **show platform software shell command package** command is issued. It impacts the RP2 (x86_64_*) image only.

  Workaround: There is no workaround. Do not issue the **show platform software shell command package** command.

- CSCua39107

  Symptoms: In a FlexVPN Spoke to Spoke setup, Resolution reply goes via the Tunnel interface to the Hub.

  Conditions: This symptom is only observed when NHO is added for the V-Access, overriding an existing route. This issue is not seen when H route is added.

  Workaround: Distribute the summarized address from the Hub, thus avoiding addition of NHO at the Spokes. The Spokes will then add H route instead of NHO.

- CSCua40790

  Symptoms: Memory leaks when SNMP polling cbgpPeer2Entry MIB.

  Conditions: This symptom occurs when BGPv4 neighbors are configured.

  Workaround: There is no workaround if this MIB is to be polled.

- CSCua42089

  Symptoms: Configuring Ingress redirection for service group 61 (Mask) and applying an extended ACL in the outbound direction on the same interface causes software switching even when there are no punt entries in the TCAM.

  Conditions: This symptom is observed when WCCP service 61 with Mask assignment in the Ingress indirection, along with an outbound ACL, is configured on the same interface.

  Workaround: Do not configure the outbound ACL along with a WCCP service.

- CSCua43930

  Symptoms: Checksum value parsed from GRE header is not populating causing the GRE tunnel checksum test case to fail.

  Conditions: This symptom is observed on a Cisco ISR G2.

  Workaround: There is no workaround.

- CSCua48584

  Symptoms: The Cisco ME 3600X's ARP resolution may fail after flexlink switchover.

  Conditions: This symptom is observed on the Cisco ME 3600X running Cisco IOS Release 15.2(S) or Cisco IOS Release 15.2(2)S1 with flexlink configured.

Workaround: Shut the active port of the flexlink pair. In other words, do a manual switchover through CLI.

- CSCua62054

  Symptoms: Egress DSCP classification does not work when a policy is applied on the main interface which has trunk EFP configured.

  Conditions: This symptom is observed when a DSCP-based service policy is configured on the main interface and it does not classify the traffic for DSCP.

  Workaround: Use normal EFP instead of trunk.

- CSCua62102

  Symptoms: Traffic is classified based on prec/dscp/tos, along with Layer 4 (TCP/UDP) ACLs in the service policy. This issue is not seen without ACLs.

  Conditions: This symptom is observed when you configure policy-map matching prep/dscp/tos with Layer 4 TCP/UDP ACLs in the ingress direction.

  Workaround: There is no workaround.

- CSCua64546

  Symptoms: In a scaled setup with IPV4 and IPV6 ACL together (not necessarily on the same interface), IPV4 ACLs may stop working if the IPV6 ACL configured later overwrites the IPv4 ACL results and vice versa.

  Conditions: This symptom is observed with IPV4 and IPV6 ACLs configured on the box.

  Workaround: There is no perfect workaround. Reconfiguring the IPV4 ACL can recover the functionality but will affect the IPV6 ACL.

  Further Problem Description: Only the IPV4 or IPV6 ACL configuration will work.

- CSCua64700

  Symptoms: The IPsec tunnel state goes to Up-Idle after 4-5 days of the router being up and running.

  Conditions: This symptom is observed if you have low rekey value, as with the rekey, the new SPI gets allocated. This issue is seen with WS-IPSEC-3 and to verify this, check the below counter.

  ```
  show crypto ace spi
  ```

  If there is no decrement in the SPI allocated counter and there is a consistent increment in the counter, the chances are high that you will encounter this issue.

  Once the value reaches 61439, you will encounter this issue.

  ```
  MTCVPNK03#sh cry ace spi
  SPI in use .......................... 0
  Normal SPI allocated ................ 61439
  ```

  Workaround: There is no workaround. You need to reload the box.

- CSCua68398

  Symptoms: The ES+ card crashes.

  Conditions: This symptom is observed with a scaled EVC and VPLS configurations.

  Workaround: Stop the traffic. After the line cards boot up and the ports are up, start the traffic.

- CSCua79516

  Symptoms: SYN packets to establish ftp-data connections are sporadically dropped at the Cisco ASR router.

Conditions: This symptom is observed under the following conditions:

- Using the active mode FTP.
- Using PAT.
- The symptom is observed on a Cisco ASR 1000 router.

Workaround 1: Use the passive mode FTP.

Workaround 2: Use the static NAT/dynamic NAT configuration.

- CSCua85837

  Symptoms: Depending on the aces in the redirect-list ACL used, only a subnet of the traffic gets redirected based on ports.

  Conditions: This symptom is observed when the WCCP service has a redirect-list ACL applied which in turn has port-specific aces in them.

  Workaround: Remove the L4 operators from the redirect-list ACL.

- CSCua85934

  Symptoms: A session provisioning failure is seen in the ISG-SCE interface. The deactivate or disconnect request has the message authenticator wrongly calculated.

  Conditions: This symptom is observed with the ISG-SCE interface.

  Workaround: There is no workaround.

- CSCua87877

  Symptoms: A crash occurs in ucode.

  Conditions: This symptom is observed with 160cps SIP calls.

  Workaround: There is no workaround.

- CSCua98690

  Symptoms: The ES+/ES20/SIP-400 (any card which supports EVC) card may crash due to memory corruption.

  Conditions: This symptom is observed when the MAC ACL is configured on EFP.

  Workaround: There is no workaround.

- CSCub01576

  Symptoms: ESP reloads on the Cisco ASR 1000 router due to ucode crash.

  Conditions: This symptom is observed on the Cisco ASR 1000 router where the Layer 4 Redirect feature is configured. This problem was first introduced in Cisco Release 15.2(01)S. This issue may be not seen at all in some customer environments to about once a week in medium-sized high CPS ISG production networks.

  Workaround: There is no workaround.

- CSCua09073

  Symptoms: If 6708 generates txCRC errors, CSCtq73026 accounts for these errors in TestErrorMonitor diagostic test and takes the necessary recovery action. But for CSCtq73026 to be invoked, the TestErrorMonitor test should be included in the test suite for 6708. This test is missing and hence, the fix in CSCtq73026 will also not be invoked.

  Conditions: See the description of CSCtq73026. For this fix to be take effect, TestErrorMonitor should be added in the test suite. In this DDTS, we are adding this test so that in case of an error, as mentioned in CSCtq73026, recovery action will be triggered.

Workaround: There is no workaround.

- CSCtq48455

  Symptoms: After Flex Link failover, all VLAN SVIs associated with VLANs forwarding on the Flex Link interfaces go down.

  Conditions: This symptom is observed with Flex Links configured with VLAN SVIs.

  Workaround: Remove the Flex Links and then reconfigure them.

- CSCtw51052

  Symptoms: HSRP hello packets are dropped on a Cisco ME 3600X switch when there are two Cisco ME 3600X switches acting as switches between the HSRP boxes, and there is a port-channel connecting the two ME 3600 switches with both the Tengig ports as its members. HSRP is configured on VLANs.

  Conditions: This symptom is not seen consistently. It is seen only on a few VLANs while the others may be working as expected.

  Workaround: Removing and readding the VLANs fixes the issue. Issue the **no vlan** *vlan-id* command followed by the **vlan** *vlan-id* command. Removing and adding the VLAN from the port-channel and its members may also fix the issue.

- CSCtx54990

  Symptoms: The **static mac address** command disappears randomly on reload on a Cisco ME 3600X switch running the me360x-universalk9-mz.151-2.EY image.

  Conditions: This symptom occurs randomly. This issue has been seen in several customer switches and in the lab.

  Workaround: Reapply the **static** commands after reload. There is no other workaround.

- CSCty20330

  Symptoms: SNMP requests a large block of memory.

  ```
  Feb 15 23:44:28.285 CST: %SYS-2-MALLOCFAIL: Memory allocation of 2424504504
  bytes failed from 0x15047BC, alignment 0
  Pool: Processor  Free: 803990516  Cause: Not enough free memory
  Alternate Pool: None  Free: 0  Cause: No Alternate pool
   -Process= "SNMP ENGINE", ipl= 0, pid= 264
  ```

  Conditions: This symptom is observed with SNMP.

  Workaround: There is no workaround.

- CSCtz48867

  Symptoms: In the customer network, this problem was triggered under the following situation:

  ```
  Active WG          Standby WG

     |                  |

     |                  |

  Active BR -------- Standby BR

     |

     |

  Client
  ```

"Active BR" and "Standby BR" are two Cisco ME 3600X switches. The link between the two Cisco ME 3600X switches is an etherchannel (two member ports). Multicast traffic from the "Active WG" and "Standby WG" flow down the path. The multicast clients join the multicast group via an SVI interface in the two switches and the L2 etherchannel between the switches trunks that particular VLAN.

In a normal situation, the client should be able to receive multicast streams 224.0.1.x (from Active WG) and 224.0.127.x (from Standby WG). After Active BR is reloaded, multicast streams 224.0.127.x can no longer be forwarded from the Standby BR to the Active BR.

Conditions: This symptom occurs when the Active BR is reloaded. In a normal situation, the client should be able to receive multicast streams 224.0.1.x (from Active WG) and 224.0.127.x (from Standby WG). After the Active BR is reloaded, multicast streams 224.0.127.x can no longer be forwarded from the Standby BR to the Active BR.

Workaround: After a "clear ip mroute *" in the standby BR, the problem is resolved.

- CSCua84606

  Symptoms: With L2PT tunnel or forwarding, the Cisco ME 3600X switch or the Cisco ME 3800X switch cannot process more than two VLAN tags. Such packets get dropped.

  Conditions: This symptom is observed with L2PT tunnel or forwarding. The Cisco ME 3600X switch or the Cisco ME 3800X switch cannot process more than two VLAN tags. Such packets get dropped.

  Workaround: There is no workaround.

- CSCtw79171

  Symptoms: Platform asserts at adjmgr_l2_create.

  Conditions: This symptom occurs with excessive flapping of a link.

  Workaround: There is no workaround.

- CSCty50421

  Symptoms: With control word set (C bit) explicitly in MPLS bindings for the VC, the L2PT tunnel over EFP xconnect does not work.

  Conditions: This symptom is observed when control word is set (C bit) explicitly in MPLS bindings for the VC.

  Workaround: Disable control word.

- CSCua14594

  Symptoms: Memory leak is seen when polling for the following PW MIBS:

```
1.3.6.1.4.1.9.10.106.1.5.1.1 (cpwVcPerfTotalInHCPackets)
1.3.6.1.4.1.9.10.106.1.5.1.2 (cpwVcPerfTotalInHCBytes)
1.3.6.1.4.1.9.10.106.1.5.1.3 (cpwVcPerfTotalOutHCPackets)
1.3.6.1.4.1.9.10.106.1.5.1.4 (cpwVcPerfTotalOutHCBytes)

Address    Size   Alloc_pc  PID  Alloc-Proc       Name
34417B84      308 13774B30  473  SNMP ENGINE     AToM VC event trace
```

  This memory leak, on repeated polling, may lead to device crash.

  Conditions: This symptom is observed with Cisco IOS Release 3.6S upon polling of the SNMP VC statistics query.

  Workaround: There is no workaround.

- CSCub25360

Symptoms: In a Flexlink switchover scenario, it seems that for some reason, the Cisco ME 3600X switch does not sent out a dummy Mcast packet for the SVI.

Conditions: This symptom is observed with a Cisco ME 3600X Flexlink switchover.

Workaround: There is no workaround.

- CSCtg47129

  Symptoms: Enhancements in NAT processing are seen in VRF environments.

  Conditions: This symptom is observed with packets that need NAT in a VRF.

  Workaround: There is no workaround.

- CSCua66308

  Symptoms: Classification-related error messages and tracebacks are seen on the CLI console, and the configuration is not downloaded to the data path.

  Conditions: This symptom is observed with large configurations with multiple deny statements.

  Workaround: Observe caution when using deny statements in a configuration.

- CSCuc68092

  Symptoms: A CPU hog and an LDP flap is seen on executing the **sh int transceiver detail** command.

  Conditions: This symptom occurs after executing the **sh int transceiver detail** command for the first time after the box is reloaded.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.2(2)S1

Cisco IOS Release 15.2(2)S1 is a rebuild release for Cisco IOS Release 15.2(2)S. The caveats in this section are resolved in Cisco IOS Release 15.2(2)S1 but may be open in previous Cisco IOS releases.

- CSCtl01184

  Symptoms: Sometimes an EVC that is configured on ES+ sends frames out with CFI bit set in the VLAN tag.

  Conditions: This symptom is observed on EVCs that are configured on ES+.

  Workaround: There is no workaround.

- CSCtr47317

  Symptoms: After a switchover, a Cisco Catalyst 6500 series switch may be replicating some spanned traffic indefinitely and flooding the network with the span copies.

  Conditions: The issue is seen after the following sequence:

  - An internal service module session for a FWSM or other service modules exists:

    ```
    UUT#show monitor session all
    Session 1
    Type  : Service Module Session
    ```

  - If you attempt to configure a span session with the session number already in use:

    ```
    UUT(config)#monitor session 1 source interface Gi2/7 , Gi2/40
    % Session 1 used by service module
    ```

  - The command seems to be rejected, but it is synchronized to the standby supervisor.

  - A switchover happens.

  Workaround: There is no workaround.

- CSCts40043

  Symptoms: A Cisco router may crash due to a segmentation fault.

  Conditions: The symptom is observed when a fail-close ACL is applied to the GDOI crypto map in GETVPN implementation.

  Workaround: There is no workaround.

- CSCtt35379

  Cisco IOS Software contains a vulnerability in the Border Gateway Protocol (BGP) routing protocol feature.

  The vulnerability can be triggered when the router receives a malformed attribute from a peer on an existing BGP session.

  Successful exploitation of this vulnerability can cause all BGP sessions to reset. Repeated exploitation may result in an inability to route packets to BGP neighbors during reconvergence times.

  Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability. This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-bgp

- CSCtt99627

  Symptoms: The **lacp rate** and **lacp port priority** commands may disappear following a switchover from active to standby RP.

  Conditions: This affects the Cisco 7600 platform.

  Before performing a switchover one may check the configuration on the standby RP to see if the commands are present or not. If the commands are not present on the standby RP then they will disappear if a switchover occurs.

  Workaround: Prior to switchover if the commands do not show up on the standby RP as described above, then unconfiguring and reconfiguring the command on the active RP will fix the issue.

  Otherwise if the commands disappear after a switchover then the commands must be reconfigured on the newly active RP.

- CSCtu32301

  Symptoms: Memory leak may be seen.

  Conditions: This is seen when running large **show** commands like **show tech-support** on the line card via the RP console.

  Workaround: Do not run the show commands frequently.

- CSCtu35052

  Symptoms: Sweep ping fails when an ATM interface is configured with AAL5 encapsulation.

  Conditions: This symptom occurs when the ATM packet size is greater than 1484 bytes.

  Workaround: There is no workaround.

- CSCtu40028

  Symptoms: The SCHED process crashes.

  Conditions: The issue occurs after initiating TFTP copy.

Workaround: There is no workaround.

- CSCtw46061

  Symptoms: The following output shows the leaked SA object continuing to be in the "OBJECT_IN_USE" state. The state is supposed to be changed to OBJECT_FREEING by crypto_engine_delete_ipsec_sa(). This is in turn being called by ident_free_outbound_sa_list().

```
shmcp-fp40#sh crypto eli
Hardware Encryption : ACTIVE
Number of hardware crypto engines = 1
CryptoEngine IOSXE-ESP(14) details: state = Active
Capability    : DES, 3DES, AES, RSA, IPv6, GDOI, FAILCLOSE

IKE-Session   :     0 active, 12287 max, 0 failed
DH            :   211 active, 12287 max, 0 failed
IPSec-Session :   323 active, 32766 max, 0 failed
```

  Conditions: This symptom is observed on a Cisco ASR 1000 series router

  Workaround: There is no workaround.

- CSCtw78451

  Symptoms: A Cisco ASR 1000 series router may reload when multiple users are logged in running **show** commands.

  Conditions: This symptom is only seen when the Cisco ASR router is used as a DMVPN headend and there are hundreds of tunnels flapping.

  Workaround: There is no workaround. However, this appears to be a timing issue when there is instability in a large-scale environment.

- CSCtw80678

  Symptoms: Multilink PPP ping fails when the serial interfaces experience QMOVESTUCK error.

  Conditions: This symptom may be observed if multilink PPP member links and serial interfaces on which the QMOVESTUCK error is reported are on the same SPA.

  Workaround: There is no workaround.

- CSCtw95466

  Symptoms: When a large number of Ethernet or VLAN xconnect sessions are configured on a Cisco 7600 router, the Supervisor Processor may reload.

  Conditions: This symptom is observed when **aaa new-model** is configured.

  Workaround: Configure **no aaa new-model**.

- CSCtw99989

  Symptoms: During normal operation a Cisco ASR 1000 Series Aggregation Services router may show the following traceback:

```
%FMANRP_ESS-3-ERREVENT: TC still has features applied. TC evsi
```

  Conditions: The symptom is observed during PPP renegotiation.

  Workaround: There is no workaround.

- CSCtw99991

  Symptoms: Chunk memory leak is seen in the ES+ LC after configuring the IP source guard EVC configurations.

Conditions: This issue is seen on a Cisco 7600 router with ES+ LC running Cisco IOS interim Release 15.2(01.16)S.

Workaround: There is no workaround.

- CSCtx02522

  Symptoms: The router displays intermittent traceback errors.

  Conditions: Occurs when you configure REP.

  Workaround: There is no workaround.

- CSCtx04709

  Symptoms: Some EIGRP routes may not be removed from the routing table after a route is lost. The route is seen as “active” in the EIGRP topology table, and the active timer is “never”.

  Conditions: This symptom is seen when a multiple route goes down at the same time, and query arrives from neighbor router. Finally, neighbor detects SIA for affected router and neighbor state is flap. However, active entry is remaining after that, and route is not updated.

  Workaround: The **clear ip eigrp topology** *network mask* command may remove unexpected active entry.

- CSCtx11740

  Symptoms: The traffic convergence takes longer because of additional/unwanted traffic is punted to CPU as we do not have *,GM code changes. The *,GM entries help drop the traffic that is not needed by MFIB (PI) code.

  Conditions: This symptom is seen with link and node failures in dual-home scenarios.

  Workaround: There is no workaround.

- CSCtx32329

  Symptoms: When using the **show ipv6 rpf** command, the router crashes or displays garbage for RPF idb/nbr.

  Conditions: This symptom can happen when the RPF lookup terminates with a static multicast route that cannot be resolved.

  Workaround: Do not use static multicast routes, or make sure that the next hop specified can always be resolved. Do not use the **show** command.

- CSCtx35064

  Symptoms: Traffic remains on blackholed path until holddown timer expires for PfR monitored traffic class. Unreachables are seen on path, but no reroute occurs until holddown expires.

  Conditions: This symptom is seen under the following conditions:

  - MC reroutes traffic-class out a particular path (BR/external interface) due to OOP condition on the primary path.
  - Shortly after enforcement occurs, an impairment on the new primary path occurs causing blackhole.
  - PfR MC does not declare OOP on the new primary path and attempt to find a new path until holddown timer expires. Causes traffic loss.

  Workaround: Reduce the holddown timer to 90 seconds (minimum value) to minimize impact.

- CSCtx37768

  Symptoms: QoS classification does not match traffic against an egress policy map between MPLS and IP access.

Conditions: This symptom is observed when a QoS policy is applied on an EVC bridge domain interface.

Workaround: Use one of the following workarounds:

- Reload the router.
- Remove and re-apply an encapsulation configuration such a VLAN.
- Remove and re-attach the bridge domain under the EVC.
- Perform a **shutdown/no shutdown** on the BDI interface.

- CSCtx49073

  Symptoms: Free space check fails and IOS core dump never completes.

  Conditions: The symptom is observed when there is not enough storage media space for Cisco IOS core dump.

  Workaround: Make sure there is enough storage space for Cisco IOS core dump.

- CSCtx66011

  A vulnerability in the Internet Key Exchange (IKE) protocol of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a memory leak that could lead to a device reload.

  The vulnerability is due to incorrect handling of malformed IKE packets by the affected software. An attacker could exploit this vulnerability by sending crafted IKE packets to a device configured with features that leverage IKE version 1 (IKEv1).

  Although IKEv1 is automatically enabled on a Cisco IOS Software and Cisco IOS XE Software when IKEv1 or IKE version 2 (IKEv2) is configured, the vulnerability can be triggered only by sending a malformed IKEv1 packet.

  In specific conditions, normal IKEv1 packets can also cause an affected release of Cisco IOS Software to leak memory.

  Only IKEv1 is affected by this vulnerability.

  An exploit could cause Cisco IOS Software not to release allocated memory, causing a memory leak. A sustained attack may result in a device reload.

  Cisco has released free software updates that address this vulnerability. There are no workarounds to mitigate this vulnerability.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130925-ike

  Note: The September 25, 2013, Cisco IOS Software Security Advisory bundled publication includes eight Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the September 2013 bundled publication.

  Individual publication links are in “Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication” at the following link:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep13.html

- CSCtx80078

  Symptoms: Packets are getting punted to CPU or being forwarded with EVC mac security.

  Conditions: This symptom is seen with implicit deny of packets with routable IPv4 header.

Workaround: There is no workaround.

- CSCtx82775

  Symptoms: Calls on the Cisco ASR 1000 series router seem to be hung for days.

  Conditions: The symptom is observed when MTP is invoked for calls.

  Workaround: Reload the router or perform a no sccp/sccp.

- CSCtx84948

  Symptoms: A Cisco ASR 1000 series router malfunctions after consecutive ESP crashes triggered by CSCtr56576. This symptom is observed when the interfaces are up/up but are not sending traffic. You can also identify this state using the following command:

  ```
  Router#show platform software interface fp active name GigabitEthernet5/0/0
  Name: GigabitEthernet5/0/0, ID: 23, QFP ID: 22, Schedules: 4096
  Type: PORT, State: disabled, SNMP ID: 16, MTU: 1500   <<<<<<
  ```

  The output of the command indicates that at the ESP level, the interface is disabled and can not forward traffic.

  Conditions: The Cisco ASR 1000 series router has redundant ESPs and consecutive ESP crashes. This symptom has been caused only by CSCtr56576.

  Workaround: **Shut/no shut** the disabled interface to resume the traffic.

- CSCtx85247

  Symptoms: An ES20 line card is reset on doing redundancy switchover of RSPs.

  Conditions: This symptom is seen with redundancy switchover of RSPs.

  Workaround: There is no workaround.

- CSCtx85489

  Symptoms: A memory leak is followed by a router crash.

  Conditions: This issue is seen in a Cisco 7600 router that is running Cisco IOS Release 15.2(2)S. Configuring and unconfiguring PBR “N” number of times from an interface triggers the crash. The root cause for this issue is that each time when PBR is configured and unconfigured, memory is leaked.

  Workaround: There is no workaround.

- CSCtx91831

  Symptoms: IP address of the SVI interface is not installed in the routing table.

  Conditions: When we have an IP address configured for the BD, the following sequence of configurations puts the box in a state where the corresponding ip- address is not installed in the routing table.

  ```
  no vlan <vlan-id> --- same as the BD
  Int vlan <vlan-id> shutdown --- At this point the Int vlan goes down no shutdown
  vlan <vlan-id>
  ```

  This issue seen only when we have SVI and BD EFP and will not be seen for SVI and trunk ports.

  Workaround: A **shut/no shut** of the interface VLAN after adding the **vlan** *vlan-id* command fixes the problem.

- CSCtx94279

  Symptoms: A line card crashes.

Conditions: This symptom is observed in switch traffic and flood traffic (line rate and less that 128-byte packet size) with more than one port in the egress path flood.

Workaround: There is no workaround.

- CSCtx94393

  Symptoms: ESP crashes at fman_avl_free.

  Conditions: The symptom is observed with the following conditions:

  - Scale IKEv2 4k IPsec sessions with FlexVPN dVTI server.
  - Scale IKEv1 1k IPsec sessions with dVTI server.
  - CAC (50) enabled on both server and clients.
  - DPD (60/15/on-demand) enabled.
  - Do a **clear crypto session** per 20 minutes on server.
  - 20M bidirectional traffic

  Workaround: There is no workaround.

- CSCtx94772

  Symptoms: Cannot configure xconnect on an SVI when an RFP having the same BD is configured with pop 2 symmetric.

  Conditions: This issue is seen only when EFP is configured first and then the xconnect over SVI.

  Workaround: Configure the xconnect over SVI before configuring the RFP with the same pop 2 and same BD.

- CSCty06191

  Symptoms: When an IPHC configuration is applied on a multilink bundle interface and the interface is flapped, the IPHC configuration does not apply successfully on a line card.

  Conditions: The symptom is observed with a multilink interface flap.

  Workaround: Unconfigure and then reconfigure the IPHC configuration on the multilink interface.

- CSCty14596

  Symptoms:

  1. PIM neighbor is not established over routed pseudowire.
  2. PW cannot pass PIM traffic when destination LTL in DBUS header is 0x7ff8.

  Conditions: These symptoms are seen under the following conditions:

  - Configure PIM over routed pseudowire.
  - Core facing card is ES+.
  - Outgoing interface of the PW is a TE Tunnel over the physical interface.
  - Cisco IOS 15.0(1)S and later releases.

  Workaround: Make the outgoing interface of PW:

  1. Over physical interface only (i.e. without tunnel).
  2. TEFRR over port-channel interface.
  3. Issue will not be observed on ES20.
  4. Issue will not be observed in Cisco IOS Release 15.0(1)S and later releases.

- CSCty16620

  Symptoms: Backup pseudowire in SVIEoMPLS does not come up after reloading the router.

  Conditions: This symptom is seen under the following conditions:

  1. Remote PE on the backup PW does not support pseudowire status TLV.
  2. The “no status TLV” is not configured in pw-class used in the PW, which does not support pseudowire status TLV.

  Workarounds:

  Proactive workaround: Configure “no status TLV” into the pw-class used if the remote side does not support status TLV.

  Reactive workaround: Reprovision the backup pseudowire after reload.

- CSCty19713

  Symptoms: The ESP or CPP of a Cisco ASR 1000 series router crashes.

  Conditions: This symptom is observed in the NAT Application Layer Gateway (ALG) for DNS packets.

  Workaround: There is no workaround.

- CSCty23747

  Symptoms: MAC address withdrawal messages are not being sent.

  Conditions: This symptom is seen with flapping REP ports on UPE.

  Workaround: There is no workaround.

- CSCty28384

  Symptoms: The police actions are not accepted if given in different commands.

  Conditions: If police actions are given in different commands, they are not accepted.

  Workaround: Configure the policer actions in a single command.

- CSCty28796

  Symptoms: The **show snmp mib | in flash** command on the router does not show any flash entries. Also snmpwalk for flash objects shows the following error:

  ```
  "No Such Object available on this agent"
  ```

  Conditions: This symptom is observed on Cisco ME 3600X and ME 3800X.

  Workaround: There is no workaround.

- CSCty30886

  Symptoms: A standby RP reloads.

  Conditions: This symptom is observed when bringing up PPPoE sessions with configured invalid local IP address pool under virtual-template profile and “aaa authorization network default group radius” on the box with no radius present. No IP address is assigned to PPPoE Client.

  Workaround: There is no workaround.

- CSCty32728

  Symptoms: CPU hog is seen when MVPN configuration is replaced with another using the **configure replace** command.

  Conditions: This symptom is observed on a stable MVPN network when replacing the configuration with dual-home receiver/source configuration once the router comes up with the tunnel.

Workaround: There is no workaround.

- CSCty34200

  Symptoms: In MVPN scale environment, a crash is observed after “no ip multicast-routing”. A memory leak is observed after changing data MDT address.

  Conditions: This symptom is seen in MVPN scale scenario.

  Workaround: There is no workaround.

- CSCty42626

  Symptoms: Certificate enrollment fails for the Cisco 3945 router and the Cisco 3945E router due to digital signature failure.

  Conditions: This symptom is observed when the Cisco 3945 router or the Cisco 3945E router enrolls and requests certificates from a CA server.

  Workaround: There is no workaround.

- CSCty45999

  Symptoms: The “aps group acr 1” line disappears after power off and on a Cisco 7600 router in working and protection groups.

  Conditions: This symptom occurs when the Cisco 7600 router suddenly loses power, and the “aps group acr 1” line does not appear again. If you run the **show controller SONET 1/1/0** command, you will see every E1 on “unconfigured” status.

  Workaround: Delete the “aps protect 1 X.X.X.X” & “aps working 1” lines. The “framing” must be changed in order to delete every E1 channel configuration, then “framing” should be configured as it was in the beginning. Then “aps group acr 1” line is configured as well as “aps protect 1 X.X.X.X” and “aps working 1” lines. Finally every E1 must be configured as it was before this issue occurs. You can copy the E1 configuration before to delete anything and then paste it at the end.

- CSCty46022

  Symptoms: A Cisco ASR 1000 experiences high ESP CPU constantly.

  Conditions: The symptom is observed when ISG sessions with DHCP initiator are experiencing fragmented traffic and the fragmented traffic has a small packet size. The packets will be punted to ESP CPU and cause it to be busy.

  Workaround: There is no workaround.

- CSCty51088

  Symptoms: On a Cisco ME 3600X or Cisco ME 3800X, when traffic for a group (S2,G) is sent to an interface that is already acting as the source for another group (S1,G), it does not receive any traffic since no (S2,G) entry is formed.

  Conditions: This symptom is observed when the receiver interface is already a source interface for another multicast stream.

  Workaround: None

- CSCty52047

  Symptoms: IKE SAs are not getting deleted by DPD (crypto isakmp keepalive).

  Conditions: This symptom is observed on a Cisco ASR 1000 router with DPD enabled.

  Workaround: Manually delete the stuck isakmp session:

  clear crypto isakmp conn-id

  You can get the conn-id from the output of the **show crypto isakmp sa** command.

- CSCty54319

  Symptoms: OSPF and protocols using 224.0.0.x will not work btw CE-CE over a VLAN.

  Conditions: This symptom occurs when IGMP snooping is disabled.

  Workaround: Toggle IGMP snooping two times.

- CSCty54885

  Symptoms: The Standby RP crashes when the Active RP is removed to do a failover.

  Conditions: This symptom is observed when the last switchover happens with redundancy forced-switchover.

  Workaround: Do a switchover only with redundancy forced-switchover instead of removing the RP physically.

- CSCty57746

  Symptoms: On the Cisco ASR 903 router, the **show environment** command displays incorrect values, including P0 and P1 voltages and Amps values.

  Conditions: This symptom is observed with the Cisco ASR 903 router when you apply the **show environment** command.

  Workaround: There is no workaround.

- CSCty58656

  Symptoms: A Cisco 7600 series router with ES+ module may crash.

  Conditions: The symptom is observed with the QoS policy map that has a name hash that is same as an existing policy used by the ES+ module and configuring a child policy or adding a child policy that is already in use.

  Workaround: Do not call a child policy map.

- CSCty60467

  Symptoms: SSM ID leak issues or SSM stats show unprovisioned segment counters. The leak can be observed with the command **show ssm stats**. Look for the following in the output:

  ```
  Segment States Counters
    Type            Class           State           Count
    IP-SIP          SSS             Unprov          1050  <<< the count
  indicates the IDs are getting leaked.
  Alarm: Counter reaches 1 Million: indicates you may be nearing ID exhaust state.
  ```

  Conditions: The symptom is observed with the following steps:

  1. Configure “ip dhcp ping packets 10” on an ISG.
  2. Initiate an L2-connected ISG DHCP session by triggering DHCP discover from the client.
  3. Start TCP traffic from the client immediately.
  4. The issue can be observed commonly on high CPS (greater than best practice).
  5. Observed in Cisco IOS XE Release 3.2 and XE 3.5.

  Workaround: Configuring “ip dhcp ping packets 0” will bring down the rate of SSM ID leak.

- CSCty61212

  Symptoms: The removal of crypto map hangs the router.

  Conditions: This symptom is observed with the removal of GDOI crypto map from interface.

Workaround: There is no workaround.

- CSCty62559

  Symptoms: On the Cisco ASR 1000 series router, FP crash occurs at cpp_qm_obj_add_to_parent with 8k xconnects.

  Conditions: This symptom is observed with the Cisco ASR 1000 series router while doing SPA reload after RP switchover with 8k xconnects.

  Workaround: There is no workaround.

- CSCty62887

  Symptoms: When more than 1024 DTL requests are made during free sip msg_info pool, the Cisco ASR 1000 will crash.

  Conditions: Multiple factors could contribute to this. It depends on the number of messages contained in SIP ALG.

  Workaround: There is no workaround.

- CSCty68402

  Symptoms: NTT model 4 configurations are not taking effect.

  Conditions: This symptom occurs under the following conditions:

```
policy-map sub-interface-account
 class prec1
  police cir 4000000 conform-action transmit  exceed-action drop
  account
 class prec2
  police cir 3500000 conform-action transmit  exceed-action drop
  account
 class prec3
  account
  class class-default fragment prec4
  bandwidth remaining ratio 1
  account

policy-map main-interface
 class prec1
  priority level 1
  queue-limit 86 packets
 class prec2
  priority level 2
  queue-limit 78 packets
 class prec3
  bandwidth remaining ratio 1
  random-detect
  queue-limit 70 packets
  class prec4 service-fragment prec4
  shape average 200000
  bandwidth remaining ratio 1
  queue-limit 62 packets
 class class-default
  queue-limit 80 packets
```

Workaround: There is no workaround.

- CSCty76106

  Symptoms: Crash is seen after two days of soaking with traffic.

  Conditions: This symptom occurs with node acting as ConPE with multiple services like REP, MST, L3VPN, L2VPN, constant frequent polling of SNMP, RCMD, full scale of routes and bidirectional traffic.

  Workaround: There is no workaround.

- CSCty81700

  Symptoms: When a remote PE reloads in MVPN network, it causes a memory leak.

  Conditions: This symptom occurs when core interface flap or remote PE node reloads causing a small amount of memory leak. If the node stays up experiencing a lot of core interface/remote PE outages, it can run out of memory and fail to establish PIM neighborship with remote PEs.

  Workaround: There is no workaround. As a proactive measure, user can periodically (depending on n/w outages) run the **show memory debug leak chunk** command and reload the node, if there are a lot of memory leaks reported by this command.

- CSCty82888

  Symptoms: Removing an ATM Permanent Virtual Path (PVP) by the **no atm pvp** command while it is configured with the **xconnect** command causes a memory leak. This can be observed using the **show circuit memory** command:

  ```
  Router#show acircuit memory | include AC ctx chunks
    AC ctx chunks            :        200/32820      (  0%) [      2] Chunk
  ```

  Also, on a dual-RP system with stateful switchover enabled, if the PVP is immediately reconfigured and the **xconnect** command is added, the standby RP may reload.

  Conditions: These symptoms have been observed on Cisco routers that are running Cisco IOS Release 15.2(2)S.

  Workaround: Unconfigure the xconnect using the **no connect** command before removing the PVP.

- CSCty91955

  Symptoms: L2-switched traffic loss within a BridgeDomain routed traffic via an SVI experiences no loss.

  Conditions: This symptom occurs with BridgeDomain that has both tagged and untagged EVCs. Issue should not happen with like-to-like scenario.

  Workaround: Make sure there is like-to-like (tagged-to-tagged or untagged-to- untagged) communication.

- CSCty93290

  Symptoms: Momentary traffic loss of multicast traffic with QoS configuration on EFP is observed.

  Conditions: This symptom is seen under the following conditions:

  1. Have multiple VLANs in OIF list.
  2. Each VLAN should have only one EFP/sp.
  3. Have QoS configured on EFPs.

  Workaround: There is no workaround.

- CSCty96049

  Cisco IOS Software contains a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. An attacker could exploit this vulnerability by sending a single DHCP packet to or through an affected device, causing the device to reload.

  Cisco has released free software updates that address this vulnerability. A workaround that mitigates this vulnerability is available. This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-dhcp

- CSCty96263

  Symptoms: Under periods of transient interface congestion, an MPLS-TP network may experience unnecessary traffic switchovers or longer than expected restoration times.

  Conditions: This symptom is observed during periods of transient interface congestion. Behavior will be caused by loss of pseudowire status packets. Lack of a classification mechanism for these packets prevents user from protecting them with a QoS policy.

  Workaround: There is no workaround.

- CSCty96579

  Symptoms: Under periods of transient interface congestion, an MPLS-TP network may experience unnecessary traffic switchovers or longer than expected restoration times.

  Conditions: This symptom is observed during periods of transient interface congestion. Behavior will be caused by loss of vital OAM packets (e.g. AIS/LDI, LKR). Lack of a classification mechanism for these packets prevents from protecting them with a QoS policy.

  Workaround: There is no workaround.

- CSCty99331

  Symptoms: CPU hog messages are seen on the console.

  Conditions: This symptom is seen when applying huge rmap with more than 6k sequences on an interface.

  Workaround: There is no workaround.

- CSCty99711

  Symptoms: SIP-400 crash may be observed due to illegal memory access.

  Conditions: This symptom is observed with Cisco IOS Release 12.2(33)SRE4 when SIP-400 has PPPoE session scale.

  Workaround: There is no workaround.

- CSCtz01361

  Symptoms: Traffic gets black holed when TE auto-backup is enabled on midpoint router and FFR is configured on the P2MP TE tunnel head end.

  Conditions: This symptom is seen when enabling FRR on the head end with auto- backup already configured on the box.

  Workaround: Remove auto-backup configuration from the midpoint router.

- CSCtz04090

  Symptoms: In a VRRP/HSRP setup, traffic from particular hosts is getting dropped. Ping from the host to any device through the VRRP routers fails.

  Conditions: This symptom is usually seen after a VRRP/HSRP switchover. The packet drops because of some packet loop that is created between the routers running VRRP/HSRP.

Workaround: A clear of the MAC table on the new VRRP master usually restores the setup to working conditions.

- CSCtz13451

  Symptoms: A Cisco ME 3800X and Cisco ME 3600X switch may experience CPU HOG errors and then a watchdog crash or memory corruption.

  Conditions: This symptom is observed when running many of the **show platform mpls handle** commands. The switch may crash.

```
SW#sh platform mpls handle 262836664 ?
  BD_HANDLE              bd/el3idc_vlan handle
  L2VPN_L2_HANDLE        l2 tunnel intf handle
  L2VPN_PW_BIND_DATA     pw bind data
  LFIB_TABLE             LFIB TABLE handle
  PORT_HANDLE            port/met handle
  RW_HANDLE              Rewrite handle
  SW_OBJ_ADJACENCY       oce type SW_OBJ_ADJACENCY
  SW_OBJ_ATOM_DISP       oce type SW_OBJ_ATOM_DISP
  SW_OBJ_ATOM_IMP        oce type SW_OBJ_ATOM_IMP
  SW_OBJ_DEAGGREGATE     oce type SW_OBJ_DEAGGREGATE
  SW_OBJ_EGRESS_LABEL    oce type SW_OBJ_LABEL
  SW_OBJ_EOS_CHOICE      oce type SW_OBJ_EOS_CHOICE
  SW_OBJ_FIB_ENTRY       oce type SW_OBJ_FIB_ENTRY
  SW_OBJ_FRR             oce type SW_OBJ_FRR
  SW_OBJ_GLOBAL_INFO     oce type SW_OBJ_GLOBAL_INFO
  SW_OBJ_ILLEGAL         oce type SW_OBJ_ILLEGAL
  SW_OBJ_IPV4_FIB_TABLE  oce type SW_OBJ_IPV4_FIB_TABLE
  SW_OBJ_IPV6_FIB_TABLE  oce type SW_OBJ_IPV6_FIB_TABLE
  SW_OBJ_LABEL_ENTRY     oce type SW_OBJ_LABEL_ENTRY
  SW_OBJ_LABEL_TABLE     oce type SW_OBJ_LABEL_TABLE
  SW_OBJ_LOADBALANCE     oce type SW_OBJ_LOADBALANCE
  SW_OBJ_RECEIVE         oce type SW_OBJ_RECEIVE
```

  Workaround: Do not run the commands as they are for development use.

- CSCtz16622

  Symptoms: A Cisco ME 3600X acts as a label disposition Edge-LSR when receiving MPLS packets with Checksum 0xFFFF that will continue to drop with Ipv4HeaderErr and Ipv4ChecksumError at nile.

  Conditions: This symptom is seen with label pop action at the Edge-LSR.

  Workaround: There is no workaround.

- CSCtz27782

  Symptoms: A crash is observed on defaulting service instance with OFM on EVC BD configured.

  Conditions: This symptom occurs when interface is in OAM RLB slave mode.

  Workaround: There is no workaround.

- CSCtz31888

  Symptoms: After state change of one of the L3 uplink interfaces, STP cost of BPDU PW increases from 200 to 2M, which can lead to blocking state in STP for this PW.

  Conditions: This symptom occurs with state change of one of the uplink L3 interfaces.

  Workaround: Increase the cost of access ring to more then 2M to avoid blocking of the BPDU PW.

- CSCtz32521

  Symptoms: In interop scenarios between Cisco CPT and Cisco ASR 9000 platforms, in order to support transport switchover requirement for 50 msec, it would require Cisco ASR 9000 or PI code to allow configuration or negotiation of minimal interval timer to 2.

  Conditions: This symptom occurs in interop scenarios between Cisco CPT and Cisco ASR 9000 platform. In order to support transport switchover requirement for 50 msec, it would require Cisco ASR 9000 or PI code to allow configuration or negotiation of minimal interval timer to 2.

  Workaround: There is no workaround.

- CSCtz35467

  Symptoms: QoS policy-map gets detached from interface on line protocol down-- >up transition happens on reload, admin **shut/no shut** and interface flap as well.

  Conditions: This symptom is observed when QoS policy-map is applied at interface and more than one child has “priority + police cir percent x” configured.

  Workaround: To be preventive use “police cir *absolute”* instead of “police cir percent x”. To be reactive use EEM applet/script.

  Further Problem Description: There is no error message in the syslog, only on console. It seems that line protocol UP can be used as the trigger action for EEM.

- CSCtz40435

  Symptoms: The L4 port-range security ACL does not work on EVC.

  Conditions: This symptom is seen when security ACL containing L4 port range operation that is applied on EVC. The behavior is not as expected. The same works on physical interface.

  Workaround: Add support for L4 port range operation similar to the case of applying it on physical interface.

  PSIRT Evaluation: The Cisco PSIRT has evaluated this issue and does not meet the criteria for PSIRT ownership or involvement. This issue will be addressed via normal resolution channels.

  If you believe that there is new information that would cause a change in the severity of this issue, please contact psirt@cisco.com for another evaluation.

  Additional information on Cisco’s security vulnerability policy can be found at the following URL:

  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtz45057

  Symptoms: High CPU is observed on the Cisco ME 3800X.

  Conditions: This symptom occurs with a loop of OTNIFMIB that causes CPU Hog and crash on Cisco ME 3800X during pulling from PPM

  Workaround: OTNIFMIB is not supported or required on Cisco ME 3800X and Cisco ME 3600X. Disable them while pulling from PPM.

- CSCtz46300

  Symptoms: Traffic is not classified under the QoS ACLs having port matching using range (inclusive range), lt (less than), and gt (greater than) operators.

  Conditions: This symptom is seen with IPv4 and IPv6 with L4 port ranger operations using range, lt, and gt, which do not work with QoS ACLs on Cisco ME 3600 and Cisco ME 3800 switches.

  Workaround: There is no workaround.

- CSCtz54823

  Symptoms: Configuration is getting locked on chopper SPA.

  Conditions: This symptom happens as follows:

  1. Shut down the controller of the SPA.
  2. Reload will bring the SPA in the locked state.

  Workaround: There is no workaround. Erase start up and reload the system to get back to configuration mode.

Open Caveats—Cisco IOS Release 15.2(2)S

This section describes possibly unexpected behavior by Cisco IOS Release 15.2(2)S. All the caveats listed in this section are open in Cisco IOS Release 15.2(2)S. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCts81627

  Symptoms: On Cisco IOS Release 15.1(2)EY1a, REP Flaps when BFD is configured on the same device. On Cisco IOS Release XE 3.6.0S, REP with fast hellos flaps when BFD is configured on the same device.

  Conditions: This symptom occurs when REP and BFD sessions with aggressive timers are configured on the same device. We could have REP flaps.

  Workaround: On Cisco IOS Release 15.1(2)EY1a, there is no workaround if both REP and BFD run on the same device. No flaps are seen after removing BFD.

  On Cisco IOS Release XE 3.6.0S, REP can run on the same device as BFD if configured with default timers. Flaps are seen only with fast-hellos on REP.

- CSCtw53121

  Symptoms: ES+ goes into major state occasionally on reload or SSO.

  Conditions: This issue is seen in the Cisco 7600 router with 40 gig ES+ line card that is running Cisco IOS Release 15.2(2)S.

  Workaround: There is no workaround.

- CSCtw70298

  Symptoms: Router crashes after the router bootup.

  Conditions: This symptom is seen with L2VPN xconnect.

  Workaround: There is no workaround.

- CSCty12641

  Symptoms: CFM ethernet ping fails with Cisco 7600 as the remote MEP end.

Conditions: This symptom is observed on a remote CFM over Xconnect MEPs with MEPs terminating on Cisco 7600 and having ESM20 line card.

Workaround: There is no workaround.

- CSCty16119

  Symptoms: MAC withdrawal does not happe.n

  Conditions: This symptom happens on shutting the VFI's VLAN on NPE. Failure of the spoke VC will work as expected.

  Workaround: Fail only the spoke VC without affecting the VFI and core VCs on NPE1.

- CSCty23747

  Symptoms: MAC Address withdrawal messages are not being sent.

  Conditions: This symptom is seen with flapping REP ports on UPE.

  Workaround: There is no workaround.

- CSCty26334

  Symptoms: The OSPFv3 neighborship between PE routers does not come up when sham-link is configured between the PE router. The problem is that VRF id of packet and VRF id of interface, on which packet is received (interface VRF1021) matches and therefore OSPF does not know it is sham-link packets and tries to associate it with process on this strange interface VRF1021. But there is no process on VRF1021.

  Conditions: This is observed only when trying to establish sham-link in SUP720.

  Workaround: There is no workaround

- CSCty28914

  Symptoms: CPU hog and CHUNKSIBLINGSEXCEED are observed followed by ES+ cash after performing line card OIR.

  Conditions: This symptom is observed after performing line card OIR of ES+ which is having scaled hardware offload BFD sessions.

  Workaround: There is no workaround.

- CSCty30952

  Symptoms: QoS policy-map gets rejected on shut/no shut of the interface or router reload.

  Conditions: This symptom occurs on router reload or shut/no shut of the interface.

  Workaround: Apply the policy-map back.

- CSCty45348

  Symptoms: DM in the port-shaper does not affect the police percent.

  Conditions: This symptom occurs when configuring a policy-map with shape in the egress direction. Do the DM and modify the rate. Policer changes do not work after the changes.

  Workaround: Have an absolute policer to ensure that we will not run into this problem. Dynamic modification of the policer might also fix the issue.

- CSCty46928

  Symptoms: The PIM SM mode is not supported for DATA-MDT groups.

  Conditions: This symptom is seen with PIM SM mode configuration for Data MDT groups and traffic stream with rate greater than mdt threshold to switch the traffic stream to Data MDT from default.

Workaround: There is no workaround.

- CSCty47231

  Symptoms: Traffic drops on removing the port-shaper.

  Conditions: Issue seen only when the policymap attach / detach is coupled with a link up/down, not seen on normal attach/detach. No issues with reload; policymap attached, and detached.

  Workaround: Default the egress interface and reconfigure. Traffic recovers.

- CSCty67401

  Symptoms: When traffic arriving on the ingress EVC BD interface is priority-tagged, the vlan id or priority value of traffic egressing out of EVC with double-encap or single-encap configuration respectively, gets incorrectly set to 0.

  Conditions: On a Cisco ME 3600X or ME 3800X that is running Cisco IOS Release 15.2(2)S, the CoS value of packet going out of EVC BD port with single-encap and vlan id of packet going out of EVC BD with double-encap are incorrectly set to 0.

  Workaround: There is no workaround.

- CSCty76106

  Symptoms: Crash after 2days of soak with traffic.

  Conditions: This symptom occurs with node acting as ConPE with multiple services like REP, MST, L3VPN, L2VPN, and constant frequent polling of SNMP, RCMD, full scale of routes and bidirectional traffic.

  Workaround: There is no workaround.

- CSCty77098

  Symptoms: Gig ports go DOWN.

  Conditions: This symptom occurs with different states during the EDVT testing.

  Workaround: There is no workaround.

- CSCty82786

  Symptoms: After removing and adding VLAN to the database, MAC Limit Shutdown does not work any more.

  Conditions: The issue is only seen after removing and adding VLAN to the database.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.2(2)S

All the caveats listed in this section are resolved in Cisco IOS Release 15.2(2)S. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCee38838

  Symptoms: A crashdump may occur during a two-call-per-second load test on a gateway, and the gateway may reload.

  Conditions: This symptom is observed on a Cisco 3745 that runs Cisco IOS Release 12.3(7)T and that functions as a gateway when you run a two-call-per-second load test that uses H.323, VXML, and HTTP. The crash occurs after approximately 200,000 calls.

  Workaround: There is no workaround.

- CSCsb53810

  Symptoms: A Cisco Catalyst 6500 series switch may not block traffic, which is supposed to be denied by an outbound ACL on a VLAN interface.

  Conditions: This issue is under investigation.

  Workaround: Reload the switch.

- CSCsg48725

  Symptoms: A TLB exception may occur on a Cisco platform that functions as a PE router in an MPLS environment, and the following error message may be generated:

  TLB (load or instruction fetch) exception, CPU signal 10 (BadVaddr : DEADBEF3)

  Conditions: This symptom is observed on a Cisco platform when TACACs accounting and authorization is enabled and when the TACACs server is reachable through the global routing table.

  Workaround: Disable AAA. If this not an option, there is no workaround.

- CSCsh39289

  Symptoms: A router may crash under a certain specific set of events.

  Conditions: The crash may happen under a combination of unlikely events when an IPv6 PIM neighbor that is an assert winner expires.

  Workaround: There is no obvious workaround, but the problem is unlikely to occur.

- CSCsj23805

  Symptoms: RP crashes when issuing the **show ip eigrp timer** command.

  Conditions: This symptom happens on DMVPN HUB with scaling of more than 2000 spokes.

  Workaround: There is no workaround.

- CSCta27224

  Symptoms: This is a sister defect to CSCta27210 to add CLI support for cell payload scrambling on SPA-1CHOC3-CE-ATM. Currently, cell payload scrambling is off by default for ATM DS1 interfaces on SPA-1CHOC3-CE-ATM and on for E1 interfaces. Cell payload scrambling is currently not configurable. This presents an issue when connecting to ATM copper T1 CPEs that require cell payload scrambling or when connecting to E1s devices that do not support cell payload scrambling. As such, this defect makes cell payload scrambling configurable (on or off) on the ATM CEOP family of SPAs for all media types including:

  - SPA-1CHOC3-CE-ATM (ATM DS1, ATM E1, ATM IMA DS1, ATM IMA E1)
  - SPA-2CHT3-CE-ATM (ATM DS3)
  - SPA-24CHT1-CE-ATM (ATM DS1, ATM E1, ATM IMA DS1, ATM IMA E1)

  Conditions: This symptom is observed when using ATM or IMA DS1 T1 or E1 on any of the following:

  - SPA-1CHOC3-CE-ATM (ATM DS1, ATM E1, ATM IMA DS1, ATM IMA E1)
  - SPA-2CHT3-CE-ATM (ATM DS3, ATM E3)
  - SPA-24CHT1-CE-ATM (ATM DS1, ATM E1, ATM IMA DS1, ATM IMA E1)

  Workaround: There is no workaround.

- CSCta27728

  Symptoms: A Cisco router may crash.

Conditions: This symptom is observed on a Cisco ASR1002 router running Cisco IOS Release 15.1(2)S1 with RSVP for MPLS TE tunnel signaling.

Workaround: There is no workaround.

- CSCtc96631

  Symptoms: Packet drops occur in downstream devices every 4ms burst from shaper.

  Conditions: The symptom is observed when shaping at high rates on very fast interface types with low memory buffer devices downstream.

  Workaround: Use Cisco ASRs instead of Cisco ISRs.

- CSCtd87072

  Symptoms: IOSD restart seen.

  Conditions: The symptom is observed when changing tunnel mode on scaled IPSec sessions.

  Workaround: There is no workaround.

- CSCte96453

  Symptoms: Switch intermittently crashes when configuring energywise features.

  Conditions: The symptom is observed when the port is configured with “energywise level 10” to bring up a previously down port.

  Workaround: There is no workaround.

- CSCtg57657

  Symptoms: A router is crashing at DHCP function.

  Conditions: This issue has been seen on a Cisco 7206VXR router that is running Cisco IOS Release 12.4(22)T3.

  Workaround: There is no workaround.

- CSCtg58029

  Symptoms: After switchover, aaa_acct_session_id iss not issued to new sessions.

  Conditions: This symptom occurs only after switchover.

  Workaround: There is no workaround.

- CSCth08962

  Symptoms: A single bit error in the SRAM of the ATM SPA will generate the following error message:

  EST5EDT,M3.2.0/: spa_atm_v2[241]: SPA ATM4/2 SAR: An error was reported by SAR firmware (unsolicited msg): Description: Single-bit SRAM ECC correctable error. [Error code 4]

  It does not cause an operation impact, but the error message will repeat every 6 seconds.

  Single bit correctable errors should be counted but not display an error message since the information is already corrected by parity. Also, the rate of these messages may increase during certain conditions, which may choke the queues on the platform.

  Conditions: This symptom occurs under normal operating conditions.

  Workaround: There is no workaround.

- CSCti00319

  Symptom 1: The warning message “Fatal error FIFO” occurs repeatedly upon PPPoEoA Session teardown.

Symptom 2: On the LC console, the message "Command Indication Q wrapped" keeps appearing.

Conditions: This symptom is observed on a Cisco ASR1001 router and kingpin router chassis under the following conditions:

1. High scale session counts.
2. Range configuration with more than 100 virtual channels (VC)
3. Back to back creation and deletion of multiple VCs with no time gap.

Workaround: There is no workaround.

- CSCti48483

  The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:

  NetMeeting Directory (Lightweight Directory Access Protocol, LDAP) Session Initiation Protocol (Multiple vulnerabilities) H.323 protocol

  All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-nat.shtml

- CSCti66155

  Symptoms: A Cisco IPSec router may unexpectedly reload due to bus error or software-forced crash because of memory corruption or STACKLOW error.

  Conditions: This is seen when the WAN link goes down and causes recursion between multiple tunnels using tunnel protection. (That is, there are tunnel 0 and tunnel 1. After the WAN link goes down, the routing table shows a link to the tunnel 0 destination through tunnel 1 and the tunnel 1 destination is through tunnel 0.)

  Workaround 1: Change the tunnel source to be the physical WAN interface so that when the WAN link does go down, the tunnels are brought down immediately.

  Workaround 2: Change the routing protocol so that the router in question does not have recursive routing when the link goes down.

  Workaround 3: If possible, create a floating null route for the tunnel destinations that is less preferred than the route normal route to the tunnel destination, but more preferred than the route that gets installed after the WAN link goes down.

- CSCti67832

  Symptoms: Cisco 3900e platform router reloads while try to enable GETVPN Group Member (GM) all-features debugs.

  Conditions: The symptom is observed on a Cisco 3900e router that is running Cisco IOS interim Release 15.1(2.7)T and while trying to enable the debug **debug crypto gdoi gm all-features**.

  Workaround: There is no workaround.

- CSCtj05903

  Symptoms: Some virtual access interfaces are not created for VT, on reload.

  Conditions: This symptom occurs on scaled sessions.

  Workaround: There is no workaround.

- CSCtj06390

  Symptom: Ping fails after configuring crypto.

Conditions: This symptom is observed on a Cisco router running Cisco IOS Release 15.1(2.18)T.

Workaround: There is no workaround.

- CSCtj10592

  Symptoms: DVTI GRE IPv4 mode fails to create virtual-access for IKEv2 connections.

  Conditions: The symptom is observed with a simple SVTI to DVTI connection.

  Workaround: There is no workaround.

- CSCtj14525

  Symptoms: Standby is not synced to active after attaching a new policy.

  Conditions: This symptom happens when dynamic policy is used such as RADIUS CoA.

  Workaround: There is no workaround.

- CSCtj30238

  Symptoms: WRED counters are wrongly updated. The default counter should be 0, but the counter is wrongly updated. All the WRED subclasses show the same count. Counters are shown for WRED subclasses for which there are no traffic matches in the class.

  Conditions: This issue is seen on the Cisco 7600 router with ES+ line card only. The Es+ line card does not support per WRED class based counters. There was a recent breakage due to the Transmit packets/bytes column that started showing up for the Es+ line card. This is wrong. As ES+ writes same value to WRED transmit count (not the per subclass base count, but total count), this value does not make sense.

  Workaround: Do not use WRED subclass Transmit packets/bytes counters for ES+ line card on the Cisco 7600 router.

- CSCtj38234

  Symptoms: IPSec IKEv2 does not respond to INVALID_SPI informational message. It should respond with another INFORMATIONAL IKE message.

  An INVALID_SPI may be sent in an IKE INFORMATIONAL exchange when a node receives an ESP or AH packet with an invalid SPI. The notification data contains the SPI of the invalid packet. The INVALID_SPI message is received within a valid IKE_SA context.

  Conditions: The symptom is observed when an IKEv2 peer sends an INFORMATIONAL IKE message notifying about an INVALID_SPI (IPSec).

  Workaround: There is no workaround.

- CSCtj64807

  Symptoms: Router crashes while issuing the **show vlans dot1q internal** command.

  Conditions: The symptom is observed with the following conditions:

  1. One QinQ subinterface configured with inner VLAN as “any”.
  2. More than 32 QinQ subinterfaces configured with same outer VLAN.
  3. All subinterfaces are removed except subinterface configured with “any” inner VLAN.

  Workaround 1: For any Cisco 10000 series router which has had its first crash - on any subinterface if the outer VLAN has second-dot1q VLAN as only “any”, immediately delete the subinterface and recreate it. Then add a dummy VLAN/sub-interface to this outer VLAN.

  Workaround 2: On any outer VLAN (in array state) if they have less than 5 inner VLANs, add a dummy VLAN/subinterface.

Workaround 3: For any Cisco 10000 series router which has not had a crash but has subinterface/outer VLAN with second-dot1q VLAN as only "any" and active sessions, add a dummy VLAN/sub-interface to this outer (tree state) VLAN.

- CSCtj76297

  Symptoms: Router hangs with interoperability of VM and crypto configurations.

  Conditions: The symptoms are seen only during interoperability between video-monitoring and crypto (IPSec VPN) with an AIM-VPN/SSL-3 card.

  Workaround: Disable AIM and use onboard CE.

- CSCtj78966

  Symptoms: A Cisco ASR 1000 router crashes with thousands of IKEv2 sessions, after many operations on IKEv2 session.

  Conditions: This symptom is seen when IKEv2 SA DB WAVL tree is getting corrupted if we fail to insert the SA due to some error, for example, PSH duplication.

  Workaround: There is no workaround.

- CSCtj79368

  Symptoms: All keyservers crash after removing RSA keys before changing to new ones based on security concerns.

  Conditions: The symptom is observed when removing RSA keys.

  Workaround: Stay on the same RSA keys.

- CSCtk03371

  Symptoms: SVI-based EoMPLS/VPLS VC fails to forward traffic even when VC is up.

  Conditions: This happens when the **ip cef accounting non-recursive** command is configured on the router. This command is documented as an unsupported command on the Cisco 7600 platform, but it should also generate an error message when configured on the Cisco 7600. Preferably it should not take any action, for example, it should not affect any other working features.

  Workaround: Unconfigure the command by typing "no ip cef accounting non- recursive".

- CSCtk15360

  Symptoms: xauth userid mode http-intercept does not prompt for a password and the Ezvpn session does not come up.

  Conditions: This symptom occurs when the EzVPN client, x-auth is configured as http-intercept.

  Workaround: There is no workaround.

- CSCtk62763

  Symptoms: A Cisco 7600 router equipped with multiple DFC line cards may experience an unexpected reload because of increased IGMP activity.

  Conditions: This symptom is observed when IGMP joins and leaves (OIF churn) at approximately 160pps or more on DFCs with around 600 mroutes that have SVIs as OIFs.

  Workaround: There is no workaround.

- CSCtk69114

  Symptoms: RP resets while doing ESP reload with crypto configuration.

  Conditions: This symptom is observed by unconfiguring and configuring interface configuration and reloading both ESPs. The RP crashes on the server.

Workaround: There is no workaround.

- CSCtl20993

  Symptoms: Router crashes during IPsec rekey.

  Conditions: The conditions for this crash are currently unknown.

  Workaround: There is no workaround.

- CSCtl23748

  Symptoms: EoMPLS over GRE (DMVPN) with IPSec protection is not working after a reboot.

  Conditions: The symptom is observed when there is a tunnel (Ethernet over MPLS over GRE over IPSec) between PE1 and PE2 and following a reload and when tunnel protection is configured.

  Workaround: There is no workaround.

- CSCtl77241

  Symptoms: The switch crashes following webauth, as AAA accounting begins.

  Conditions: This symptom occurs under the following conditions:

  - Webauth is used.
  - AAA accounting is enabled for proxy-auth.

  Workaround: Disable AAA accounting.

- CSCtn02208

  Symptoms: Old PerUser ACL is not removed on applying new ACL.

  Conditions: This symptom occurs when applying a new PerUser ACL to an existing session. The old PerUser ACL that exists on the session is not removed.

  Workaround: There is no workaround.

- CSCtn02372

  Symptoms: QoS installation fails on the CEoP SPA or traffic is not forwarded correctly after a lot of dynamic changes that continuously remove and add VCs, as on CEoP SPA, IfIDs are not freed upon deleting the PVC.

  Conditions: This symptom occurs when continuous bring-up and tear down of VCs causes the SPA to run out of IfIDs.

  Workaround: Reload the Cisco SIP-400 line card.

- CSCtn07696

  Symptoms: The Cisco 6506-E/SUP720 may crash while redirecting the **show tech-support** command output using the **ftp** command due to TCP-2-INVALIDTCB.

  Conditions: This symptom is observed with the following CLI:

  ```
  show tech-support | redirect
  ftp://cisco:cisco@10.0.255.14/Cisco/tech-support_swan21.pl.txt
  ```

  During the FTP operation, if the interface fails or shuts down, it could trigger this crash.

  Workaround: This is an FTP-specific issue. Redirect the output by TFTP or other protocols.

- CSCtn12119

  Symptoms: There is no change in functionality or behavior from a user perspective. This DDTS brings in changes to padding used during signing/verification from PKCS#1 v1.0 to PKCS #1v1.5.

Conditions: This symptom is observed during signing/verification for releases prior to Cisco IOS Release 15.1(2)T4.

Workaround: The Rommon is capable of verifying images signed using both v1.0 and v1.5. As such no workaround is necessary from a usability perspective, the image boots and runs as expected. However, it will not be in compliance with FIPS 140-3 requirements.

- CSCtn16855

  Symptoms: The Cisco 7200 PA-A3 cannot ping across ATM PVC.

  Conditions: This symptom occurs due to a high traffic rate, and the output policy applied under PVC.

  Workaround: There is no workaround. Removing the policy will resolve this issue, but the QoS functionality will not be present in this case.

- CSCtn18229

  Symptoms: A policy does not get suspended.

  Conditions: This symptom is observed if a policy is applied to fr-pvc, then the member link is flapped from the peer for mfr subint.

  Workaround: There is no workaround.

- CSCtn22728

  Symptoms: See the following:

```
Router(config)#monitor session 1 type erspan-source
Router(config-mon-erspan-src)#destination ?
  <cr>

Router(config-mon-erspan-src)#destination int g11/48
Router(config-if)#
Config Sync: Line-by-Line sync verifying failure on
command:
  destination int g11/48
due to parser return error
```

  Conditions: This symptom is seen when using unsupported interface CLI option with destination keyword in ERSPAN source session configuration, which may result in Config-Sync failure between Active and Standby-RP, therefore reloading Standby-RP.

  Workaround: Do not issue not applicable commands.

- CSCtn26750

  Symptoms: The standby RP reloads due to a config-sync error.

  Conditions: The symptom is observed when “authentication” or “encryption” is configured for an OSPFv3 virtual link. Then it is changed to use a different SPI, but IPSec fails to remove the policy for the old SPI. When it is changed back to the old SPI, the command fails with the error:

```
%OSPFv3-3-IPSEC_POLICY_ALREADY_EXIST: SPI is already in use with ospf process
```

  On the active RP the “virtual-link ipsec” configuration is removed, but on the standby RP it remains. Reconfigure “virtual-link ipsec” using the second SPI. This command succeeds on the active RP so it is synched to the standby, however the command already exists on the standby so it generates the config- sync error and reloads.

  Workaround: Instead of simply changing the SPI from X to Y, remove X using a **no** command and then configure Y.

- CSCtn39632

  Symptoms: RSA key cannot be configured under a keyring any more. The RSA key will be configured in global configuration.

  Conditions: This occurs on a Cisco ASR 1000 series router configured for RSA key encryption with a keyring name having more than 8 characters.

  Workaround: Modify the keyring name to be less than 8 characters.

- CSCtn39950

  Symptoms: An IPsec session will not come up.

  Conditions: This symptom occurs if a Cisco ISR G2 has an ISM VPN accelerator and slow interfaces such as BRI-PRI. Crypto plus ISM VPN module plus slow interfaces will not work.

  Workaround: Disable the ISM VPN module and switch to the onboard crypto engine.

- CSCtn40771

  Symptoms: The process ACL Header in the **show memory allocating- process totals** command output leaks memory with per-user ACLs and PPP session churn. This will also cause the SSS feature manager process in the **show process memory** command output to appear to have a leak.

  Conditions: This symptom occurs with IPv6 per-user ACLs and session churn.

  Workaround: There is no workaround.

- CSCtn59075

  Symptoms: A router may crash.

  Conditions: This has been experienced on a Cisco router that is running Cisco IOS Release 15.1(3)T, 15.1(3)T1, and 15.1(4)M. Flexible NetFlow needs to be running.

  Workaround: Disable Flexible NetFlow on all interfaces.

- CSCtn70367

  Symptoms: IPSEC key engine crashes at sessions setup.

  Conditions: This symptom is seen when setting up sessions with the configuration of 1000 VRFs, one IKE session per VRF, and four IPSec SA dual per session. The crash happens on IPSEC key engine. The crash occurs while UUT is establishing SAs that are requested. This issue is reproduced by clear crypto session on CES after all SAs are established.

  Workaround: There is no workaround.

- CSCtn79475

  Symptoms: A Cisco router reloads often due to stack overflow under some traffic conditions.

  Conditions: This symptom is observed when calls resulting in VOIPRTP media loop are seen.

  Workaround: There is no workaround.

- CSCtn83520

  Symptoms: VOIP_RTCP related traceback is seen.

  Conditions: This symptom is observed when IPIP gateways are involved.

  Workaround: There is no workaround.

- CSCtn95395

  Symptoms: VTEMPLATE Background Mgr crashes on DVTI server after using the **clear crypto session** command on DVTI client.

Conditions: This symptom is seen on DVTI server when sessions are setting up with the IPSec DVTI configuration of 1000 VRFs, one IKE session per VRF, and four IPSec SA dual per session. We might run into VTEMPLATE Background Mgr process crashing after executing the **clear crypto session** command a couple of times on DVTI client.

Workaround: There is no workaround.

- CSCto10336

  Symptoms: The LNS router hangs up at the interrupt level and goes into an infinite loop.

  Conditions: This symptom occurs during control channel cleanup.

  Workaround: There is no workaround. This symptom can be only removed through power cycle.

- CSCto10485

  Symptoms: With a GRE over IPSec configuration using tunnel protection, traffic originated from the router may be dropped on the receiving router due to replay check failures. This is evident by the %CRYPUO-4-PKT-REPLAY drops as shown in the syslog.

  Conditions: This issue typically occurs during high traffic load conditions.

  Workaround: There is no workaround.

- CSCto12825

  Symptoms: The multilink policy cannot be removed.

  Conditions: This symptom is observed with MPOL configured; when multilink goes to suspension, the policy cannot be removed.

  Workaround: There is no workaround.

- CSCto31255

  Symptoms: Router crashes at fair-enqueue.

  Conditions: The symptom may be seen on Cisco 5400 and 7200 platforms.

  Workaround: There is no workaround.

- CSCto60216

  Symptoms: Cisco IOS crashes in ospfv3_write.

  Conditions: This symptom occurs when the **issu runversion** command is entered multiple times within a short period of time.

  Workaround: Wait for the newly active router processor to completely initialize.

- CSCto61736

  Symptoms:

  1. NBAR remains enabled in CEF path.
  2. Packet counters not incrementing in “show adjacency lisp0 detail”.
  3. ADQ/PD not working on ATM-subinterface and frame-relay subinterfaces.
  4. **ip nbar port-map** CLI is broken.

  Conditions:

  1. The symptoms 1 and 2 are observed when NBAR is enabled and disabled on the interface.
  2. Symptoms 3 and 4 are seen when the configuration/show CLIs are executed.

  Workaround: There is no workaround.

- CSCto70125

  Symptoms: IP SLA TCP connect probe is configured via SNMP, then IP SLA Event Processor process goes to 100% CPU.

  Conditions: This issue is seen for TCP connect probes. The issue may affect multiple Cisco IOS releases but has been observed on Cisco IOS Releases 12.2 (33)SXH and 12.2(33)SXI based releases.

  Workaround: Set up probe via CLI.

- CSCto71671

  Symptoms: Using the **radius-server source-ports extended** command does not increase AAA requests source UDP ports as expected when Radius.ID has wrapped over, causing duplicate (dropped) requests on Radius, and forcing the Cisco ASR 1000 router to time out and retransmit.

  Conditions: This symptom is observed with a high AAA requests rate, and/or slow Radius response time, leading to a number of outstanding requests greater than 255.

  Workaround: There is no workaround.

- CSCto72350

  Symptoms: A stale suspended service-policy remains.

  Conditions: This symptom is observed when the policy CLI is removed when policy is suspended.

  Workaround: There is no workaround.

- CSCto72629

  Symptoms: A MAXAGE LSA is repeatedly retransmitted bringing down the OSPFv3 adjacency.

  Conditions: This symptom occurs when the unadjusted age of the LSA in the OSPFv3 database (as opposed to the advertised age, which includes time spent in the database) is less than MAXAGE. Note that the age of the LSA in the database is not updated once it is installed unless maxaging is initiated by OSPFv3 process.

  Workaround: Use the **clear ipv6 ospf process** command to clear the OSPF state based on the OSPF routing process ID.

- CSCto72927

  Symptoms: Configuring an event manager policy may cause a cisco router to stop responding.

  Conditions: This issue is seen when a TCL policy is configured and copied to the device.

  Workaround: There is no workaround.

- CSCto73151

  Symptoms: The RP resets.

  Conditions: This symptom occurs when the **show ip nhrp** command is issued to check mixed DMVPN and SVTI.

  Workaround: There is no workaround.

- CSCto73345

  Symptoms: A router crashes while reloading after configuring a crypto IPsec manual keying policy.

  Conditions: This issue is seen when a router that is configured with a crypto IPsec manual keying policy is reloaded.

  Workaround: There is no workaround.

- CSCto85731

  Symptoms: Crash seen at the nhrp_cache_info_disseminate_internal function while verifying the traffic through FlexVPN spoke-to-spoke channel.

  Conditions: The symptom is observed under the following conditions:

  1. Configure hub and spokes (flexvpn-nhrp-auto connect) as given in the enclosure.
  2. Initiate the ICMP traffic through spoke-to-spoke channel between spoke devices.
  3. Do a **clear crypto session** at Spoke1.
  4. Repeat steps 2 and 3 a couple of times.

  Workaround: There is no workaround.

  Further Problem Description: In the given conditions, one of the spoke device crashed while sending ICMP traffic (10 packets) through FlexVPN spoke-to- spoke channel. The crash decode points to “nhrp_cache_info_disseminate_internal” function

- CSCto90252

  Symptoms: A standby route processor (RP) is stuck to “init, standby” for about 10 hours.

  Conditions: This symptom occurs after reloading five or six times on a Cisco ASR 1000 series router.

  Workaround: Disable NSR.

- CSCto92529

  Symptoms: Unable to configure “ipv6 ospf authentication ipsec spi 7000 md5 <>”.

  Conditions: The symptom is seen on Cisco routers loaded with Cisco IOS interim Release 15.2(2.11)T.

  Workaround: There is no workaround.

- CSCtq10684

  Symptoms: The Cisco 2800 crashes due to a bus error and the crash points to access to free internal structures in ipsec.

  Conditions: This symptom occurs when tunnel flap is observed before the crash.

  Workaround: A possible workaround is to reload the box.

- CSCtq23793

  Symptoms: After reloading PE router in mVPN network, multicast traffic stops on one of the VRFs randomly.

  Condition: This symptom occurs under the following conditions:

  -When reloading a PE in mVPN network. -When PE has many VRFs and scaled mVPN configuration.

  Workaround: Remove and add MDT configuration.

- CSCtq24006

  Symptoms: DMVPN tunnels will not come up with an IPv6 address.

  Conditions: This symptom is observed if more than one tunnel is present on the spoke.

  Workaround: There is no workaround.

- CSCtq24557

  Symptoms: Router crash after deleting multiple VRFs. This happens very rarely.

Conditions: The symptom is observed in a large scale scenario.

Workaround: There is no workaround.

- CSCtq32282

  Symptoms: Chunk leaks observed on various platforms.

  Conditions: The issue seen while testing the ipsec_unity_solaris functionality.

  Workaround: There is no workaround.

- CSCtq37579

  Symptoms: Enabling and disabling "snmp-server traps" crash the UUT.

  Conditions: The symptom is observed when you disable the snmp-server and do a **write memory**.

  Workaround: There is no workaround.

- CSCtq39602

  Symptoms: DMVPN tunnel is down with IPSec configured. The **show dmvpn** command from the spoke shows the state is IKE.

  Conditions: After heavy traffic was pumping from DMVPN hub to spoke for some time: from a few minutes to a couple of hours.

  Workaround: Configuring "crypto ipsec security-association lifetime kilobytes disable" to disable volume-based rekeying will reduce the problem.

- CSCtq47856

  Symptoms: The following issues are observed:

  1. Crypto map is configured with a local ACL at registration time.
  2. Local ACL is removed from global configuration (without removing it from the crypto map configuration).
  3. Remove crypto map from the interface.

     Issue 1: At this point **show crypto gdoi** continues to display the TEK SA, even though the GM has no interfaces configured with a crypto map.
  4. Reapply the crypto map to the interface and let registration complete.

     Issue 2: If **crypto gdoi ks rekey** is issued on the keyserver, then **show crypto gdo** continues to display only the old TEK. New TEKs installed by subsequent rekeys are not displayed.
  5. On the keyserver, issue **crypto gdoi ks rekey replace**.

     Issue 3: GM crashes in the IPSec code while processing the new SAs and shortening the old ones.

  Conditions: The symptom is observed on a router that is running GET VPN.

  Workaround: Remove the ACL from the crypto map configuration before removing it from the global configuration.

- CSCtq59923

  Symptoms: OSPF routes in RIB point to an interface that is down/down.

  Conditions: This symptom occurs when running multiple OSPF processes with filtered mutual redistribution between the processes. Pulling the cable on one OSPF process clears the OSPF database, but the OSPF routes associated with the OSPF process from that interface still point to the down/down interface.

  Workaround: Configure "ip routing protocol purge interface".

- CSCtq61128

  Symptoms: Router is crashing with segmentation fault (11).

  Conditions: This symptom is observed on routers acting as IPSEC hub using certificates.

  Workaround: There is no workaround.

- CSCtq63225

  Symptoms: Packet drop seen when running traffic.

  Conditions: The symptom is observed when IPSec along with QoS is configured.

  Workaround: There is no workaround.

- CSCtq63487

  Symptoms: The next set action is not executed with multi-action policy Routemap when set VRF fails.

  Conditions: This symptom occurs when deleting VRF, which causes a problem when other set clause is configured with set VRF.

  Workaround: There is no workaround.

- CSCtq69083

  Symptoms: Nested IPSec tunnel with outer tunnel GRE and inner tunnel VTI/GRE is not working.

  Conditions: The symptom is observed with the v150-1.M4.6 image.

  Workaround: There is no workaround.

- CSCtq75008

  Symptoms: A Cisco 7206 VXR crashes due to memory corruption.

  Conditions:

  - The Cisco 7206 VXR works as a server for L2TP over IPsec.
  - Encryption is done using C7200-VSA.
  - More than two clients are connected.

  If client sessions are kept up for about a day, the router crashes.

  Workaround: There is no workaround.

- CSCtq75045

  Symptoms: When a router is running FlexVPN-IKEv2 in auto-reconnect mode, IPSec SAs are not renegotiated properly after a **clear crypto session** command is entered. Entering the **show crypto ikev2 client flexvpn** command will indicate that the router is in a NEGOTIATING state.

  Conditions: This symptom is observed on a router running FlexVPN on IKEv2 in auto-reconnect mode.

  Workaround: Enter the **clear crypto ikev2 client flexvpn** command to clear the FlexVPN state and renegotiate the SAs successfully.

- CSCtq79382

  Symptoms: In the HA setup and on the Active, if you have a probe configured with VRF and you remove the VRF with **no ip vrf** *vrfname* and reboot, it keeps rebooting again and again (crashes).

  Conditions: The symptom is observed when removing the VRF and rebooting the Active terminal.

  Workaround: Check that the system is in standby and that there is no VRF configured. Even though there is a probe configured with VRF, you can proceed without crashing the Active after a reboot.

- CSCtq79767

  Symptoms: IPSEC key engine crashes after using the **clear crypto session** command on CES.

  Conditions: This symptom occurs under the following conditions:

  1. Topology:

     IXIA --> CES (DVTI Client) --> UUT (DVTI Server)-->

  2. Configuration:

     1000 vrf x 1 IKE session x 4 IPsec SA dual

  3. The crash on UUT is seen after using the **clear crypto session** command on CES after all SAs have been established.

  Workaround: There is no workaround.

- CSCtq83601

  Symptoms: EoMPLS traffic does not flow after MPLS TE tunnel path change after FRR.

  Conditions: This symptom occurs under the following conditions:

  - The TE tunnel is used as PW.
  - The VC does not flap and label stack looks fine.

  This issue is seen only with port-based xconnect.

  Workaround: Shut/no shut the AC interface to try and resolve the problem.

- CSCtq84313

  Symptoms: Router hangs and then crashes due to watchdog timer expiry.

  Conditions: This symptom is observed when IP SLA probes are configured, and then the configuration is replaced with one that has no IP SLA probes.

  Workaround: Reset the ip sla.

- CSCtq88777

  Symptoms: VDSL controller and ATM interface remains up, however ATM PVC becomes inactive and virtual interface goes down.

  Conditions: The symptom is observed when the ATM PVC becomes inactive causing the virtual interface to go down.

  Workaround: Use a VBR-NRT value that is lower than trained upstream speed.

- CSCtq92940

  Symptoms: An active FTP transfer that is initiated from a Cisco IOS device as a client may hang.

  Conditions: This symptom may be seen when an active FTP connection is used (that is, the **no ip ftp passive** command is present in the configuration) and there is a device configuration or communication issues between the Cisco IOS device and the FTP server, which allow control connections to work as expected, but stopping the data connection from reaching the client.

  Workaround: Use passive FTP (default) by configuring the **ip ftp passive** command.

  Further Problem Description: Please see the original bug (CSCtl19967) for more information.

- CSCtq95384

  Symptoms: Even after the removal of NSR configurations, BGP still holds memory.

  Conditions: The symptom is observed after the removal of NSR configurations.

  Workaround: There is no workaround.

- CSCtr01431

  Symptoms: An error is encountered during configuration synchronization.

  Conditions: This issue is observed when the following sequence of steps is performed:

  1. A loopback interface is created
  2. The macro interface range is configured for the loopback interface.
  3. The loopback interface is deleted.
  4. SSO is performed.

  Workaround: There is no workaround.

- CSCtr07142

  Symptoms: A memory leak is seen at crypto_ss_open.

  Conditions: No special configuration is needed.

  Workaround: There is no workaround.

  Further Problem Description: At bootup, when the **show memory debug leaks** command is run, memory leak entries are seen for the crypto_ss_open process.

- CSCtr08680

  Symptoms: The following error messages are displayed on active and standby respectively:

  ```
  %ERROR: Standby doesn't support this command
  BERT is running on this channel group, please abort bert first.
  ```

  Conditions: This symptom is observed when trying to create a channel after BERT has been started irrespective of whether BERT is running or completed.

  Workaround: There is no workaround.

- CSCtr14675

  Symptoms: The line card crashes after removing the child policy in traffic.

  Conditions: This symptom occurs after the child policy is removed in traffic.

  Workaround: There is no workaround.

- CSCtr16857

  Symptoms: Windowing in IKEv2 is broken.

  Conditions: This symptom occurs when an error condition in AUTH exchange causes the delete message to not be sent because of incorrect windowing. The following error is seen:

  ```
  "No room in peer window request is throttled: Current Req = 2 Next Req = 1"
  ```

  Workaround: There is no workaround.

- CSCtr20300

  Symptoms: SA negotiation test is failing for ipsec_core script.

  Conditions: The symptom is observed when the SA should come into idle state after using "show crypto isakmp sa".

  Workaround: There is no workaround.

- CSCtr21296

  Symptoms: The following messages are seen continuously on the router console:

  ```
  [ipsec_dp_expand_sa]Invalid data cipher info
  [ipsec_dp_expand_action]No memory to allocate SA for decrypt action
  ```

Conditions: The issue is seen after disabling the hardware crypto engine.

Workaround: There is no workaround.

- CSCtr23134

  Symptoms: Crash seen when IKEv2 debugs are enabled.

  Conditions: The symptom is observed when using the debug “debug crypto ikev2 internal.”

  Workaround: There is no workaround.

- CSCtr24751

  Symptoms: Cisco ME 3600X BGP is flapping every 55 hours and 58 minutes on GE interface.

  Conditions: This symptom is seen with peer BGP neighbor and ingress numbers of BGP route from TenGE.

  Workaround: There is no workaround.

- CSCtr24889

  Symptoms: Adding a second static route in a VRF and then removing it causes a traceback.

```
%MPLS_IPRM-3-INTERNAL: x.x.x.x/32 (vrfname(86)); prefix path set from outinfo,
illegal outinfo type: 4
-Traceback= 62A306AC 62A30908 62A30E08 62A33D20 62A33F98 60470B78 60476644 604B8440
604B8690 604BCE00 604BCF68 6056B5F0 6056B744 610E9EA8 610DDC68 610E009C
```

  Conditions: This symptom occurs when adding a second static route in a VRF and then removing it.

  Workaround: There is no workaround.

- CSCtr25127

  Symptoms: When switching between ATM and 3G interfaces, the following traceback is observed.

```
%ALIGN-3-CORRECT: Alignment correction made at 0x23D242DCz reading 0xE85C77B

%ALIGN-3-TRACE: -Traceback= 0x23D242DCz 0x23CDE700z 0x23CFDF50z 0x225C0594z
0x225C1368z 0x22DD4564z 0x21F88D28z 0x2173449Cz

%ALIGN-3-CORRECT: Alignment correction made at 0x23D2430Cz writing 0xE85C77B

%ALIGN-3-TRACE: -Traceback= 0x23D2430Cz 0x23CDE700z 0x23CFDF50z 0x225C0594z
0x225C1368z 0x22DD4564z 0x21F88D28z 0x2173449Cz
```

  Conditions: This symptom is observed when switching between ATM and 3g interfaces.

  Workaround: There is no workaround.

- CSCtr25386

  Symptoms: BFDv6 static route association fails after reenabling interfaces.

  Conditions: This symptom is observed after interfaces are reenabled.

  Workaround: There is no workaround.

- CSCtr30121

  Symptoms: Delayed Offer to Early Offer calls that go through CUBE may not be communicated properly between CUBEs in an HA environment. The result could be no audio on failover.

  Conditions: This symptom is seen when using CUBE HA.

  Workaround: There is no workaround.

- CSCtr31153

  Symptoms: Packet decryption seems to fail with manual crypto maps configured on interface.

Conditions: The symptom is observed on a Cisco 7200 series router loaded with Cisco IOS interim Release 15.2(0.19)T0.1.

Workaround: There is no workaround.

- CSCtr31496

  Symptoms: The line card crashes after switchover with the multilink configurations.

  Conditions: This symptom occurs after switchover with the multilink configurations.

  Workaround: There is no workaround.

- CSCtr34960

  Symptoms: A router that is running Cisco IOS may run out of IO memory.

  The **show buffers** command shows that the count reaches 0 in free list.

```
Router#sh buffers
...
Interface buffer pools:
....
Medium buffers, 256 bytes (total 89647, permanent 3000, peak 89647 @
00:01:17):
     273 in free list (64 min, 3000 max allowed)

EOBC0/0 buffers, 1524 bytes (total 2400, permanent 2400):
     0 in free list (0 min, 2400 max allowed)
     2400 hits, 161836 fallbacks
     1200 max cache size, 129 in cache
....
```

  Conditions: This issue is seen post bootup. The Cisco 7600 in HA is required to hit the issue. The **show buffers old** command shows some buffers hanging on EOBC buffers list for a long time, weeks or more. The issue is a corner case, and buffer leak rate is slow.

  This DDTS fixes leaks for the **mls cef maximum-routes** and **mls cef adjacency-mcast** commands.

  See the output from the **show buffers old pack**:

```
F340.08.04-6500-2-dfc1#show buf old packet

Buffer information for EOBC0/0 buffer at 0x275A0B00
  data_area 0x275A0FB8, refcount 1, next 0x0, flags 0x0
  linktype 69 (IPC), enctype 1 (ARPA), encsize 14, rxtype 0
  if_input 0x273AF610 (EOBC0/0), if_output 0x0 (None)
  inputtime 00:00:02.764 (elapsed 00:16:36.380)
  outputtime 00:00:00.000 (elapsed never), oqnumber 65535
  datagramstart 0x275A100C, datagramsize 50, maximum size 1680
  mac_start 0x275A0FFE, addr_start 0x275A0FFE, info_start 0x0
  network_start 0x275A100C, transport_start 0x0, caller_pc 0x205DF718

275A100C: 00200000 02010000 00010006 01000000  . .............
275A101C: 00350001 00101608 00000053 000000A6  .5.........S...&
275A102C: 000603E7 01170000 00000000 00000000  ...g...........
```

```
          --------
275A103C: 000000                               ...

Buffer information for EOBC0/0 buffer at 0x275A5B48
  data_area 0x275A6000, refcount 1, next 0x0, flags 0x0
  linktype 69 (IPC), enctype 1 (ARPA), encsize 14, rxtype 0
  if_input 0x273AF610 (EOBC0/0), if_output 0x0 (None)
  inputtime 00:00:02.764 (elapsed 00:16:41.380)
  outputtime 00:00:00.000 (elapsed never), oqnumber 65535
  datagramstart 0x275A6054, datagramsize 80, maximum size 1680
  mac_start 0x275A6046, addr_start 0x275A6046, info_start 0x0
  network_start 0x275A6054, transport_start 0x0, caller_pc 0x205DF718


275A6054:          00200000 02010000 02150007      . ..........
275A6060: 01000000 000A0001 00301608 00000052  .........0.....R
275A6070: 000000A4 00480002 01047FFF 00000001  ...$.H..........
                   --------
275A6080: 00000000 00000000 00000000 00000000  ................
275A6090: 00000001 00000000 00000000 00000000  ................
275A60A0: 00000000 00

F340.08.04-6500-2-dfc1#
```

The **show buffers old packet** command output will be either 000603E7 OR 00480002.

Workaround: Reload the supervisor to clear the leaked buffers.

- CSCtr35740

  Symptoms: QoS queuing hierarchy not moved to current active link when the previously active link goes down.

  Conditions: The symptom is observed when the DMVPN tunnel active link goes down.

  Workaround: There is no workaround.

- CSCtr42341

  Symptoms: Crash at task_execute_prep.

  Conditions: The symptom is observed with a Cisco 800 series router that is configured with BFD.

  Workaround: There is no workaround.

- CSCtr42913

  Symptoms: Stale crypto maps seen even after unconfiguring tunnel protection.

  Conditions: The symptom is observed when removing the tunnel source configuration.

  Workaround: Unconfigure and configure again or unconfigure tunnel protection first.

- CSCtr46854

  Symptoms: The PPP multilink between the Cisco ISR G2 router and the Cisco ASR 1000 router crashes the Cisco ISR router.

  Conditions: This symptom is observed with the Cisco ISR G2 router.

Workaround: Remove authentication on the Serial interface on the Cisco ASR router.

- CSCtr47642

  Symptoms: On Cisco IOS Release 15.2(3)T that is running BGP configured as RR with multiple eGBP and iBGP non-clients and iBGP RR clients and enabling the BGP best-external feature using the **bgp additional-paths select best- external** command, a specific prefix may not have bestpath calculated for a long time.

  Conditions: The problem occurs on a certain condition of configuration of the below commands, and a few prefixes are withdrawn during the configuration time:

  1. Configure: **bgp additional-paths install** under vpnv4 AF
  2. Configure: **bgp additional-paths select best-external**

  Immediately disable backup path calculation/installation using the **no bgp additional-paths install** command.

  The problem does not appear if both of the above commands are configured with more than a 10-second delay as the commands will be executed independently in two bestpath runs instead of one.

  Workaround: Configure the **bgp additional-paths install** command and the **bgp additional-paths select best-external** command with a delay of 10 seconds.

- CSCtr48525

  Symptoms: When “medium p2p” is configured under a physical interface, followed by configuration of the “mpls tp link” with a unicast entry for tx-mac (in that order) and then by “no medium p2p”, the “mpls tp link” entry is removed from the interface configuration without notification. Removal of the “mpls tp link” entries based on changes in the interface P2P status via the “medium p2p” configuration is inconsistent.

  Conditions: This symptom is observed in an IPLess configuration. First, “medium p2p” is added under a physical interface, followed by configuration of the “mpls tp link” with a unicast entry for tx-mac. Then, “medium p2p” is removed from under that physical interface. It is seen that the configuration for “mpls tp link” with a unicast entry for tx-mac is also removed from under the physical interface without notification to the user.

  Workaround: There is no workaround.

- CSCtr51926

  Symptoms: IPv6 packets are not classified properly in a subinterface when a service-policy is applied on the main interface.

  Conditions: The symptom is observed when a service-policy is applied on the main interface.

  Workaround 1: Enable IPv6 explicitly on the main interface:

```
interface x/y
  ipv6 enable
```

  Workaround 2: Reconfigure the IPv6 address on the subinterface:

```
interface x/y.z
  no ipv6 address
  ipv6 address ...
```

- CSCtr52740

  Symptoms: Query on an SLA SNMP MIB object using an invalid index can cause the device to crash.

Conditions: The symptom is observed when querying history information from rttMonHistoryCollectionCompletionTime object using invalid indices.

Workaround: Instead of using "get", use "getnext" to list valid indices for the MIB OID.

- CSCtr53056

  Symptoms: The Cisco ME 3600 crashes due to watchdog timeout.

  Conditions: This symptom occurs when switchport is configured on an interface that has PIM enabled. This is a timing issue and may not be seen every time.

  Workaround: There is no workaround.

- CSCtr53739

  Symptoms: The tunnel-encap entry is wrongly programmed. The following **show** command is used:

  show platform software multicast ip cmfib vrf *vrf- name* **tunnel-encap verbose**

  Conditions: This symptom occurs during deletion and readdition of the VRF with the multicast MDT configured and P2P tunnels as the access-facing interface, along with Gigabit subinterfaces.

  This issue is seen under the following conditions:

  1. Configure the mcast VRF with P2P tunnels as access-facing, along with Gigabit subinterfaces. Use a sip400 line card as the access-facing line card.
  2. Delete the VRF, P2P tunnel, and Gigabit subinterface.
  3. Add the same VRF again after a 60-second interval.
  4. Observe the tunnel-encap entry wrong programmed on the SP, with corrupt values.

  Workaround: There is no workaround.

- CSCtr56174

  Symptoms: The MPLS-TE link count reaches a large value (4 billion+) on the Cisco ASR 1000 series router and negative value on the Cisco 7600 series router. This issue is seen in the **show mpls tr link sum** and **show mpls tr link int** command output.

  Conditions: This symptom occurs if MPLS-TE tunnels are deleted using the **no int tunX** command and if the number of TE tunnels deleted are more than the TE links on the box. Even if they are not, with every TE tunnel deleted, the link count is affected and gets reduced.

  Workaround: Do not delete MPLS-TE tunnels using the **no int tuX** command. If a TE tunnel is not required, shut it down. If these symptoms are observed, the only way is to reboot.

- CSCtr59314

  Symptoms: A router reloads when the **clear crypto session** command is issued with 4000 sessions up.

  Conditions: This symptom is observed only under load conditions.

  Workaround: There is no workaround.

- CSCtr61289

  Symptoms: FlexVPN client remains in NEGOTIATING state, despite being on auto- connect mode, when the FlexVPN server executes a **clear crypto session**.

  Conditions: This occurs in a dVTI setting, where the server has a virtual- template interface and the client has a static tunnel interface that connects to the server. This is not observed in a static setting.

  Workaround: On the client, issue a **clear crypto ikev2 client flexvpn** to clear the FlexVPN session and allow the client to reconnect to the server again.

- CSCtr61623

  Symptoms: The RP crashes at _be_ace_create_acl_node.

  Conditions: This symptom is observed when configuring the 4K DVTI VT.

  Workaround: There is no workaround.

- CSCtr67852

  Symptoms: Invalid route entries injected by the RRI mechanism after an HSRP failover happens in a stateful IPSec HA setup.

  Conditions: The symptom is observed following a failover in a stateful IPSec HA setup and the use of RRI.

  Workaround: Clear all crypto sessions with **clear crypto session** or remove and add back the crypto map to the interface where it is applied.

- CSCtr69416

  Symptoms: Configuring "redistribute connected" in OSPF does not work for some interfaces. Configuring "redistribute ospf" in other protocols works even if OSPF is not enabled on interfaces.

  Conditions: This symptom occurs under the following conditions:

  - Enable OSPF on the interface using the **ip ospf area** command.
  - Delete the OSPF process using the **no router ospf** command.

  This issue is seen if the OSPF process is reenabled and the interface is not a part of a new OSPF process anymore.

  Workaround: Use the **ip ospf area** and the **no ip ospf area** commands to reset internal flags.

- CSCtr72835

  Symptoms: The "Unable to initialize the geometry of nvram" message is coming continuously on the console while performing ISSU upgrade from Cisco IOS Release XE 3.4S to Release XE 3.5S.

  Conditions: This symptom is seen when performing ISSU upgrade from Cisco IOS Release XE 3.4S to Release XE 3.5S.

  Workaround: There is no workaround.

- CSCtr79347

  Symptoms: crashes at BGP Task without a BGP configuration change or BGP neighbor up/down event.

  ```
  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = BGP Task

  Traceback summary
  % 0x80e7b6 : __be_bgp_tx_walker_process
  % 0x80e3bc : __be_bgp_tx_generate_updates_task
  % 0x7f8891 : __be_bgp_task_scheduler
  ```

  Conditions: No conditions but this is a rarely observed issue.

  Workaround: There is no workaround.

- CSCtr79905

  Symptoms: Error message seen while detaching and reattaching a service policy on an EVC interface.

Conditions: The symptom is observed when detaching and reattaching the service policy on an EVC interface when port shaper is configured on the interface.

Workaround: There is no workaround.

- CSCtr81559

  Symptoms: The PPP session fails to come up occasionally on LNS due to a matching magic number.

  Conditions: This symptom is observed during LCP negotiation, when the random magic number generated on the client matches the magic number generated on the LNS. PPP assumes it to be a loopback and disconnects the PPP session. This condition occurs rarely.

  Workaround: To avoid this, renegotiate the LCP. Configure the client using the **retry** command. This may cause the next session to come up correctly.

- CSCtr82351

  Symptoms: Router crashes when trying to change OSFP area/multipath parameters.

  Conditions: This symptom is seen when the NLFM learning process causes CPU HOG, and the router is forced to crash by watchdog.

  Workaround: There is no workaround.

- CSCtr82600

  Symptoms: More than half the amount of multicast traffic is dropped.

  Conditions: This issue is seen in scale condition when moving from data MDTs to default MDTs.

  Workaround: Clear all the mroutes in each VRF.

- CSCtr86149

  Symptoms: A router crashes if placing a call from an ISDN phone to an IP phone. The call is a secure SIP call (TLS); the phone is also using secure SCCP.

  Conditions: The router is in secure SRST mode due to a WAN outage.

  Workaround: There is no workaround.

- CSCtr86666

  Symptoms: EIGRP flap due to retry limit exceeded. On peer it is waiting for INIT ACK and complains of out of order sequence number.

  Conditions: DMVPN network with a spoke running Cisco IOS Release 15.1(4)M.

  Workaround: There is no workaround.

- CSCtr87070

  Symptoms: Enable login failed with error "% Error in authentication".

  Conditions: The symptom is observed with TACACS single-connection.

  Workaround: Remove TACACS single-connection.

- CSCtr87740

  Symptoms: A router may crash due to a bus error.

  Conditions: The symptom seems to be related to high traffic and an ongoing rekey taking place.

  Workaround: There is no workaround.

- CSCtr88739

  Symptom 1: Routes may not get imported from the VPNv4 table to the VRF. Label mismatch may also be seen.

Symptom 2: The routes in BGP may not get installed to RIB.

Conditions: The symptoms are only observed with routes with the same prefix, but a different mask length. For example, X.X.X.X/32, X.X.X.X/31, X.X.X.X/30 ..... X.X.X.X/24, etc. These issues are not easily seen and are found through code walkthrough.

For symptom 1, each update group is allocated an advertised-bit that is stored at BGP net. This issue is seen when the number of update groups increases and if BGP needs to reallocate advertised-bits. Also, this symptom is observed only with a corner case/timing issue.

For symptom 2, if among the same routes with a different prefix length, if more specific routes (15.0.0.0/32) do not have any bestpath (for example, due to NH not being reachable or inbound policy denying the path, but path exists due to soft-reconfiguration), then even if a less specific route (15.0.0.0/24) has a valid bestpath, it may not get installed.

Workaround for Symptom 1: Remove “import-route target” and reconfigure route-target.

Workaround for Symptom 2: Clear ip route x.x.x.x to resolve the issue.

- CSCtr92285

  Symptoms: The following log is seen, and VCs cannot be configured.

  SSM CM: SSM switch id 0 [0x0] allocated ACLIB [Gi9/1/0.3830, 3830]: Failed to setup switching for VLAN interface ...

  Conditions: This symptom is observed with the access circuit interface shut and core flaps occurring, along with pseudowire redundancy. Also, leaks occur per flap.

  Workaround: There is no workaround. If VCs can be removed, do so to release some IDs. Otherwise, try a redundancy switchover.

- CSCtr93337

  Symptoms: A route-map for IPv6 is configured with set VRF action. After sending the traffic, VRF neighbor is not getting resolved.

  Conditions: This symptom is seen when IPv6 PBR is configured with set VRF part.

  Workaround: Before sending the traffic, resolve neighborship by sending ping or using BGP routing protocol.

- CSCtr93685

  Symptoms: SPA console is disabled and, interface goes up/down on executing the command for SPA keepalive failure.

  Conditions: This symptom is seen after executing the **slay -s SIGSEGV spa_ipc** command at the SPA console. The SPA is UP and the controller is UP. No alarms are seen at the controller output. All the serial interfaces go UP/DOWN on the local end, and at the remote end they are DOWN/DOWN.

  After this, unable to login on the SPA console. The issue is seen on the chopper spa also.

  Workaround: Reset the line card.

- CSCtr94545

  Symptoms: Standby crashes at fm_global_feature_add_for_vrf.

  Conditions: The system crashes when virtual servers are deleted.

  Workaround: There is no workaround.

- CSCts00341

  Symptoms: When executing a CLI that requires domain-name lookup such as **ntp server** *server.domain.com*, the command fails with the following message on the console:

ASR1k(config)#ntp server server.domain.com <<< DNS is not resolved with dual RPs on ASR1k Translating "server.domain.com"...domain server (10.1.1.1) [OK]

%ERROR: Standby doesn’t support this command ^ % Invalid input detected at ’^’ marker.

ASR1k(config)#do sh run | i ntp ASR1k(config)#

Conditions: This symptom occurs on a redundant RP chassis operating in SSO mode.

Workaround: Instead of using *hostname* in the command, specify the IP address of the host.

- CSCts01653

  Symptoms: Spurious memory access seen on video monitoring router.

  Conditions: The issue is seen after recreating the interface.

  Workaround: There is no workaround.

- CSCts02627

  Symptoms: The **show mac-address-table** command displays invalid/incomplete port list for entries learned on VPLS Bridge Domain.

  It is observed that port-channel “Po1” is displayed as “Po”, and the Virtual Circuit IDs are missing in the port list of the mac-address-table entries. This is a display issue.

  Conditions: This symptom is observed only with mac-address-table entries that are learned on VPLS Bridge Domain VLAN.

  Workaround: There is no workaround.

- CSCts05166

  Symptoms: A Cisco 7200 series router drops frame-relay LMI from third party if C/R bit is set to 1 in it. This further drops the frame-relay link.

  Conditions: This symptom is seen when frame-relay+other side is sending LMI with C/R bit 1 occasionally. Encapsulation frame-relay on Cisco can be Cisco or IETF. Both noticed the problem.

  Workaround: There is no workaround.

- CSCts06929

  Symptoms: Disposition traffic gets dropped after SSO as the new local labels allocated by AToM do not get programmed on the line cards.

  Conditions: This symptom occurs when pseudowires are configured on the setup without graceful restart configured. Then, SSO is performed and two local labels have the same disposition information. This really manifests as a traffic drop issue when the scale is high.

  Workaround: Configuring graceful restart resolves this issue.

- CSCts11594

  Symptoms: A mediatrace session is scheduled with an attached session- parameter. The session is unscheduled and the session-parameters removed so that the default session parameters should be used.

  On the first schedule, traceback is seen. The session is again unscheduled and scheduled for second time and a crash is seen.

  Conditions: The symptom is observed when using custom session-parameters for a session and then removing it. Then using the default session-parameters followed by scheduled and unscheduled twice.

  Workaround: Use either the default session-parameters or custom session- parameters. Do not toggle between both.

- CSCts12193

  Symptoms: With the single hop MPLS TE tunnel from the core router to the PE router, removing the MDT default configuration may cause some control planes to go down (like LDP, BGP). This is due to misprogrammed adjacency in the hardware.

  Conditions: This symptom occurs when unconfiguring the MDT default configuration.

  Workaround: Restore the configuration.

- CSCts13255

  Symptoms: Standby SUP720 crash is observed on the Cisco 7600 router in c7600s72033-advipservicesk9-mz.150-1.S3a.bin. This issue is random and recurring. Tracebacks are generated with the following error message:

  %CPU_MONITOR-STDBY-3-PEER_FAILED: CPU_MONITOR peer process has failed to receive heartbeats

  Conditions: This symptom is observed on the Cisco 7600 router with mistral based supervisors like SUP720. This issue is fairly uncommon, but affects all the versions after Cisco IOS Release 12.2(33)SRE, including Cisco IOS Releases 15.0S, 15.1S and 15.2S. This does not affect RSP 720.

  Workaround: There is no workaround.

- CSCts13720

  Symptoms: When static pseudowires are configured with VCCV BFD, some of the VCs may not come up.

  Conditions: This symptom occurs when a static pseudowire is configured with VCCV BFD.

  Workaround: For the VCs that are DOWN, issue the **clear xconnect peer** *peer-ip-address* **vcid** *vcid value* command to bring the VC back UP.

- CSCts14799

  Symptoms: Memory leak is observed on IPSEC key engine and IPSec background.

  Conditions: This symptom occurs with 2000 IPv6 over IPv4 GRE tunnels protected by IPSEC.

  Workaround: There is no workaround.

- CSCts15034

  Symptoms: A crash is seen at dhcpd_forward_request.

  Conditions: This symptom is observed with the DHCP relay feature when it is used with a scaled configuration and significant number of DHCP relay bindings.

  Workaround: If possible, from a functional point of view, remove the **ip dhcp relay information option vpn** command. Otherwise, there is no workaround.

- CSCts16013

  Symptoms: Longevity testing session churn causes RP crash on the Cisco ASR1K router. RP crash occurs due to memory leak by the QOS Accounting feature.

  Conditions: This symptom is observed during testing with the QOS Accounting feature PAC2. This issue is seen when there are a large number of sessions and churns with “aaa-accounting” in the QOS policy-map.

  Workaround: There is no workaround.

- CSCts16285

  Symptoms: The system may experience delays in updating multicast information on the line cards. MFIB/MRIB error messages may be observed when IPC messages from the line card to the RP time out. In the worst case, the line card may become disconnected if timeouts continue for a long period.

  Conditions: This symptom occurs when the system has a very heavy IPC load or CPU load.

  Workaround: Take necessary actions, if possible, to reduce the IPC load. Sometimes, the IPC load could be due to noncritical processes.

- CSCts18404

  Symptoms: A Flex VPN (IKEv2) client may lose complete connectivity via its VPNs even though SAs are in place.

  Crypto routes are missing, and the tunnel negotiated address is missing too. Other config-exchange information may be missing too.

  Conditions: This symptom is observed on a Flex VPN client that may end up having duplicate IKEv2 SAs with a server. When this condition occurs and one of the duplicate SAs is removed (which usually happens naturally but can also happen administratively), all config-exchange configurations are withdrawn despite the fact there is still another IKEv2 SA active.

  Workaround: There is no clean workaround.

  The only solution is to manually clear the IKEv2 SAs on the Flex Client to force a renegotiation. Because the Flex Clients can be disseminated in the field and because network conditions can trigger duplicate SAs on a massive amount of clients, this workaround is barely practical.

- CSCts20246

  Symptoms: The DR for the receiver segment forwards IPv6 multicast packets on the Accepting Interface of S,G.

  Conditions: This symptom occurs while multicast stream is running and the RPF interface towards the source and RP goes down on the DR and the interface connected to the receiver (oif in S,G before interface goes down) becomes the RPF interface for the source and RP and hence iif for S,G.

  Workaround: There is no workaround.

- CSCts23708

  Symptoms: No NHRP routes will be added for all other discovered prefixes.

  Conditions: This symptom is seen when spoke to spoke traffic is triggered.

  Workaround: There is no workaround.

- CSCts23841

  Symptoms: V-cookie is not present in account profile query replies.

  Conditions: This symptom is observed in recent ISG images.

  Workaround: There is no workaround.

- CSCts23882

  Symptoms: ISG calculates the radius response authenticator in CoA account- profile-status-query replies wrongly, resulting in an invalid response.

  Conditions: This symptom is observed when the CoA/WWW based session authentication is triggered via a CoA account logon using the “old” SSG command attributes.

  Workaround: Configure a fix “NAS-IP-Address” value with the **radius- server attribute 4** *x.x.x.x* command.

- CSCts24348

  Symptoms: PBR "set vrf" feature can cause unnecessary ARP requests and packet drops if some other feature is configured on the same router interface and packets are punted to process-switching path. This issue slows down TCP traffic considerably as first SYN in a flow may always be dropped.

  Conditions: The symptom is observed with multi-VRF selection using the Policy Based Routing (PBR) feature. It was observed in all IOS versions with new CEF code (Cisco IOS Release 12.4(20)T and upwards). The issue was not seen in Cisco IOS Release 12.4(15)T and Release 12.4(25).

  Workaround: This issue can be alleviated by using proxy ARP on the upstream device. Otherwise, there is no workaround.

- CSCts27042

  Symptoms: PIM bidirectional traffic loops upon DF-election and RPF-change.

  Conditions: The symptom is observed with several hundred streams combined with a routing change (interface shutdown/no shutdown or metric increment/decrement).

  Workaround: There is no workaround.

- CSCts27333

  Symptoms: Multicast traffic is forwarded in software due to MTU failures.

  Conditions: This symptom is seen with packet size greater than the standard interface MTU being forwarded on the standby supervisor in a VSS setup. The problem is only seen with GRE tunnel OIF, where the tunnel MTU is incorrect in spite of the underlying interface being configured to accept a higher MTU.

  Workaround: There is no workaround.

- CSCts28315

  Symptoms: A DHCP PD request does not accept a specific server.

  Conditions: The symptom is observed because the router does not include any IA Prefix option in Request message. This is correct behavior of RFC:

  http://tools.ietf.org/html/rfc3633#section-10

  A requesting router may set the IPv6 prefix field to zero and a given value in the prefix-length field to indicate a preference for the size of the prefix to be delegated.

  Workaround: There is no workaround.

- CSCts31111

  Symptoms: Coredump generation fails on the Cisco 800.

  Conditions: This symptom occurs when coredump is configured.

  Workaround: Go to ROMmon, and set a variable WATCHDOG_DISABLE before the coredump happens, as follows:

  conf t config-reg 0x0 end wr reload yes <rommon prompt> DISABLE_WATCHDOG=yes sync set conf-reg 0x2102 reset

- CSCts31791

  Symptoms: Traceback is seen at id_to_ptr.

  Conditions: This symptom occurs when a multilink is brought up using a virtual-access in the Cisco 7600 or ASR platform.

  Workaround: There is no workaround.

- CSCts31868

  Symptoms: The router crashes at fmanrp_ess_is_valid_ess_segment.

  Conditions: This symptom is observed at fmanrp_ess_is_valid_ess_segment.

  Workaround: There is no workaround.

- CSCts31870

  Symptoms: Routed multicast traffic on Cisco ME 3600X and Cisco ME 3800X may be dropped intermittently.

  Conditions: This issue has been seen under the following conditions:

  - Cisco ME 3600X is running Cisco IOS Release 15.1(2)EY.
  - Multicast stream can be received on any type of interface (L2/L3).

  Packets are intermittently software switched and may be dropped on the CPU. Issue can be verified via the following:

```
Switch#show ip mfib 239.1.1.1
<output omitted>

 (*,239.1.1.1) Flags: C HW
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   332/0/1366/0, Other: NA/NA/NA
   Vlan100 Flags: A NS
   Vlan200 Flags: F NS
     Pkts: 0/0
 (10.0.0.10,239.1.1.1) Flags: HW
   SW Forwarding: 335/0/1344/2, Other: 0/0/0  <----  SW Forwarding for S,G 
increments
   HW Forwarding:   16651904/778/1366/8305, Other: NA/NA/NA
   Vlan100 Flags: A
   Vlan200 Flags: F NS
     Pkts: 0/335
```

  Workaround: There is no workaround.

- CSCts32920

  Symptoms: Traffic gets punted to the RP.

  Conditions: This symptom occurs when there are multiple P2P-GRE tunnels in a particular VRF. Remove one particular P2P-GRE tunnel from that VRF.

  Workaround: Shut/no shut P2P-GRE tunnels in that particular VRF, for which traffic is getting punted to the RP.

- CSCts32963

  Symptoms: Standby is not coming up.

  Conditions: This symptom occurs when a distribute-list is configured. The ACL is created if it does not exist. Then remove the ACL, but the distribute-list configuration that ties to the ACL is not removed. Configure the IPv6 ACL configuration with the same ACL name. Save the configuration and reload it.

  Workaround:

1) When an access list is removed, remove corresponding distribute-list configuration as well.

2) Do not use the same access list name for IPv4 and IPv6.

- CSCts34693

  Symptoms: A Cisco router may crash with the following error message:

  000199: *Aug 23 16:49:32 GMT: %BGP-5-ADJCHANGE: neighbor x.x.x.x Up

  Exception to IOS Thread: Frame pointer 0x30CF1428, PC = 0x148FDF84

  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = EEM ED Syslog -Traceback= 1#07279b80de945124c720ef5414c32a90 :10000000+48FDF84 :10000000+48FE400 :10000000+4B819C8 :10000000+4B81964 :10000000+F5FAD8 :10000000+F5FD10 :10000000+F5FEF0 :10000000+F5FF94 :10000000+F60608

  Conditions: This symptom is observed in a Cisco ASR 1004 router running IOS Release 15.0(1)S. This problem appears to be related to an EEM script that executes on a syslog event.

  event manager applet BGP-MON event tag BGP-DOWN syslog pattern "BGP-5-ADJCHANGE.*Down" event tag BGP-UP syslog pattern "BGP-5-ADJCHANGE.*Up" trigger correlate event BGP-DOWN or event BGP-UP action 02 cli command "enable" action 03 cli command "sh log" action 04 mail server "$_email_server" to "$_email_to" from "$_info_routername@mcen.usmc.mil" subject "Problems on $_info_routername, BGP neighbor Change" body "$_cli_result"

  Workaround: There is no workaround at this time.

- CSCts37314

  Symptoms: The session goes down after changing the BFD timers.

  Conditions: This symptom is observed after changing the BFD timers.

  Workaround: Perform shut/no shut on the interface.

- CSCts37446

  Symptoms: Traceback is observed while testing the antireplay feature.

  Conditions: Traceback is observed while configuring the routers randomly. It is not observed manually.

  Workaround: There is no workaround.

- CSCts39240

  Symptoms: The **advertise** command is not available in BGP peer-policy templates.

  Conditions: This symptom is observed on Cisco router running Cisco IOS Release 15.2(01.05)T, Cisco IOS Release 15.2(00.16)S, Cisco IOS Release 15.1 (03)S0.3, or later releases.

  Workaround: The keyword and functionality is still available to be configured in the BGP neighbor command.

- CSCts39284

  Symptoms: Packet is corrupted. The bottom of the label stack bit is not set correctly.

  Conditions: This symptom is seen when ibgp+label is configured.

  Workaround: There is no workaround.

- CSCts39535

  Symptoms: BGP IPv6 routes that originate from the local router (via network statements or redistribute commands) fail to match any specified condition in an outbound route map used on a neighbor statement, regardless of the expected matching results. Thus, the route map may not be applied correctly, resulting in erroneous filtering or advertising of unintended routes.

  Further testing revealed that the **suppress-map** and **unsuppress-map** commands (used in conjunction with the **aggregate-address** command) are also broken, in the sense that the route-map filtering will fail to correctly suppress or unsuppress a subnet under the aggregated prefix.

  Conditions: An outbound route map with a match statement is used in a “neighbor” statement for an IPv6 or VPNv6 neighbor in BGP, and there are locally originated routes, either through network statements or by redistribution. All “match” statements except for “as-path,” “community,” and “extcommunity” are impacted; this includes match ipv6 address, protocol, next-hop, route-source, route-type, mpls, tag.

  Workaround: None for the same router. However, inbound route maps work fine, so configuring inbound route maps on the neighboring router can compensate.

  Another way to handle it would be to configure prefix lists directly on the network statement. So filtering will be preserved. But, there will not be a way to “set” anything as route maps can typically do.

- CSCts41217

  Symptoms: Memory leak occurs in const_mfib_lc_* processes.

  Conditions: This symptom is observed during deletion and addition of VRFs. Multicast needs to be enabled in the VRF and the P2P tunnels should be present in the VRF. VRF should be removed before deleting the P2P tunnels for this to happen.

  Workaround: Delete all the P2P tunnels before removing the VRF

- CSCts42154

  Symptoms: After the Cisco IOS ASR 1006 router is reloaded, it fails to reregister to the key server. From the debugs, it is observed that the attempt to register is generated too early before the GDOI is ON. This registration attempt is made before the interface, through which GDOI registration traffic with the key server passes, goes to the UP state.

  Conditions: This symptom is observed on a Cisco IOS ASR 1006 router that runs Cisco IOS Release 15.0(1)S2 and Cisco IOS Release 15.0(1)S3.

  Workaround: Use the **clear crypto gdoi** command to fix this issue.

- CSCts44718

  Symptoms: A router may crash.

  Conditions: The crash may occur when a service policy that has a flow monitor as an action is applied to a virtual interface and that virtual interface is deleted. It may also occur when the service policy is applied to a physical interface that is removed by OIR.

  Workaround: Before deleting (or OIRing) the interface, remove the flow monitor from the policy or the policy from the interface.

- CSCts45619

  Symptoms: T.38 Fax calls through the CUBE enterprise on the Cisco ASR platform with the Cisco IOS MTP colocated on the ASR can fail with cause 47 and subsequently leak a structure on the forwarding plane, causing future call failures.

  Conditions: This symptom is observed with T.38 calls through the CUBE enterprise on the Cisco ASR platform (only) with colocated MTPs in the call flow.

Workaround: On nonredundant ASR platforms, a reload is required to clear the hung structures on the forwarding plane. On the Cisco ASR1006 with redundant RPs and ESPs, you can perform a switchover of the ESPs (FPs) to clear the problem, as follows:

hw-module slot F0 reload ! confirm via show platform that the F0 is in a ok, standby state, takes some time for the F0 to reload. sh platform ! do not execute the below command until F0 is back online hw-module slot F1 reload ! again, confirm via show platform that the F1 is in a ok, standby state sh platform

- CSCts47566

  Symptoms: During standby RP bootup, an incorrect ICMP punt entry for MPLS interfaces gets programmed. This entry appears even if the interface has no ACL applied in the input/output direction.

  2037#show tcam inter gi4/0/3 acl in ip

  * Global Defaults shared

  Entries from Bank 0

  punt icmp any any eq 11 <<<<<<<<<<<<<<<< permit ip any any (1895 matches)

  Entries from Bank 1

  Conditions: This symptom is observed with the ICMP punt entry, which is required to allow trace route across MPLS cloud. This is a workaround for a hardware problem with Tycho. The feature is called “FM_FEATURE_MPLS_ICMP_BRIDGE”. This workaround is required only if there are aggregate labels programmed in the superman VPN cam, but can get set incorrectly even when there is no VRF configuration on the box.

  Workaround: To clear the entry set unnecessarily, disable/enable MPLS on the interface for which it appears.

- CSCts47605

  Symptoms: For ECMP on the Cisco ASR1k router, RSVP does not select the right outgoing interface.

  Conditions: This symptom is observed with RSVP configuration with ECMP.

  Workaround: There is no workaround.

- CSCts47776

  Symptoms: Router crashes due to Mediatrace performance monitor debug.

  Conditions: The issue is seen with debug performance monitor database.

  Workaround: There is no workaround.

- CSCts47982

  Symptoms: Multicast traffic drops on trunk ports with output drops incrementing.

  Conditions: This symptom is observed when non-rpf packets make it to the node due to the network redundancy. The hardware met is wrongly programmed for rpf- fail packet handling.

  Workaround: Shut the interface on which non-rpf packets are coming on. Alternatively, change the DR priorities so that multicast forwarding happens only from one of the nodes.

- CSCts48300

  Symptoms: Interface queue wedge may occur when malformed traffic is received on port UDP 465. A maximum of 50 packets will become wedged.

  Conditions: Some malformed traffic must exist.

Workaround: There is no workaround.

- CSCts49032

  Symptoms: Data traffic is getting block-holed.

  Conditions: This symptom occurs with the removal/addition of default MDT address in VRF, with time gap of 30 minutes.

  Workaround: Deletion/addition of VRF.

- CSCts51980

  Symptoms: STM1-SMI PAs of version 3.0 do not come up.

  Conditions: This symptom is observed when the new version of PAs do not come up with enhanced flexwan.

  Workaround: There is no workaround. Without the PA, flexwan will come up.

- CSCts52643

  Symptoms: Session will not get offloaded to hardware when enabling HWO using the **no platform bfd enable-offload** command.

  Conditions: This symptom is seen when all workload credit is allocated so no more sessions are coming up.

  Workaround: There is no workaround.

- CSCts55322

  Symptoms: More traffic is sent out because of stale MET entries.

  Conditions: This symptom occurs in a scale condition when the route towards the core on the source PE is changed.

  Workaround: There is no workaround.

- CSCts55371

  Symptoms: OSPF will not flood link state updates over an interface. The command **show ip ospf flood-list** will show interface entries similar to:

  Interface Tunnel1, Queue length 181 Link state retransmission due in 1706165974 msec

  Note the high value for the retransmission timer.

  Conditions: The symptom is observed with some newer S and T releases including Cisco IOS Release 15.1(2)S, Release 15.1(3)S, and Release 15.2(1)T.

  The issue can occur on interfaces where OSPF has not flooded updates for more than 24 days. This can include interfaces that are newly configured for OSPF if the router has been up longer than that. Interfaces that flood LSAs at least once every 24 days will not be affected.

  Workaround: To clear a hung interface use **clear ip ospf process**.

- CSCts56044

  Symptoms: A Cisco router crashes while executing a complex command. For example:

  show flow monitor *access_v4_in cache aggregate ipv4 precedence sort highest ipv4 precedence top 1000*

  Conditions: This symptom is observed while executing **show flow monitor** *top* top-talkers command.

  Workaround: Do not execute complex flow monitor top-talker commands.

- CSCts56277

  Symptoms: The Cisco IOSd crashes.

  Conditions: This symptom occurs during CC reload.

  Workaround: This issue is inconsistently seen. After the crash happens, the SIP comes up fine.

- CSCts57115

  Symptoms: After the following procedure is executed, multicast traffic on several VRFs is not forwarded to the outbound tunnel interface for MDT.

  The procedure is as follows: 1) Reload the router. 2) Perform RP switchover. 3) Perform active ESP(F0) hardware reload. 4) Perform active ESP(F1) hardware reload.

  Conditions: This symptom is observed when MVPN sends out multicast traffic on a lot of VRFs.

  Workaround: Use the **ip pim sparse-mode** command to reconfigure the loopback0(global) interface.

- CSCts57295

  Symptoms: The following commands will be displayed by the **show running configuration** command even if only the **mac- address-table notification change mac-address-table notification mac- move** command is used or if only the **mac address-table notification change mac address-table notification mac-move** command is used. Also, we can delete all of them by deleting one pair of them.

  mac-address-table notification change mac-address-table notification mac-move

  mac address-table notification change mac address-table notification mac-move

  When reloading the device with the above command, the switch crashes and reboots itself.

  Conditions: This symptom is seen when reloading the device with the following commands:

  mac-address-table notification change mac-address-table notification mac-move

  mac address-table notification change mac address-table notification mac-move

  Workaround: There is no workaround.

- CSCts58394

  Symptoms: The SNMP graph traffic rate (collected from the port-channel subinterface) does not match the 5-minute offered rate from “show policy-map inter port-channel x.x”.

  Conditions: This symptom occurs on the Cisco 7600-S running Cisco IOS Release 15.0(1)S4 with the port-channel subinterface on 76-ES+XC-40G3CXL. This issue is seen only when there is EARL recirculation of packets and affects only the ingress traffic rate.

  Workaround: There is no workaround.

- CSCts59014

  Symptoms: Only one ATM VC shaper token is updated per cycle in a high-scale scenario.

  Conditions: This symptom is observed with HQOS on ATM VC with many ATM VCs per interface.

  Workaround: There is no workaround.

- CSCts59564

  Symptoms: PIM neighbor over MDT tunnel goes down.

  Conditions: The symptom is observed with **hw-module reset** of access and core card, followed by an SSO.

  Workaround: There is no workaround.

- CSCts62082

  Symptoms: Router generates the following message:

  %NHRP-3-QOS_POLICY_APPLY_FAILED: Failed to apply QoS policy 10M-shape mapped to NHRP group xx on interface Tunnelxx, to tunnel x.x.x.x due to policy installation failure

  Conditions: The symptom is observed when "per-tunnel" QoS is applied and there are more than nine DMVPN spokes. (Up to eight spokes, with QoS applied is fine.)

  Workaround: There is no workaround.

- CSCts63501

  Symptoms: The non-EOS forwarding path for the explicit null label (reserved label 0) is programmed as drop on the line card, resulting in PW traffic loss with an MPLS LDP explicit-null configuration.

  Conditions: The PW traffic loss occurs on line cards in which MPLS LDP explicit-null is set.

  Workaround: There is no workaround.

- CSCts64539

  Symptoms: The BGP next hop is inaccessible. The **show ip route** command output in the global and VRF routing tables shows that the next hop is reachable. The **show ip bgp vpnv4 all attr next-hop** command output shows max metric for the next hop.

  Conditions: This symptom occurs when an import map uses the "ip vrf name next-hop" feature while importing single-hop eBGP routes from the global routing table to the VRF routing table.

  Workaround 1: If "set ip next-hop" is not configured in import route map, this issue does not occur.

  Workaround 2: If "neighbor x.x.x.x ebgp-multihop" is configured, this issue does not occur. The knob needs to be configured for all eBGP peers, where routes are imported to the VRF with "et ip next-hop".

  Workaround 3: If "neighbor x.x.x.x disable-connected-check" is configured for a single-hop eBGP, this issue does not occur. The knob needs to be configured for all eBGP peers, where routes are imported to the VRF with "set ip next-hop".

- CSCts65564

  Symptoms: In a large scale DMVPN environment, a DMVPN hub router may crash in the IOS process under high scale conditions.

  Conditions: This only occurs if CRL caching is disabled (with the command **crl cache none** under the pki trustpoint configuration).

  Workaround: Enable CRL caching (this is the configured default).

- CSCts67465

  Symptoms: If you configure a frequency greater than the enhanced history interval or if the enhanced history interval is not a multiple of the frequency, the standby will reset.

  Conditions: The symptom is observed always, if the standby is configured as an SSO.

  Workaround: Remove enhanced history interval configuration before resetting the frequency.

- CSCts68541

  Symptoms: In IPsec scaling test, when CPE is keeping reload, all IPsec sessions will be torn down and reestablished. During the session flapping, RP reset is observed sometimes.

  Conditions: This symptom is seen with CPE reloading continually.

  Workaround: There is no workaround.

- CSCts68630

  Symptoms: IPv6 ACL may not match the traffic as per the configuration when there is an ACL configuration change.

  Conditions: This issue is seen when you configure an ACL list with a mix of ACL entries with the source address set to “any” and set with a specific value.

  Workaround: You can enter the ACL list entries in sequence in increasing order, for example:

  permit icmp any host 2A00:2180:400:212:31:220:174:1 sequence 10 permit icmp any host 2A00:2180:4400:204:109:193:249:1 sequence 20 permit icmp any host 2A00:2180:4400:192:199:150:1:1 sequence 30 log-input permit tcp any eq bgp host 2A00:2180:4400:204:109:193:249:1 sequence 110 permit tcp any host 2A00:2180:4400:204:109:193:249:1 eq bgp sequence 115 permit tcp any eq bgp host 2A00:2180:4400:192:199:150:1:1 sequence 120 permit tcp any host 2A00:2180:4400:192:199:150:1:1 eq bgp sequence 125 permit udp any eq 1645 any range 1024 49151 sequence 210 permit udp any eq 1812 any range 1024 49151 sequence 220 permit udp any eq bootps any eq bootps sequence 310 permit udp any host 2A00:2180:4400:204:109:193:249:1 range 3784 3785 sequence 410 deny ipv6 any 2A00:2180::/37 sequence 510 deny ipv6 any host 2A00:2180:4400:204:109:193:249:1 sequence 610 deny ipv6 any host 2A00:2180:4400:192:199:150:1:1 sequence 615 log-input permit ipv6 any any sequence 999 log-input

- CSCts69204

  Symptoms: PPPoE sessions do not get recreated on the standby RP.

  Conditions: This symptom occurs on the standby RP.

  Workaround: There is no workaround.

- CSCts69973

  Symptoms: Spoke with 100 tunnels crashed at nhrp_process_delayed_resolution_event_wrapper.

  Conditions: Source interfaces of the tunnels started to bring up.

  Workaround: There is no workaround.

- CSCts70790

  Symptoms: A Cisco 7600 router ceases to advertise a default route configured via “neighbor default-originate” to a VRF neighbor when the eBGP link between a Cisco 7600 router and its VRF eBGP peer flaps.

  Conditions: This symptom is observed when another VPNv4 peer (PE router) is advertising a default route to the Cisco 7600 router with the same RD but a different RT as the VRF in question. When the VRF eBGP connection flaps, the VRF default is no longer advertised.

  Workaround: Remove and re-add the **neighbor default- originate** command on the Cisco 7600 router and do a soft clear for the VRF neighbor.

- CSCts71958

  Symptoms: When the router is reloaded due to crash, the **show version** output shows the reload reason as below:

  Last reload reason: Critical software exception, check bootflash:crashinfo_RP_00_00_20110913-144633-PDT

  After this, the same reason is shown even if the router is reloaded several times using the **reload** command.

  Conditions: The issue seen after a crash.

Workaround: There is no workaround.

- CSCts72911

  Symptoms: In case of a GR/NSF peering, after an SSO switchover, the restarting router (PE, in this case) does not advertise RT constrain filters to the non-restarting peer (RR, in this case).

  Conditions: The symptom is observed after an SSO switchover in GR/NSF peering. Due to the RT constrain filters not sent by the restarting router after the SSO, the non-restarting router does not send back the corresponding VPN prefixes towards the restarted router.

  Workaround: There is no workaround.

- CSCts74982

  Symptoms: Performance Monitor is unable to create monitor object for policy because of collision when creating monitor object.

  Conditions: The issue is seen with dynamic Performance Monitor policy on Mediatrace routers.

  Workaround: There is no workaround.

- CSCts76410

  Symptoms: Tunnel interface with IPSec protection remains up/down even though there are active IPSec SAs.

  Conditions: The symptom is observed during a rekey when the IPSec lifetime is high and the control packets do not reach the peer. The issue was observed on Cisco IOS Release 12.4(20)T and Release 15.0(1)M7.

  Workaround: Shut/no shut the tunnel if the situation occurs. You can use EEM to recover automatically.

- CSCts76964

  Symptoms: The Cisco ASR router crashes with tracebacks, as given below:

  Exception to IOS Thread: Frame pointer 0x7F5CED910380, PC = 0x2F4A2E7

  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = Crypto IKMP -Traceback= 1#261f9625131701783f9129d7afdd6633 :400000+2B4A2E7 :400000+4FAFFBF :400000+4FBC2FB :400000+4FBC662 :400000+371635B :400000+63E0B86 :400000+63DCB63 :400000+63F13A6 :400000+63F15 6D :400000+629144E :4 00000+63E51A1 :400000+64BE0B1 :400000+64BE037 :400000+63E5D59 :400000+624BB06 :400000+63DBC34

  Fastpath Thread backtrace: -Traceback= 1#261f9625131701783f9129d7afdd6633 c:7F5DE3D0F000+BDDD2

  Auxiliary Thread backtrace: -Traceback= 1#261f9625131701783f9129d7afdd6633 pthread:7F5DE1D0E000+A7C9

  RAX = 0000000000000000 RBX = 006DE6F05C7F0000 RCX = 0000000000000000 RDX = 0000000000000000 RSP = 00007F5CED910380 RBP = 00007F5CED9103A0 RSI = 0000000000000000 RDI = 4060D60A00000000 R8 = 00000000F0466060 R9 = A038E6F05C7F0000 R10 = 000000000AEF96B8 R11 = 8038E6F05C7F0000 R12 = 0000000000000000 R13 = 00007F5CF0A51A80 R14 = 4060D60A00000000 R15 = 0000000000000000 RFL = 0000000000010246 RIP = 0000000002F4A2E7 CS = 0033 FS = 0000 GS = 0000 ST0 = 0000 0000000000000000 ST1 = 0000 0000000000000000 ST2 = 0000 0000000000000000 ST3 = 0000 0000000000000000 ST4 = 0000 0000000000000000 ST5 = 0000 0000000000000000 ST6 = 0000 0000000000000000 ST7 = 0000 0000000000000000 X87CW = 037F X87SW = 0000 X87TG = 0000 X87OP = 0000 X87IP = 0000000000000000 X87DP = 0000000000000000 XMM0 = 0D0D0D0D0D0D0D0D0D0D0D0D0D0D0D0D XMM1 = 00040000000000000000080000040001 XMM2 = 806E29E23003000000000000000000800 XMM3

= FD01000580030D028001000180010004 XMM4 = 00000000000000000000000000000000 XMM5 = 00000000000000000000000000000000 XMM6 = 00000000000000000000000000000000 XMM7 = 00000000000000000000000000000000 XMM8 = 00000000000000000000000000000000 XMM9 = 00000000000000000000000000000000 XMM10 = 00000000000000000000000000000000 XMM11 = 00000000000000000000000000000000 XMM12 = 00000000000000000000000000000000 XMM13 = 00000000000000000000000000000000 XMM14 = 00000000000000000000000000000000 XMM15 = 00000000000000000000000000000000 MXCSR = 00001F80

Writing crashinfo to bootflash:crashinfo_RP_00_00_20110308-100545-UTC

Conditions: The symptom is observed under the following conditions:

- GETVPN is operational on the Cisco ASR router.
- Registration to the Key-Server happens over the physical links.
- There is one primary and secondary link to the Key-Server.
- The crypto map is enabled on the primary interface first. Everything works fine here.
- The crypto map is enabled on the secondary interface.The ASR crashes as soon as you enable it on the Secondary interface with tracebacks, as shown above.
- The crash is also observed if the secondary interface is down and the crypto map is applied on it, although the crash is not observed instantly.
- The issue is also observed in Cisco IOS Release 15.1(3)Sa, along with Cisco IOS Release 12.2(33)XNE (could be reproduced only once at the first instance, and was not seen in subsequent tries) and Cisco IOS Release 12.2(33)XNF2.

When the same GDOI crypto-map is applied to two interfaces (in primary and secondary role), without the local-address configuration and TBAR enabled, and when KS sends the TBAR pseudotime update, the GM code gets confused between the two interfaces and the crash is observed. It is considered to be more of a timing issue.

Workaround 1: Disable TBAR on the Key-Server, that is, either with no replay or by changing it to counter-based to resolve the issue.

Workaround 2: Use the **crypto map** *name* **local-address** *logical-address* command globally on the Cisco ASR router and let the registration happen through the loopback.The loopback should be reachable to the Key-Server over the primary and the secondary links, respectively. Then, enable the crypto map on the primary and secondary interfaces, which will work fine.

- CSCts81427

  Symptoms: With a scaled dLFIoATM configuration on FlexWAN, after issuing SSO, some of the interfaces stop pinging.

  Conditions: This symptom is observed after doing SSO.

  Workaround: Shut/no shut of the ATM interface helps to resolve the problem.

- CSCts82058

  Symptoms: Creation of Overlay interface leads to router crash.

  Conditions: This symptom is seen when configuring overlay interface and enabling OTV commands followed by the **otv join-interface** command on the core facing interface.

  Workaround: There is no workaround.

- CSCts84357

  Symptoms: Router crashes when deconfiguring router ISIS which has the BFD enabled.

Conditions: This symptom is seen where there are multiple ISIS instances that have BFD enabled, and one of the ISIS instances is deleted.

Workaround: Do not enable ISIS BFD on multiple ISIS instances or disable ISIS BFD from the instance before deconfiguring it.

- CSCts85694

  Symptoms: The following error message is displayed:

  %FMANRP_ESS-3-ERREVENT: TC still has features applied. TC evsi (0x104C2E4)

  Conditions: This symptom is seen when clearing the sessions after a long time, and the memory leak increases incrementally. Leak is very slow.

  Workaround 1: Do not bring down all sessions together.

  Workaround 2: Do not tear down the sessions (scale numbers: 4k and above) together from different sources (say clearing PPP sessions and ISG sessions in lab; in field, clearing might happen via other triggers) simultaneously with no time gap between them.

  Workaround 3: Do not have accounting accuracy configured.

  Workaround 4: In this case, ISG Features are applied on TC and Session both. If we do not apply the features on the TCs, chances of this happening are less.

- CSCts86788

  Symptoms: CPU Hog messages start to appear followed by a crash.

  Conditions: This symptom is observed when the **show mpls traffic-eng fast-reroute database interface** *name* **detail** command is issued on an interface where there are no MPLS-TE tunnels.

  Workaround: Do not issue this command on an interface where there are no MPLS-TE tunnels.

  Further Problem Description: The trigger is simple, that is, issuing the FRR **show display** command on an interface on which there are no MPLS-TE tunnels.

- CSCts88467

  Symptoms: Drops happen earlier than expected.

  Conditions: This symptom occurs if the queue-limit is incorrectly calculated.

  Workaround: Configure a queue-limit explicitly to fix this issue, then remove and reapply the policy. Configuring queue-limit in parent policy automatically triggers calculation based on the parent queue-limit value on the child queue-limits based on bandwidth allocated to various classes.

- CSCts88817

  Symptoms: ASA-SM(s) and SCV-NAM3 in a Cisco Catalyst 6000 series switch may be reloaded by supervisor associated with the following syslogs reported by the switch:

  %CPU_MONITOR-SP-6-NOT_HEARD: CPU_MONITOR messages have not been heard for 31 seconds [4/0] %CPU_MONITOR-SP-6-NOT_HEARD: CPU_MONITOR messages have not been heard for 31 seconds [9/0] %CPU_MONITOR-SP-6-NOT_HEARD: CPU_MONITOR messages have not been heard for 61 seconds [4/0] %CPU_MONITOR-SP-6-NOT_HEARD: CPU_MONITOR messages have not been heard for 61 seconds [9/0] %CPU_MONITOR-SP-6-NOT_HEARD: CPU_MONITOR messages have not been heard for 91 seconds [4/0] %CPU_MONITOR-SP-6-NOT_HEARD: CPU_MONITOR messages have not been heard for 91 seconds [9/0] %OIR-SP-3-PWRCYCLE: Card in module 4, is being power-cycled 'off (Module not responding to Keep Alive polling)' %C6KPWR-SP-4-DISABLED: power to module in slot 4 set off (Module not responding to Keep Alive polling) %OIR-SP-3-PWRCYCLE: Card in module 9, is being power-cycled 'off (Module not responding to Keep Alive polling)' %C6KPWR-SP-4-DISABLED: power to module in slot 9 set off (Module not responding to Keep Alive polling)

Conditions: The lockup may occur if there are non-fabric cards in the chassis with the ASA or NAM3 card. Non-fabric cards have a model number of 61xx, 62xx, 63xx, and 64xx.

Workaround: There is no workaround.

- CSCts89761

  Symptoms:

  1. Inline service policy Configuration: Unable to configure monitor parameters once the flow monitor is specified. See the following example:

  Router(config)#interface GigabitEthernet0/2/1 Router(config-if)#service-policy type performance-monitor inline input Router(config-if-spolicy-inline)#match access-group 110 Router(config-if-spolicy-inline)#flow monitor FM_DEF_TCP <--- After this point, all configs will print out an error message Router(config-if-spolicy-inline)#monitor parameters <----- Not accepted Router(config-spolicy-inline-mparam)#interval duration 10 <-------- Not accepted Router(config-spolicy-inline-mparam)#history 5 <------------ Not accepted

  2. Non-inline service policy: Unable to change monitor parameters once the flow monitor is bound to a policy-map and attached to an interface. See the following example:

  If an attempt is made to change monitor parameters of an already attached policy as below, it will be rejected.

  UUT_451(config)#policy-map type performance-monitor VM_POLICY UUT_451(config-pmap)#class VM_CLASS UUT_451(config-pmap-c)#flow monitor VM_MONITOR UUT_451(config-pmap-c)#monitor parameters UUT_451(config-pmap-c-mparam)#history 6 <----------- Error message will show up if previous history value is different UUT_451(config-pmap-c-mparam)#interval duration 7 <----- Error message will show up if previous interval duration is different UUT_451(config-pmap-c-mparam)#react 102 mrv <-------- Error message will show up if this react was not configured before or if the subsequent command changes the threshold value of the already-configured react.

  Conditions:

  1. This symptom is seen when configuring an inline service policy for performance monitor on ASR platform.
  2. This symptom is seen when modifying monitor parameters of a non-inline service policy for performance monitor on a Cisco ASR platform.

  Workaround:

  1. To configure inline service policy, always specify all monitor parameters first and put the **flow monitor** *monitor name* command as the last command in the configuration.
  2. To change monitor parameters, remove the service-policy by using the **no service-policy** command, make your changes, and then reattach the service-policy.

  The above configuration restrictions do not apply if the enclosing policy-map is not attached to any interface. Also the changes do not apply if you specify an "empty" flow monitor, for example a flow monitor without an enclosing valid flow record.

- CSCts90734

  Symptoms: IKEA message trace entry memory leak is seen.

  Conditions: This symptom occurs when there is an IPsec session.

Workaround: There is no workaround.

- CSCts91603

  Symptoms: Higher rate is seen on the QoS policies attached on the L3 interface, which has multicast interest.

  Conditions: This symptom is seen when the non-rpf packets make way into the node due to wrong handling by the hardware met. The L3 interfaces see these packets where they are dropped. But before they get dropped, they get accounted in the egress QoS policy on the L3 interface.

  Workaround: Shut the interface on which these non-rpf packets make way or clear the multicast groups once.

- CSCts97124

  Symptoms: Active crashes upon configuring a large number of TP tunnels with scale configurations either using copy paste or loading from a configuration file.

  Conditions: This symptom is not very consistent, not reproducible all the time, and happens only on adding tunnel TP configurations. The crash occurs when the protect-lsp is being configured.

  Workaround: Manually add the MPLS-TP tunnels through CLI instead of copying from a configuration or copy pasting a large configuration.

- CSCts97803

  Symptoms: When a policy-map is configured with two RTP class-maps and two RTP encapsulated MDI class-maps, flows are monitored on them. Changing one of the RTP class-maps to MDI will lead to the crash. Also when a policy-map is configured with both RTP and MDI class-maps, and if the flow being monitored by them is RTP encapsulated MDI flows, then RTP monitoring will not work.

  Conditions: This symptom is seen when policy-map is configured with both RTP and MDI class-maps. The RTP flow to be monitored should be RTP encapsulated MDI flow.

  Workaround: There is no workaround.

- CSCts97856

  Symptoms: PIM Assert is sent out from a router with metric [0/0], though the router has a less preferred path to reach the Source or RP.

  Conditions: This symptom occurs when an mroute is first created and its RPF lookup to the Source or RP is via BGP or Static, which involves recursive lookup, or there is no valid path to reach Source or RP. This issue only occurs in a small window in milliseconds. After the window, the metric [0/0] is corrected.

  Workaround: There is no workaround.

- CSCts97925

  Symptoms: IPv6 pings within VRF fail, where the next-hop (egress) is part of the global.

  Conditions: This symptom is observed only with IPv6, and not with IPv4.

  Workaround: Disable IPv6 CEF.

- CSCts98336

  Symptoms: IKEv2 router crashes in exec when unconfiguring an active IKEv2 profile.

  Conditions: The symptom is observed when an IKEv2 profile is in use. The crash is occurring only if the profile is configured in a certain way.

  Workaround: Unconfigure first the AAA authorization block.

Conf t crypto ikev2 profile <profilename> no aaa authorization group <type> list <AAA list name> name-mangler <Mangler name>

no crypto ikev2 profile <profilename>

- CSCtt00253

  Symptoms: When both active and standby are Up, active crashes.

  Conditions: This symptom occurs when doing redundancy force switchover.

  Workaround: There is no workaround.

- CSCtt01056

  Symptoms: When a shell map configuration includes a parameter with no default value, that is, parameter1="", "<>", or "", then that parameter should be considered mandatory. During service activation of that shell map, if parameter1 is not provided by Radius, the activation should be rejected:

  - In case of service activation from Access-Accept, the session should be terminated.
  - In case of service activation from COA, the COA should be NAKed, and the services rolled back.

  Conditions: This symptom is observed with a shell map configuration when some parameters do not have the default value configured, such as param="", "<>", or "". This issue is seen with service activation with a missing mandatory parameter.

  Workaround: There is no workaround.

- CSCtt02313

  Symptoms: When a border router (BR) having a parent route in EIGRP is selected, “Exit Mismatch” is seen. After the RIB-MISMATCH code was integrated, RIB-MISMATCH should be seen, and the TC should be controlled by RIB-PBR, but they are not.

  Conditions: This symptom is observed when two BRs have a parent route in BGP and one BR has a parent route in EIGRP. The preferable BR is the BR which has a parent route in EIGRP. The BRs having BGP have no EIGRP configured.

  Workaround: There is no workaround.

- CSCtt02645

  Symptoms: CPUHOG is seen due to flapping of all NHRP.

  Conditions: This symptom is observed with scaling to 3k spokes on RP1.

  Workaround: There is no workaround.

- CSCtt03126

  Symptoms: Cisco ME 3600X is not passing multicast packets to 224.0.0.x through EVC configuration unicast traffic and multicast traffic except 224.0.0.x passes through without any issues. This has been observed on TenGig interface on the Cisco ME 3600X.

  Conditions: This symptom is seen under the following conditions:

  1. Bridge Domain is greater than 4094 or
  2. Spanning tree mode is not MST or
  3. Packets coming into the Cisco ME 3600X are untagged.

  Workaround:

  1. Make sure that the packets coming into the Cisco ME 3600X are tagged with VLAN ID. If it is a L3 port, then create a subinterface and configure encapsulation dot1q vlan.

2. Configure Spanning Tree mode as MST.
3. Bridge Domain should be less than 4094.

- CSCtt03485

  Symptoms: ES40: IDBMAN crash is seen with "no ip flow-export destination <> vrf <>".

  Conditions: This symptom occurs when "ip flow-export destination 10.21.1.1 3000 vrf vrf_1120" is removed.

  PE2(config)#no ip flow-export destination 10.21.1.1 3000 vrf vrf_1120

  PE2#show vlan internal usage | i NDE both NDE internal VLANs 1013, 1015 are cleared from 'internal VLAN table'

  PE2#show monitor event-trace idbman all | i NDE clear NDE_1013 vlan 1013 clear NDE_1013 vlan 1013 mapping 1013 is cleared, but 1015 is not cleared from idbman mapping

  PE2#test platform debugger callfn name idbman_dump_vlans 0 Calling address (0x0AF46AFC) 1: Vl1 : 1 1015: NDE_1015 : 1015 mapping 1015 is still present in IDBMAN, eventhough 1015 is a free VLAN, so, it can be allocated to any new interface

  Now, 1015 can be allocated for any other new interface, as it is cleared from "internal VLAN table", whereas it is not cleared from IDBMAN mapping. Thus, you can reproduce the IDBMAN inconsistency with NDE interfaces.

  When a new interface comes UP, the IDBMAN set will fail, as there is already an old mapping existing (NDE_1015). When you try to delete this new interface, it will try to clear the mapping in IDBMAN. But, it finds the old mapping (NDE_1015); hence, you must perform forced crash in idbman_if_clear_vlan_id and configure "ip flow-export destination 10.21.1.1 3000 vrf vrf_1120".

  PE2#show vlan internal usage | i NDE 1013 NDE 1015 NDE_vrf_0

  PE2#show monitor event-trace idbman all | i NDE set NDE_1013 vlan 1013 set NDE_1015 vlan 1015

  PE2#test platform debugger callfn name idbman_dump_vlans 0 Calling address (0x0AF46AFC) 1: Vl1 : 1 1013: NDE_1013 : 1013 1015: NDE_1015 : 1015

  Workaround: Reload.

- CSCtt04093

  Symptoms: VC is not coming up after unshutting the preferred path/Tunnel.

  Conditions: This symptom is seen when configuring ATOM Tunnel from CE1 to CE2 using next hop destination address as preferred path and disabling fall back option.

  Shut down the preferred path and verify that AToM VC is not routed to another available route and that AToM VC is down.

  Now the preferred path is not found, and VC is down.

  Workaround: There is no workaround.

- CSCtt04411

  Symptoms: Load image on router with c7200-adventerprisek9-mz.152-1.12.T.

  Conditions: This symptom is observed when verifying the SNMP configurations on server for the entry of the threshold table.

  Workaround: There is no workaround.

- CSCtt04448

  Symptoms: There is a loss of IGMP snooping entries with a traffic drop at the pmLACP PoA boxes occurring.

  Conditions: This symptom is observed when removing/re-adding member links.

  Workaround: There is no workaround.

- CSCtt07525

  Symptoms: Spoke router may crash when NHRP is cleared on another spoke.

  Conditions: The symptom is observed with FlexVPN and with spoke-to-spoke tunnels.

  Workaround: There is no workaround.

- CSCtt11210

  Symptoms: Routers enrolled to hierarchical PKI on different subordinate CAs, may be unable to establish tunnels using IKEv1/IKEv2.

  The "debug crypto isakmp" debugs will show that the certificate-request payload contains the issuer-name of the subordinate CA certificate, not the subject-name as it would be expected.

  Conditions: The symptom is observed when the router does not have the Root CA certificate installed.

  Workaround: Install the Root CA certificate in a separate trustpoint on all involved routers.

- CSCtt11748

  Symptoms: RP crashes when route-map is deleted.

  Conditions: This symptom occurs when removing route-map. The match and set <default> interface NULL0 causes the crash.

  Workaround: Remove match and set clauses before removing route-map.

- CSCtt12919

  Symptoms: Invalid queueing policy is accepted.

  Conditions: This symptom is seen when a flat queueing policy is accepted, which used to be valid for FRTS.

  Workaround: There is no workaround. The policy is invalid and will never be installed.

- CSCtt15963

  Symptoms:

  1. Inline service policy Configuration: Unable to configure monitor parameters once the flow monitor is specified. See the following example:

     Router(config)#interface GigabitEthernet0/2/1 Router(config-if)#service-policy type performance-monitor inline input Router(config-if-spolicy-inline)#match access-group 110 Router(config-if-spolicy-inline)#flow monitor FM_DEF_TCP <--- After this point, all configs will print out an error message Router(config-if-spolicy-inline)#monitor parameters <----- Not accepted Router(config-spolicy-inline-mparam)#interval duration 10 <-------- Not accepted Router(config-spolicy-inline-mparam)#history 5 <------------ Not accepted

  2. Non-inline service policy: Unable to change monitor parameters once the flow monitor is bound to a policy-map and attached to an interface. See the following example:

     If an attempt is made to change monitor parameters of an already attached policy as below, it will be rejected.

UUT_451(config)#policy-map type performance-monitor VM_POLICY UUT_451(config-pmap)#class VM_CLASS UUT_451(config-pmap-c)#flow monitor VM_MONITOR UUT_451(config-pmap-c)#monitor parameters UUT_451(config-pmap-c-mparam)#history 6 <----------- Error message will show up if previous history value is different UUT_451(config-pmap-c-mparam)#interval duration 7 <----- Error message will show up if previous interval duration is different UUT_451(config-pmap-c-mparam)#react 102 mrv <-------- Error message will show up if this react was not configured before or if the subsequent command changes the threshold value of the already-configured react.

Conditions:

1. This symptom is seen when configuring an inline service policy for performance monitor on ASR platform.
2. This symptom is seen when modifying monitor parameters of a non-inline service policy for performance monitor on a Cisco ASR platform.

Workaround:

1. To configure inline service policy, always specify all monitor parameters first and put the **flow monitor** *monitor name* command as the last command in the configuration.
2. To change monitor parameters, remove the service-policy by using the **no service-policy** command, make your changes, and then reattach the service-policy.

The above configuration restrictions do not apply if the enclosing policy-map is not attached to any interface. Also the changes do not apply if you specify an “empty” flow monitor, for example a flow monitor without an enclosing valid flow record.

- CSCtt16102

  Symptoms: Tracebacks are seen after unconfiguring ACL configuration.

  Conditions: This symptom is seen when configuring an ACL and removing the configuration. Tracebacks are observed on unconfiguring the ACL.

  spoke2(config)#ip access-list standard ha_rtr > spoke2(config-std-nacl)# permit 50.0.0.0 0.255.255.255 spoke2(config)# no ip access-list standard ha_rtr % The acl is not > configured.

  Workaround: There is no workaround.

- CSCtt16487

  Symptoms: High CPU is seen when changes are made to the Cisco WCCP Access Control List (ACL).

  Conditions: This symptom is observed in a Cisco WCCP ACL.

  Workaround: There is no workaround.

- CSCtt17762

  Symptoms: Mtrace does not show the IP address of RPF interface of a multicast hop.

  Conditions: The symptom is observed on an IP PIM multicast network.

  Workaround: There is no workaround.

- CSCtt17785

  Symptoms: In the output of **show ip eigrp nei** *det*, a Cisco ASR router reports peer version for Cisco ASA devices as 0.0/0.0. Also, the Cisco ASR router does not learn any EIGRP routes redistributed on the Cisco ASA device.

Conditions: This symptom is observed only when a Cisco ASR router is running on Cisco IOS Release 15.1(3)S and the Cisco ASA device is Cisco ASA Version 8.4(2).

Workaround: Downgrade the Cisco ASR router to Cisco IOS Release 15.1(2)S.

- CSCtt17879

  Symptoms: The **bgp network backdoor** command does not have any effect.

  Conditions: This symptom occurs:

  - On 64-bit platform systems. - When the network is learned after the backdoor has been configured.

  Workaround: Unconfigure and reconfigure the network backdoor.

- CSCtt18743

  Symptoms: On a Cisco IOS ISR G2 router with CUBE feature, intermittent registration fails in P2P mode registration pass-through.

  Conditions: This symptom occurs if the CallID in the “show sip-ua registration passthrough status” is larger than a certain value.

  Workaround: Reload the Cisco IOS ISR G2 CUBE router.

- CSCtt19442

  Symptoms: Cisco 7600 subinterface that is configured for bridging after router reload sends traffic even when being shutdown. This traffic is sent from physical interface to which subinterface correspond and further received on the other side of the link.

  Conditions: This symptom is seen when bridging is configured on subinterface.

  Workaround:

  - Doing a **no shutdown**, then **shutdown** on the subinterface clears the issue. - Remove bridging configuration from subinterface.

  Deleting subinterface, and then recreating it does not fix the issue.

- CSCtt23038

  Symptoms: IOSD crashes while executing the **show flow monitor name monitor2** command after an RP downgrade on bay 0.

  Conditions: This symptom is observed during a Cisco ASR 1004 ISSU downgrade from MCPDEV to Cisco IOS XE Release 3.5.

  Workaround: There is no workaround.

- CSCtt23367

  Symptoms: The status on active PoA is A/U. The status on standby PoA is S/A.

  Conditions: This symptom is seen after HA switchover. When configuring a new mLACP port-channel on new ACTIVE RP, it may get stuck in A/U state.

  Workaround: Remove the port-channel and RG configuration and add back again.

- CSCtt24777

  Symptoms: RP crashes at be_crypto_ipsec_update_peer_path_mtu.

  Conditions: This symptom occurs when configuring the tunnel MTU.

  Workaround: There is no workaround.

- CSCtt25612

  Symptoms: The router crashes with traceback error messages and the standby takes over. After this, the router is stable.

  Conditions: There is no known trigger or changes that were made as per the user update.

  Workaround: There is no workaround.

- CSCtt26074

  Symptoms: Memory leak with IP SLAs XOS Even process.

  Conditions: The symptom is observed with IP SLA configured.

  Workaround: There is no workaround.

- CSCtt26532

  Symptoms: With QoS policy-map configured on a BFD interface, modifying the QoS policy-map flaps the BFD session.

  Conditions: This symptom is observed when BFD and QoS policy-maps are configured on the same interface.

  Workaround: There is no workaround.

  Further Problem Description: QoS and BFD use a common flag that gets reset and set during QoS policy-map update, causing the BFD session to flap. BFD session flap leads to the OSPF session also going down.

- CSCtt26643

  Symptoms: A Cisco ASR 1006 router running Cisco IOS Release 15.1(2)S2 or Cisco IOS Release 15.1(3)S0a crashes with Signal 11.

  Conditions: This symptom is observed on a Cisco ASR 1006 router running the asr1000rp1-adventerprisek9.03.04.00a.S.151-3.S0a.bin image. The **show version** command causes the “Last reload reason: Critical software exception” error.

  Workaround: There is no workaround.

- CSCtt28703

  Symptoms: VPN client with RSA-SIG can access a profile where his CA trustpoint is not anchored.

  Conditions: This symptom is seen with the use of RSA-SIG.

  Workaround: Restrict access by using a certificate-map matching the right issuer.

- CSCtt29615

  Symptoms: Any CLI command issued under af-interface mode in EIGRP router may lead to router crash.

  Conditions: This problem is observed in a Cisco router that is running Cisco IOS Release 15.2(1)S.

  Workaround: There is no workaround.

- CSCtt30212

  Symptoms: IP SLA CFM Probes over PW fail.

  Conditions: This symptom occurs when ECMP exists towards the core.

  Workaround: Do not have ECMP.

- CSCtt31634

  Symptoms: Traffic drops.

Conditions: This symptom occurs when the hw-module reloads the IM on active and posts which switchover is performed.

Workaround: After switchover, use the **hw-module subslot reload** command to recover from the problematic state, and traffic will resume.

- CSCtt32165

  Symptoms: The Cisco Unified Border Element Enterprise on the Cisco ASR 1000 series router can fail a call with cause 47 immediately after the call connects.

  Conditions: This symptom is observed with a sufficient call volume and a call flow that redirects many calls. The Cisco ASR router can fail to provision the forwarding plane for the new call due a race condition where a prior call is not completely cleaned up on the forwarding plane before trying to use the same structure again.

  The **show voice fpi stats** command output indicates that a failure has occurred if the last column is greater than zero. For example:

  show voip fpi stats | include provisn rsp

  provisn rsp 0 32790 15

  Workaround: There is no workaround. However, Cisco IOS Release 3.4.1 is less impacted by these call failures due to a resolution of defect CSCts20058. Upgrade to Cisco IOS Release 3.4.1 until such time as this defect is resolved. In a fully redundant Cisco ASR 1006 router, you can failover the ESP slots to clear the hung entries in the forwarding plane. Other platforms will require a reload.

- CSCtt33158

  Symptoms: If WRED is already present and the queue limit is configured in packets then WRED thresholds become 0.

  Conditions: Use the below mentioned config to repro the problem.

  policy-map parent class class-default shape aver 2000 service-policy child

  policy-map child class class-default random-detect

  int g0/0/0 service-policy out parent

  policy-map child class class-default queue-limit 2000

  Workaround: Remove WRED and reattach it.

- CSCtt35379

  Cisco IOS Software contains a vulnerability in the Border Gateway Protocol (BGP) routing protocol feature.

  The vulnerability can be triggered when the router receives a malformed attribute from a peer on an existing BGP session.

  Successful exploitation of this vulnerability can cause all BGP sessions to reset. Repeated exploitation may result in an inability to route packets to BGP neighbors during reconvergence times.

  Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability. This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-bgp

- CSCtt35936

  Symptoms: EIGRP route updates are not sent to DMVPN spokes. The **show ip eigrp inter** command output shows pending routes in interface Q, which remains constant. The **show ip eigrp int deta** command output shows that the next sequence number of the interface remains the same (does not advance).

  Conditions: This symptom occurs when EIGRP session flapped, resulting in routes being withdrawn and restored.

  Workaround: Add a static route on any spoke that kicks out EIGRP learned routes from the RIB table; this will again kick the interface on the HUB.

- CSCtt36513

  Symptoms: Crash seen on a Cisco ASR for the process IPSec key engine.

  Conditions: The symptom is observed when you have more than 4K sessions up on the ASR.

  Workaround: There is no workaround.

- CSCtt36757

  Symptoms: The following error message is noticed when configuring QoS on the interface of an ES+ card:

  %X40G_QOS-DFC9-3-CFN: qos tcam programming failed for policymap
  AGGR-CHA-INTERFACE-OUTPUT-POLICY

  Conditions: The symptom is observed after a misconfiguration in the interface. The interface was misconfigured as switchport which removed the QoS configuration from the interface configuration but not from the line card. After the interface was configured back to an L3 port, the issue started occurring when the same policy was reapplied.

  Workaround: A new policy can be applied but the required policy cannot be applied again.

- CSCtt37516

  Symptoms: Line card crash with priority traffic when QoS policy is applied.

  Conditions: The symptom is observed with the QoS priority feature.

  Workaround: There is no workaround.

- CSCtt39944

  Symptoms: The **show mls cef adjacency usage** is not showing the adjacency count correctly.

  Conditions: The symptom is observed in highly scaled networks. The platform code is not counting the last non-stats region allocation for adjacency usage.

  Workaround: There is no workaround.

- CSCtt43552

  Symptoms: A Cisco router reloads with the **warm-reboot** command.

  Conditions: This symptom is observed on the Cisco router while running Cisco IOS Release 15.2(2.2)T.

  Workaround: There is no workaround. Remove CLI “warm-reboot” from configuration (router will not be able to use warm reboot feature)

- CSCtt43834

  Symptoms: Netflow counter gets incremented when sending SSM group range as v2.

  Conditions: The symptom is observed when doing an SSO.

Workaround: There is no workaround.

- CSCtt43843

  Symptoms: After reloading aggregator, PPPoE recovery is not occurring even after unshutting the dialer interface.

  Conditions: This symptom is occurring with a Cisco 7200 platform that is loaded with the Cisco IOS Interim Release 15.2(1.14)T0.1 image.

  Workaround: There is no workaround.

- CSCtt45536

  Symptoms: "FlowVar- Chunk malloc failed" messages are seen and this may be accompanied by slow console response.

  Conditions: The symptom is observed when a mix of IPv4 and IPv6 traffic is going through the router configured with QoS, VM, etc.

  Workaround: There is no workaround.

- CSCtt45654

  Symptoms: In a DVTI IPSec + NAT-t scaling case, when doing session flapping continually, several Virtual-Access interfaces are "protocol down" and are not deleted.

  Conditions: This symptom can be observed in a DVTI IPSec + NAT-t scenario when session flapping is done in the spoke side.

  Workaround: There is no workaround.

- CSCtt46638

  Symptoms: A Cisco 7604 running Cisco IOS Release 12.2(33)SRE4/SRE5 crashes when changing the tunnel source and destination of an IPsec sVTI.

  Conditions: The symptom is observed once the IPsec session is up and traffic is flowing through. If the tunnel source or destination is changed, the router crashes. This does not occur with a plain GRE tunnel.

  Workaround: There is no workaround.

- CSCtt46730

  Symptoms: Platform crashes during IKEv2 negotiation between the spoke and the hub with Cisco TrustSec (CTS) enabled on the Cisco 3945E platform.

  Conditions: This symptom is seen with re-negotiation of IKEv2 SA between the peers.

  Workaround: There is no workaround.

- CSCtt46873

  Symptoms: In an MVPN setup, when the **mdt default** command is removed from under the VRF, unicast packets coming from the core, such as LDP and BGP, get dropped, leading to router isolation.

  Conditions: This issue is primarily seen when mls mpls tunnel-recir is not configured on the box (or does not get enabled due to the absence of a sip10g device). In such a case, MDT tunnel VLAN gets allocated, but is never released, until the **mdt default** command is removed. Since the decap adjacency handling the unicast packets is a GRE decap, with an MDT tunnel VLAN allocated, removal/re-add of **mdt default** command will program the adjacency with the MDT tunnel VLAN. Another removal along with a race condition might leave the adjacency with the tunnel VLAN (now deallocated), thereby causing the unicast packets to be dropped.

Workaround: Configure mls mpls tunnel-recir on the box and remove/re-add the **mdt default** command or reload with mls mpls tunnel-recir configured to be safe.

- CSCtt70585

  Symptoms: IPv6 traffic is not flowing.

  Conditions: This symptom is seen with IPSec v6 tunnels.

  Workaround: There is no workaround.

- CSCtt90672

  Symptoms: CFM MEP enters the INACTIVE state on deleting the subinterface.

  Conditions: This symptom is observed under the following conditions:

  1. Create a subinterface (vlan 104) for EOAM communication. Check "CC-Status" = Enabled.
  2. Create a QinQ subinterface (vlan tags: 104 128) for subscriber on the same physical interface. Check "CC-Status" = Enabled.
  3. Later, delete the QinQ subinterface from the step 2 above (DT's provisioning system does it, for example, for a new policy change). The "CC-Status" goes to inactive.

  Workaround: Unconfigure and reconfigure the **continuity check** command under the corresponding Ethernet CFM domain/service global configuration for this CFM MEP.

- CSCtt98823

  Symptoms: Clock quality is bad from Cisco ME 3600X and Cisco ME 3800X.

  Conditions: This symptom is seen with normal network clock configurations.

  Workaround: There is no workaround.

- CSCtt99101

  Symptoms: Management port stops responding due to O/P queue wedge 40/40.

  Conditions: This issue is seen after 4-5 days when the box is up, and traffic is passing via management port.

  Workaround: Reload the box.

- CSCtu00699

  Symptoms: On a DMVPN hub router, the IOS processor memory pool can get fragmented due to memory allocated for "Crypto NAS Port ID".

  Conditions: This happens when there is network instability potentially causing tunnels to flap frequently.

  Workaround: There is no workaround.

- CSCtu01172

  Symptoms: The Cisco ASR 1000 series router without an actual redundant router may crash when configured for CUBE HA based on the document "Cisco Unified Border Element High Availability (HA) on ASR platform Configuration Example."

  Conditions: This symptom is observed with the Cisco ASR 1000 series router.

  Workaround: Remove the application configuration, that is, "no application redundancy".

- CSCtu02286

  Symptoms: With pim-bidir in MVPN core, MVPN traffic might not flow if a PE is also a rendezvous point (RP) for the pim-bidir in core.

Conditions: This symptom occurs with pim-bidir in MVPN core.

Workaround: Use non pim-bidir modes.

- CSCtu06894

  Symptoms: Cisco UBE crashes when the **show sip-ua calls** command is executed while there is an active SIP call through system.

  Conditions: This symptom is present on Cisco 2821 routers. The router crashes only when Cisco UBE receives an SDP length greater than 9000 bytes as part of a SIP message. And at the same time, if the show command is executed, the crash occurs. Otherwise, the crash is not seen.

  Workaround: There is no workaround.

- CSCtu07626

  Symptoms: Router processing SIP traffic crashes.

  Conditions: The following error may be seen prior to the crash:

  %SDP-3-SDP_PTR_ERROR: Received invalid SDP pointer from application. Unable to process.

  Workaround: There is no workaround.

- CSCtu08608

  Symptoms: The standby RP crashes due to VoIP HA Session App.

  Conditions: The Cisco ASR 1000 platform with redundant RPs and Cisco Unified Border Element Enterprise. The signature in the crashinfo is as follows:

  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = Voip HA Session App

  Workaround: There is no workaround.

- CSCtu11677

  Symptoms: A Cisco router may unexpectedly reload due to bus error or segV exception or generate a spurious error when the cSipStatsSuccessOkTable snmp object is polled.

  Conditions: This is seen on a voice gateway when the cSipStatsSuccessOkTable snmp object is polled.

  Workaround: Create an SNMP view and then block the oid for cSipStatsSuccessOkTable and then apply it to all SNMP communities on the device:

  snmp-server view blockmib iso include snmp-server view blockmib 1.3.6.1.4.1.9.9.152.1.2.2.5 exclude

  and then apply it to the community:

  snmp-server community <community> view blockmib ro

- CSCtu12574

  Symptoms: The **show buffers** command output displays:

  1) Increased missed counters on EOBC buffers. 2) Medium buffer leak.

  Router#sh buffers Buffer elements: 779 in free list (500 max allowed) 1582067902 hits, 0 misses, 619 created

  Interface buffer pools: .... Medium buffers, 256 bytes (total 89647, permanent 3000, peak 89647 @ 00:01:17): 273 in free list (64 min, 3000 max allowed)

  EOBC0/0 buffers, 1524 bytes (total 2400, permanent 2400): 0 in free list (0 min, 2400 max allowed) 2400 hits, 161836 fallbacks 1200 max cache size, 129 in cache ....

The leak is small. It is a leak of 64 bytes per buffer that is leaked, and the leak appears to be very slow.

Conditions: The **show buffers old** command output displays some buffers hanging on the EOBC buffers list for a really long time, such as weeks or even more. This issue is a corner case and the buffer leak rate is slow.

This DDTS tracks the leak specific to IPC application l3-mgr.

From the **show buffers old pack** output: 0A9C4ED8: 00200000 02150000 0202080B 01000000 . ... --> IPC Header 0A9C4EE8: 97D49493 00081608 03493E4D 06927C9A .T.......I>M..|. 0A9C4EF8: 00520002 00000000 00000000 000000 .R............ --> ICC Header -- --

And, if we look at the ICC header at the underscored items 00520002:

0052 (represents the class name) ----> L3_MGR_DSS_REQUESTS 0002 (represents the request name) ----> L3_MGR_MLS_REQ

Workaround: Reload the system.

- CSCtu13232

  Symptoms: Standby crash is observed on doing runversion between Cisco IOS Releases XE3.4.1 and XE3.6.

  Conditions: No special configurations are needed to reproduce.

  Workaround: There is no workaround.

- CSCtu14461

  Symptoms: Y.1731PM DMM probe cannot be successfully scheduled.

  Conditions: This symptom occurs on a Cisco ME 3800X platform. When a user schedules a Y.1731PM DMM probe on UP MEP with the core facing interface as switchport, statistics are not collected.

  Workaround: There is no workaround.

- CSCtu14878

  Symptoms: In unknown circumstances, when ECMP paths are created between a Cisco ME 3800 VPNv4 Pre-Agg router and a Cisco ASR 9000 3107 ABR router (through HA failures or intentional configuration), the ME 3800 will blackhole all VPNv4 traffic.

  Conditions: The symptom is observed with the following conditions:

  - Running IGP to 3107 ABR router.
  - Running labelled BGP to reach far end destination and to provide VPN labels.
  - Have ECMP paths from Cisco ME 3800 to Cisco ASR 9000 ABR router as shown from “show ip cef vrf vrfname prefix mask det”.

  Workaround: There is no workaround.

- CSCtu17006

  Symptoms: Mediatrace is not working because RSVP fails to select the output interface.

  Conditions: This symptom is observed only with PFR configuration.

  Workaround: Remove the PFR configuration.

- CSCtu18201

  Symptoms: A Cisco router crashes due to low stack with the following display:

  %SYS-6-STACKLOW: Stack for process BGP Event running low, 0/6000

Conditions: This symptom occurs with a low stack.

Workaround: There is no workaround.

- CSCtu18786

  Symptoms: Device may crash showing "VoIP" error messages. Decodes point to voice functions.

  Conditions: The symptom is observed when SIP is enabled on the device.

  Workaround: There is no workaround.

- CSCtu19450

  Symptoms: A system that is running Cisco IOS may reload when a large number of routes are simultaneously deleted at the same time that the inetCidrRouteTable is being walked.

  Conditions: This symptom is only likely to happen when there are large numbers of interfaces and routes within the system, and when large numbers of routes are being rapidly removed, and the system is loaded, at the same time that the inetCidrRouteTable is being walked.

  Routes may be deleted from the system both directly, and also indirectly for example, when a significant number of PPPoE sessions are removed.

  Workaround: Avoid walking the inetCidrRouteTable while significant numbers of routes are being removed from the routing system.

- CSCtu21967

  Symptoms: A router configured to be an IP voice gateway may crash.

  Conditions: The exact conditions for this crash are currently unknown.

  Workaround: There is no workaround.

- CSCtu22952

  Symptoms: Traffic stops forwarding suddenly when a port channel has an EVC configuration.

  Conditions: The symptom is observed when you have a port-channel interface with multiple member links on an LACP configured via EVC. By sending single source-destination traffic, it moves from one member link to another.

  Workarounds: Configure bridge-domain under the EVC and:

  1. Use etherchannel in FEC mode (mode ON) instead of LACP; or
  2. Remove EVC.

- CSCtu25150

  Symptoms: A Cisco router acting as a voice gateway may unexpectedly reload due to a SegV exception or bus error, or may experience a spurious access.

  Conditions: The exact conditions leading to the crash are not known. The issue is only present in Cisco IOS Release 15.1(4)M and later.

  Workaround: There is no workaround.

- CSCtu28990

  Symptoms: RP crash is observed at SYS-6-STACKLOW: Stack for process XDR Mcast.

  Conditions: This symptom is observed when performing shut/no shut on interfaces on a configuration-rich system.

  Workaround: There is no workaround.

- CSCtu29729

  Symptoms: An attempt to create a frame-relay sub-interface on a serial interface may result in error. The serial interface can then not be configured as a frame-relay interface.

  Conditions: This symptom is observed when a serial interface is configured as a multi-link frame-relay bundle link with a subsequent attempt to change the configuration to a frame-relay interface.

  Workaround: There is no workaround.

- CSCtu29815

  Symptoms: If the CCM sub is restarted before the switchover from PUB to SUB, the MGCP GW needs at least 10 minutes to finish the switchover.

  Conditions: The symptom is observed under the following conditions:

  - MGCP GWx1. - Version: c2800nm-spservicesk9-mz.151-3.T.bin. - CUCM: version 8.6.1x2. - Primary CCMPUB and CCMSUB.

  Workaround: Restart the MGCP process from the gateway by using **no mgcp** and **mgcp**.

  Further Problem Description: When the CCMSUB's service is down (or machine is powered off), CM service sends a TCP FIN to MGCPGW, however from the debug of MGCPGW, the backhaul link between CCMSUB does not refresh as the TCP layer is stuck at CLOSEWAIT. It is confirmed that the MGCP GW is not notified about this at all, or the MGCP GW does not actively check the status the backup backhaul link.

  Then CCMSUB's started/powered on/recovered, however the CCMPUB is down/powered off this time. MGCP application itself will failover immediately, so does the backhaul link. However as the backhaul link's status was not updated as the TCP layer is still in CLOSEWAIT, the backhaul link is in a false OPEN status and CCM will not be able to leverage this gateway to make outbound calls and all incoming calls are being impacted as well.

- CSCtu30649

  Symptoms: Standby is reset.

  Conditions: This issue is seen when the ISSU standby is reset because of MCL failure.

  Workaround: There is no workaround.

- CSCtu31659

  Symptoms: Cisco ME-3600X series switch running Cisco IOS Release 12.2(52)EY2 and/or Release 15.1(2)EY will crash when the **diagnostic start test all** command is entered.

  Conditions: The symptom is observed with no specific configuration. The switch will crash with an empty configuration.

  Workaround: Avoid running the **diagnostic start test all** command.

- CSCtu32929

  Symptoms: DMVPN tunnel is failing to come up with Cisco TrustSec functionality enabled. NHRP is failing.

  Conditions: The symptom is observed when IKEv2 security association is up and NHRP negotiation fails to bring up the DMVPN tunnel.

  Workaround: Disable TrustSec CLI (with **crypto ikev2 cts sgt**).

- CSCtu33956

  Symptoms: The dialer with PPP encapsulation is seen when DSL is the WAN interface. L2PT does not work.

Conditions: This symptom is observed under the following conditions:

- The PPPoE dialer client needs to be configured on the physical SHDSL interface.
- The GRE tunnel destination interface should point to the dialer interface.
- The MPLS pseudowire should go over the tunnel interface.
- After the PPPoE session is set up, the GRE tunnel traffic gets dropped at the peer end of the PPPoE session.

Workaround: There is no workaround.

- CSCtu34207

  Symptoms: CoA for SessProv request timeout from ISG to SCE.

  Conditions: Issue is seen after an upgrade to Cisco IOS 15.1S train (seen in Cisco IOS Release 15.1(2)S1 too).

  Workaround: There is no workaround.

  Further Problem Description: The packet is seen in the TCPDUMP on the SCE. Cisco IOS Release 12.2(33)XNF2 does not show the issue. SCE shows in the debug:

  bad authentication validate failed

- CSCtu35116

  Symptoms: VPDN session keeps on trying to come up with MPLS MTU higher than 1500.

  Conditions: The symptom is observed when you upgrade a Cisco 7200VXR from the c7200-a3jk91s-mz.122-31.SB18 to the c7200-adventerprisek9-mz.122-33.SRE4 image.

  Workaround: There is no workaround.

- CSCtu35713

  Symptoms: IPv4 address saving: IPCP state change does not trigger session accounting update.

  Conditions: This symptom is observed under the following conditions:

  1. Enable IPv4 address saving on BRAS.
  2. Configure AAA periodic accounting using the **aaa accounting update periodic** *time in mins* command.
  3. Initiate IPCP negotiation from the client.
  4. After IPCP negotiation is complete, BRAS does not send an interim accounting update containing IPv4 address save VSA and the new IPv4 address assigned to the client.

  Workaround: Configure AAA accounting with the **aaa accounting update newinfo periodic** *time in mins*.

- CSCtu35933

  Symptoms: L2 multicast groups stop being forwarded across EVC with IGMP snooping enabled.

  Conditions: The symptom is observed with a lot of IGMP activity. It occurs after a long time.

  Workaround: There is no workaround.

- CSCtu36562

  Symptoms: cikeFailureReason and cipsecFailureReason from CISCO-IPSEC-FLOW- MONITOR MIB do not report the proper failure reasons for failed IKE negotiations (ph1 or ph2).

  Conditions: The symptom is observed with failed IKE negotiations (ph1 or ph2).

  Workaround: There is no workaround.

- CSCtu36674

  Symptoms: Packets stop being transmitted in the output direction on L2transport local connect PVC on the ATM interface.

  Conditions: This symptom is observed when local connect is configured and a new ATM subinterface is configured on the same ATM main interface as the one with local connect PVC.

  Workaround 1: Perform shut/no shut on local connect.

  Workaround 2: Unconfigure/reconfigure local connect.

- CSCtu38244

  Symptoms: After bootup, the GM cannot register and is stuck in "registering" state. Issuing the **clear crypto gdoi** command is required for a successful registration to the keyserver.

  Conditions: The symptom is observed upon router bootup.

  Workaround: Either do a **clear crypto gdoi** after a reload, or configure a second keyserver entry. This does not have to be an existing keyserver, it can be just a dummy address.

- CSCtu39819

  Symptoms: The Cisco ASR 1002 router configured as an RSVPAgent for Cisco Unified Communication Manager crashes under extended traffic.

  Conditions: This symptom is observed on a Cisco ASR 1002 router configured as an RSVPAgent for CUCM End-to-End RSVP feature. The router crashes after 45 minutes of traffic run with 150 simultaneous up MTP-RSVP sessions.

  The image used is "asr1000rp1-adventerprisek9.03.04.00a.S.151-3.S0a.bin".

  Workaround: There is no workaround.

- CSCtu41137

  Symptoms: IOSD Core@fib_table_find_exact_match is seen while unconfiguring tunnel interface.

  Conditions: The core is observed while doing unconfiguration.

  Workaround: There is no workaround.

- CSCtu43731

  Symptoms: On an RP1, RP switchover causes an RP reset.

  Conditions: This symptom is observed with RP switchover under the following conditions:

  - The router must be an RP1 - The configuration of Flexible NetFlow (FNF) or equivalent must be applied to 4000 or more interfaces. In this case of testing, 4000 DVTI interfaces were in use.

  An equivalent of FNF is AVC or passive Video Monitoring. That is, those configured on a comparable number of interfaces will have the same effect.

  Workaround 1: Prior to doing a controlled switchover, such as ISSU, deconfigure FNF from some interfaces to take it well under the threshold at which the issue can occur.

  Workaround 2: Do not enable FNF monitoring.

- CSCtu51904

  Symptoms: You can observe decrementing free memory by each repetition of the process by using the **show memory statistics** command under the active SP.

  Conditions: The symptom is observed by removing "default mdt" under the VRF configuration and then adding it back. The memory leak is recognized on the active SP.

  Workaround: Reload the router.

- CSCtu60863

  Symptoms: IGMP reports do not get installed in the IGMP group list.

  Conditions: The symptom is observed when the port-security feature is enabled on the switchport which is part of the VLAN on which the IGMP reports are received.

  Workaround: Remove "switchport port-security" from ports associated with the VLAN on which the IGMP reports are received.

- CSCtu89771

  Symptoms: The Cisco ASR 1000 series router RP crashes while unconfiguring or removing the **no area 0 authentication ipsec spi <>** command.

  This behavior is not observed at the first few instances of unconfiguring the above CLI.

  Conditions: This symptom is observed only in automated tests where unconfiguring the authentication with the above CLI is executed multiple (approximately 3) times on the Cisco ASR 1000 series router. This leads to the RP crashes.

  Workaround: There is no workaround.

- CSCtu92213

  Symptoms: Console is stuck and irresponsive.

  Conditions: This symptom is seen when EVC with QoS is scaled, and traffic is being sent through many policy-maps with a large queue limit.

  Workaround: Configure a smaller queue-limit under each class on all egress policy-maps in use.

- CSCtu92289

  Symptoms: VCCV BFD on PW HE (routed pseudowire) is not working.

  Conditions: VCCV BFD is not working on routed pseudowire but works fine on scalable EoMPLS.

  Workaround: There is no workaround.

- CSCtu92673

  Symptoms: L2TP tunnels are not getting established with PPPoE relay.

  Conditions: This issue is seen on a Cisco 7200 router that is running Cisco IOS Interim Release 15.2(01.12)S.

  Workaround: There is no workaround.

- CSCtv19529

  Symptoms: Router crashes on unconfiguring the last available DHCP pool. Crash will also be seen on running the **no service dhcp**.

  Conditions: This crash can happen only if "DHCP Client" process is running on the router along with the DHCP relay processes (DHCPD Receive, DHCPD Timer, DHCPD Database).

  The client process can be started:

  1. from an DHCP autoinstall attempt during router startup (with no nvram config).
  2. if the **ip address dhcp** is run on one of the interfaces.
  3. if the router was used for DHCP proxy client operations.

  The relay processes are started when a DHCP pool is created by the **ip dhcp pool** *pool* command.

  Workaround: Have a dummy DHCP pool created using the **ip dhcp pool** *dummy_pool* command, and never delete this pool. Other pools can be created and removed at will, the *dummy_pool* should not be removed. In addition, do not execute the **no service dhcp** command.

- CSCtv21900

  Symptoms: Intermittent one-way audio occurs from an MGCP gateway to a Cisco IP phone.

  Conditions: This symptom is observed under the following conditions:

  - Encrypted call with SRTP
  - MGCP Controlled Gateway
  - Cisco IOS Release 15.1(4)M or later releases

  Phone logs show the following message:

  6622: DBG 23:29:50.256330 DSP: RTP RX: srtp_unprotect() again 6623: DBG 23:29:50.257139 DSP: RTP RX: srtp_unprotect() failed with error code 7 6624: DBG 23:29:50.276390 DSP: RTP RX: srtp_unprotect() failed with auth func 3

  The “Rcvr Lost Packet” counter on the Cisco IP phone begins to increment as soon as the call connects.

  Workaround 1: Downgrade the software to Cisco IOS Release 15.1(3)T or earlier releases.

  Workaround 2: Perform a hold/resume on the one-way audio call. This mitigates the problem.

- CSCtw43640

  Symptoms: An IP ping/CFM session through Handoff FPGA fails.

  Conditions: This symptom is observed after switchover with IM in slot 5.

  Workaround: There is no workaround.

- CSCtw45055

  Symptom: A Cisco ASR router may experience a crash in the BGP Scheduler due to a segmentation fault if BGP dynamic neighbors have been recently deleted due to link flap. For example:

  Nov 10 08:09:00.238: %BGP-5-ADJCHANGE: neighbor *X.X.X.X Up Nov 10 08:10:20.944: %BGP-3-NOTIFICATION: received from neighbor *X.X.X.X (hold time expired) x bytes Nov 10 08:10:20.944: %BGP-5-ADJCHANGE: neighbor *X.X.X.X Down BGP Notification received Nov 10 08:10:20.945: %BGP_SESSION-5-ADJCHANGE: neighbor *X.X.X.X IPv4 Unicast topology base removed from session Neighbor deleted Nov 10 08:10:34.328: %BGP_SESSION-5-ADJCHANGE: neighbor *X.X.X.X IPv4 Unicast topology base removed from session Neighbor deleted Nov 10 08:10:51.816: %BGP-5-ADJCHANGE: neighbor *X.X.X.X Up

  Exception to IOS Thread: Frame pointer 0x3BE784F8, PC = 0x104109AC

  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = BGP Scheduler

  The scheduler process will attempt to reference a freed data structure, causing the system to crash.

  Conditions: This symptom is observed when the Cisco ASR router experiences recent dynamic neighbor removals, either because of flapping or potentially by manual removal. This issue only happens when BGP dynamic neighbor is configured.

  Workaround: There is no workaround.

- CSCtw45168

  Symptoms: DTMF interworking fails when MTP is used to convert OOB---RFC2833 and vice versa.

  Conditions: This symptom is observed when MTP is used to convert OOB---RFC2833 and vice versa. This issue is seen starting from Cisco IOS XE Release 3.2S. Cisco IOS XE Release 3.1S should work fine.

  Workaround: There is no workaround.

- CSCtw45592

  Symptoms: The **ntp server** *DNS-name* command is not synced to the standby. When the **no ntp server** *hostname* command is issued later on the active, the standby reloads because the config was not added.

  Conditions: When the device is reloaded or when the DNS name is not resolved, the config is not added. After the standby SYNC failure, then issuing the **no ntp server** *hostname*.

  Workaround: Use the IP/IPv6 addresses instead of the hostname for NTP configurations.

- CSCtw46625

  Symptoms: The QL value is DNU although the four least significant bits of SSM S1 byte are pointing to PRC (bits: 0010).

  Conditions: This symptom is observed when SSM S1 byte is received on CEoPs SPAs or channelized SPA-1XCHSTM1/OC3.

  Workaround: Force the QL PRC value by executing the following command:

  network-clock quality-level rx QL-PRC controller SONET 1/2/0

- CSCtw48209

  Symptoms: High-end Cisco devices running Cisco IOS are likely affected. Active features at the time of this problem manifestation include any condition that leads to RSVP SNMP notification generation in Cisco IOS. BGP/MPLS TE instability, leading to changes to RSVP session status change, is observed in a test scenario while running Cisco IOS Release SXI4 and Cisco IOS Release SXI7. The issue is not reproducible consistently.

  Conditions: This symptom is observed with Cisco IOS Release 12.2(33)SXI4, Cisco IOS Release 12.2(33)SXI7, Cisco IOS Release 12.2SR, Cisco IOS Release 12.2SX, and Cisco IOS Release 15S.

  Workaround: Disable RSVP notification using the **no snmp-server enable traps rsvp** command.

- CSCtw50141

  Symptoms: Incremental leaks at __be_ber_get_stringa pointing to LDAP process.

  Conditions: The symptom is observed when NTLM authentication is being used with an LDAP server and with the router acting as the NTLM proxy.

  Workaround: There is no workaround.

- CSCtw50277

  Symptoms: Policy manager is getting apply config failed on standby while policy is activated through CoA. The router later crashes in policy code.

  Conditions: This symptom is seen when CoA activated policy install is failing on standby RP.

  Workaround: There is no workaround.

- CSCtw50941

  Symptoms: Crash occurs when trying to modify the class-map configuration of the SG aware firewall (using “match security-group”).

  Conditions: The symptom is observed with class-map configuration changes made on security-group class filters.

  Workaround: Do not attach the “match security-group” filter or modify the class-map with this filter.

- CSCtw51134

  Symptoms: IMA interface configuration is lost post stateful switchover (SSO).

  Conditions: This symptom occurs after SSO.

Workaround: There is no workaround.

- CSCtw52097

  Symptoms: RG is stuck in STANDBY COLD-BULK state when the RG state is trying to restore to its appropriate state after a failover.

  Conditions: The symptom is observed when HA pairs are in an Active-Active scenario and control interfaces are using subinterfaces.

  Workaround: There is no workaround.

- CSCtw52610

  Symptoms: Some of the TCes will switch to fallback interface, and the remaining TCes on primary interface will be in OOP state.

  Conditions: The issue is seen when primary link is considered OOP based on utilization despite using the **no resolve utilization** command.

  Workaround: There is no workaround if PfR policy with and without utilization is needed. If PfR policy based on utilization is not needed, then configure "max-xmit-utilization percentage 100".

- CSCtw53767

  Symptoms: ZBFW HA configured with A/R and QoS fails for asymmetric traffic.

  Conditions: The symptom is observed when ZBFW HA and QoS are configured together.

  Workaround: There is no workaround.

- CSCtw56439

  Symptoms: The **ip mtu** command that is configured on an IPsec tunnel disappears after a router reload.

  Conditions: The symptom is observed with IPsec and the **ip mtu** over a tunnel interface.

  Workaround: There is no workaround.

- CSCtw58586

  Symptoms: IKEv2 CLI configuration currently requires to manually link the crypto IKEv2 profile default to the crypto IPSec profile default. This enhancement request will change the behavior and create an automatic anchorage.

  Conditions: This symptom is seen in IKEv2 usage.

  Workaround: There is no workaround.

- CSCtw60333

  Symptoms: HTTP process hangs. This impacts the webauth authentication scaling factor.

  Conditions: The symptom is observed when the **clear ldap server** *server-name* command issued or the connection is closed during any outstanding LDAP. Transactions are in progress or are waiting for an LDAP response from the LDAP server.

  Note: it is not only related to the secure-server. It is also applicable with an IP HTTP server. So generally it is applicable if you are using webauth with LDAP as the authentication server.

  Workaround: Do not issue **clear ldap server** when any LDAP transactions for web authentication are in progress.

- CSCtw61872

  Symptoms: The router will crash when executing a complex sort on the flexible netflow cache from multiple CLI sessions.

Conditions: The symptom is observed when executing a complex sort with top- talkers on a show command from multiple CLI sessions (note that normal show commands without top-talkers are fine):

sh flow monitor QoS_Monitor cache sort highest counter packets top 1000 sh flow monitor QoS_Monitor cache sort highest counter packets top 10000

Workaround: Do not execute complex sorts with top-talkers on the show output from multiple CLI sessions.

- CSCtw62310

  Symptoms: The **cells** keyword is added to "random-detect" whenever a policy-map is removed from an interface/map-class via "no service- policy".

  Conditions: The symptom is observed when removing the policy-map from map- class.

  Workaround: There is no workaround.

  Further Problem Description: The CLI is technically valid if it has been manually configured as "cells" prior to the removal. The issue is that the template policy is being changed automatically to "cells" whenever the removal happens, regardless of what the original configuration was, and that is not the expected behavior.

- CSCtw62858

  Symptoms: Cell payload scrambling is off by default for ATM DS1 interfaces on SPA-1CHOC3-CE-ATM.

  Conditions: The symptom is observed when you are using ATM or IMA DS1 T1 or E1 on any of these:

  - SPA-1CHOC3-CE-ATM (ATM DS1, ATM E1, ATM IMA DS1, ATM IMA E1). - SPA-2CHT3-CE-ATM (ATM DS3, ATM E3). - SPA-24CHT1-CE-ATM (ATM DS1, ATM E1, ATM IMA DS1, ATM IMA E1).

  Workaround: There is no workaround.

  Further Problem Description: Currently, cell payload scrambling is off by default for ATM DS1 interfaces on SPA-1CHOC3-CE-ATM and on for E1 interfaces. Cell payload scrambling is currently not configurable. This presents a problem when connecting to ATM copper T1 CPEs that require cell payload scrambling or when connecting to E1s devices that do not support cell payload scrambling.

- CSCtw66863

  Symptoms: A Cisco router may crash when using VXML script with Cisco proprietary tag *Cisco-data*.

  Conditions: This symptom is observed when the *Cisco-data* tag uses memory beyond allocated, which causes router to crash intermittently.

  Workaround: There is no workaround.

- CSCtw68745

  Symptoms: A Cisco ASR 1000 router acting as DHPCv6 Relay standby crashes when there is high DHCPv6 incoming traffic and if DHCPv6 relay is configured on many (around 5k) interfaces.

  Conditions: This symptom occurs when there is high DHCPv6 incoming traffic and if DHCPv6 relay is configured on many (around 5k) interfaces.

  Workaround: There is no workaround.

- CSCtw72260

  Symptoms: Traffic flow is not learned.

  Conditions: The symptom is observed with a Cisco 7600 with line card and performance-traffic policy-map. Using IP-CBR, MDI, or RTP metric. Does not impact Cisco ASR 1000.

  Workaround: Do an OIR/reload.

- CSCtw72708

  Symptoms: Malloc failure, CPU hog, and memory leaks are seen creating the MD entry with your own IP address as the next-hop listener.

  Conditions: Issue is seen on a Cisco 7600 series router that is running Cisco IOS 15.2(04)S version. There are two triggers:

  1. When LI is configured on the Cisco 7600 with the remote's MDip as one of your own; resulting in CPU hog and memory failures.
  2. When one generic stream is deleted, an internal counter is decremented twice. Thus disabling the LI feature even when there is another active tap installed.

  Workaround: Configure the MD listener IP address with the correct IP address.

- CSCtw74099

  Symptoms: A Cisco ME 3600 may crash if the Ethernet Controller (eTSEC) tx ring is hung.

  Conditions: The symptom is observed if the management port is up.

  Workaround: Shut down the management port.

- CSCtw78064

  Symptoms: The **display-logout** message on a Cisco SCCP Phone is not cleared even after pressing other buttons on the phone.

  Conditions: This symptom is observed on the Cisco SCCP phone (also known as Skinny Phone or ePhone) when the last extension mobility (EM) user in a hunt group logs out using the HLog button. This symptom is observed even if the last EM user logs out of the hunt group and logs back in.

  Workaround: There is no workaround.

- CSCtw79488

  Symptoms: Multicast is not forwarded out on EVC.

  Conditions: This has been observed with Cisco IOS Release 15.1(2)EY and EY1a and with the following configuration:

  interface GigabitEthernetx/y switchport trunk allowed vlan none switchport mode trunk

  service instance <> ethernet encapsulation dot1q <VLAN-1> l2protocol tunnel bridge-domain <BD> ! !

  ! interface Vlan<BD> no ip address xconnect <IP> <VC-ID> encapsulation mpls !

  Workaround: Configure any dummy IP address on interface VLAN. It does not need to be in the same segment:

  ! interface Vlan<BD> ip address A.B.C.D M.M.M.M xconnect <IP> <VC-ID> encapsulation mpls !

- CSCtw79579

  Symptoms: Standby fails to be in standby HOT state after reload.

  Conditions: This symptom is seen after removal of an IM and doing RSP stateful switchover (SSO) and then trying to bring up the standby RSP.

Workaround: There is no workaround.

- CSCtw84414

  Symptoms: Standby reset due to configuration sync failure.

  Conditions: The symptom is observed with the CLI **monitor session** *session* **source remote vlan**.

  Workaround: There is no workaround.

- CSCtw84664

  A vulnerability exists in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause an affected device to reload. Affected devices must be configured to process SIP messages and for pass-through of Session Description Protocol (SDP) for this vulnerability to be exploitable.

  Cisco has released free software updates that address this vulnerability. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerability.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-sip

- CSCtw85883

  Symptoms: The error "ace_add_one_map failed" occurs while adding an ACE to a crypto acl that is being used by a crypto map.

  Conditions: This symptom is observed when the crypto map is applied to an interface and the crypto acl being modified is also in use.

  Workaround: Remove the crypto map and apply the ACL changes to avoid the error.

- CSCtw86212

  Symptoms: ISG is failing to support radius attribute filter configuration.

  Conditions: ISG is setting up a session via EAP/RP authentication, whereas authorization radius attribute(s) should be passed on by ISG to its radius client and ISG should ignore it locally when creating the session. It occurs only in the case of radius proxy.

  Workaround: Possibly do not send the undesired radius attributes to ISG in authentication/authorization replies and configure the required parameters on each radius-client (from an ISG perspective).

- CSCtw86712

  Symptoms: RP crashes.

  Conditions: The symptom is observed when you apply certain tunnel configurations.

  Workaround: There is no workaround.

- CSCtw86793

  Symptoms: A Cisco router running Cisco IOS 15.2T will generate phase II rekeys using IKEv1 instead IKEv2.

  Conditions: The symptom is observed with an IKEv2 DVTI hub (tunnel mode GRE IP).

  Workaround: Anchor the IKEv2 profile into the IPsec profile.

- CSCtw86880

  Symptoms: IOSD crashes during unconfiguration.

Conditions: The symptom is observed when you clear the IP sessions and then immediately unconfigure the port-bundle that is in use. Issue seems to be timing related.

Workaround: There is no workaround.

- CSCtw87783

  Symptoms: Applying a "match-protocol" causes the Cisco ASR 1000 to freeze and then reload.

  Conditions: This symptom appears when writing a "match-protocol ..." command while applying an MQC class-map on certain protocols (RTSP, NNTP).

  Workaround: There is no workaround.

- CSCtw88094

  Symptoms: The standby management processor reloads during configuration sync when there is a mismatch in the IP SLA configuration.

  Conditions: This symptom occurs shortly after the "ip sla schedule X start specific_start_time" command is issued multiple times on the same probe instance. Hence, when the configuration is synced to the standby management processor, a PRC error occurs. The PRC error causes a reload of the standby management processor.

  Workaround: Unschedule the probe before rescheduling for a specific start time.

- CSCtw88599

  Symptoms: If "port acl" is configured, diagnostics for the port fail during bootup. If the port ACL is on a supervisor port then the router goes for a reload.

  Conditions: The symptom is observed when you configure "port acl" on a switch port and reload the router.

  Workaround: Disable diagnostics for the module.

- CSCtw94319

  Symptoms: Crash is seen at dhcpd_forward_request.

  Conditions: This symptom is seen when the IP DHCP Relay feature is used in scaled configuration.

  Workaround: Remove the **ip dhcp relay information option vpn** command, if possible. Otherwise, there is no workaround.

- CSCtw97513

  Symptoms: STP BPDUs are not sent over more than one VFI neighbor.

  Conditions: The symptom is observed with full mesh Virtual Private LAN Services (VPLS). The STP does not converge end-to-end.

  Workaround: There is no workaround.

- CSCtw98456

  Symptoms: A LAN-to-LAN VPN tunnel fails to come up when initiated from the router side, or when it is up (after being initiated by the peer). Incoming traffic is OK but no traffic is going out over the tunnel.

  Inspection of the IVRF routing table shows that there is a route to the remote destination with the correct next hop, but the route does not point to the egress interface (the interface with the crypto map in the FVRF).

  For example, the IVRF routing table should show:

  S 10.0.0.0 [1/0] via 192.168.0.1, GigabitEthernet1/0/1

  but instead it shows:

S 10.0.0.0 [1/0] via 192.168.0.1

where GigabitEthernet1/0/1 is the interface in the FVRF with the crypto map, and 192.168.0.1 is the next-hop in the FVRF through which the VPN peer is reachable.

Consequently, no traffic from the IVRF is routed to the egress interface, so no traffic is hitting the crypto map and hence the encryption counters (in **show crypto ipsec sa**) remain at zero.

Conditions: This has been observed on a Cisco ASR 1000 series router that is running Cisco IOS Release 15.1(3)S1. (Cisco IOS Release 15.0(1)S4 has been confirmed not to be affected.) Other Cisco IOS versions and other hardware platforms may be affected.

Workaround: Configure a static route to the remote network. For example:

ip route vrf IVRF 10.0.0.0 255.0.0.0 GigabitEthernet1/0/1 192.168.0.1

where GigabitEthernet1/0/1 is the interface in the FVRF with the crypto map, and 192.168.0.1 is the next-hop in the FVRF through which the VPN peer is reachable.

- CSCtw99290

  Symptoms: The source or destination group-address gets replaced by another valid group-address.

  Conditions: The symptom is observed during the NVGEN process if it suspends (for example: when having a huge configuration generating the running-config for local viewing or during the saving of the configuration or during the bulk sync with the standby and the NVGEN process suspends). The global shared buffer having the address gets overwritten by another process before the NVGEN completes.

  Workaround: There is no workaround.

- CSCtx00689

  Symptoms: Speed configurations may be rejected on standby. This causes a standby sync failure.

  Conditions: The symptom is observed when you configure speed on the main interface.

  Workaround: There is no workaround.

- CSCtx01329

  Symptoms: A Cisco 2921 using Cisco IOS Release 15.2(2)T and configured for crypto with access lists may have problems booting up. CPU hog messages and a watchdog crash may be seen.

  Conditions: The conditions are undetermined.

  Workaround: Use Cisco IOS Release 15.1(3)T.

- CSCtx01604

  Symptoms: Cisco IOS might crash on some 64-bit platform if CNS ID is configured as the IP address of some active network interface, and this IP address is changed in the middle of some critical CNS feature operations.

  Conditions: This problem presents a bad planning of bootstrapping a Cisco IOS device via an unreliable network interface whose IP address could be changed any time during the bootstrapping.

  Workaround: Do not use any dynamic network interface IP address as CNS ID.

- CSCtx01918

  Symptoms: On the hub if you configure IVRF for static crypto-map then, after an invalid-spi recovery, the new ISAKMP has an incorrect IVRF (global). IPsec phase II fails with a “proxy identities not supported” error message. The other related issues seen are:

  1. Initial contact not being sent when IKE SA is triggered by invalid-spi recovery.

2. When quick mode is initiated, it picks the self-initiated IKE SA and hence the QM packet is dropped at the other end.

Conditions: The symptom is observed with a router running HSRP with VRF aware IPsec static crypto map. When you shutdown the active router's external interface, the IPsec tunnel failsover to the standby router. The standby router has an invalid-spi recovery configured. The invalid-spi recovery kicks but new ISAKMP has an incorrect IVRF and IPsec phase II fails.

Workaround: Manually clear SA at spoke site using **clear crypto sa**.

- CSCtx04712

  Symptoms: Removal of crypto map hangs the router.

  Conditions: The symptom is observed following removal of "gdoi crypto map" from interface.

  Workaround: There is no workaround.

- CSCtx05464

  Symptoms: CE multicast fails over VPLS when the PE device is an ME 3800x.

  Conditions: The symptom is observed with VPLS configured in a mesh with at least five VPLS peers.

  Workaround: For routing protocols, use unicast neighbors.

- CSCtx05942

  Symptoms: The session to the service module from the Supervisor Fails. This can happen with SAMI, NAM, NAM-2 etc. modules.

  For example, if the SAMI card is in Slot 2, the **session slot** *2* **processor 0** command fails to create a telnet session and fails to give out the following messages:

  SUP#session slot 2 proc 3 The default escape character is Ctrl-^, then x. You can also type 'exit' at the remote prompt to end the session Trying 127.0.0.33 ... % Connection timed out; remote host not responding

  Conditions: This symptom occurs with Cisco IOS Release 15.2(1)S release. It is not observed with Cisco IOS Release 15.1(3)S1 or lower version.

  Workaround: Downgrading the Supervisor to Cisco IOS Release 15.1(3)S1 or lower version resolves this issue.

- CSCtx09614

  Symptoms: With the preconfigured ATM configuration, the standby RSP does not boot up.

  Conditions: This symptom is observed when one of the RSPs is up and the running configuration has the ATM configuration under the controller.

  Workaround: There is no workaround. Without an ATM configuration, the standby RSP goes to standby mode.

- CSCtx16782

  Symptoms: FlexVPN hub to spoke stays in NEGOTIATING state.

  Conditions: The symptom is observed on a FlexVPN spoke and seen at connection with hub.

  Workaround: There is no workaround.

- CSCtx19332

  Symptoms: A Cisco router crashes when "remote mep" is unlearned while auto EOAM operations are executing.

Conditions: This symptom is observed if "remote mep" is unlearned from the auto database (shutdown on interface or remote mep reload) while the "IP SLA ethernet-monitor jitter" operation is still running. The crash occurs if the initial control message times out.

Workaround: There is no workaround.

- CSCtx21206

  Symptoms: BFDv6 hardware offloaded sessions do not come up with all IPv6 source addresses.

  Conditions: This symptom is observed with interface source IPv6 addresses that have some specific bits in the 6th byte set like 6001:1:C::1..

  Workaround: Reconfigure the source IPv6 addresses to some address that will not match the criteria mentioned in the above Conditions.

- CSCtx29543

  Symptoms: A Cisco router may crash when an IPv4 default route update occurs or when doing the **show ip route** command.

  Conditions: This symptom occurs under the following conditions:

  1. At least one IPv4 route associated with each of the 23 possible supernet mask lengths exist.
  2. A default route exists.
  3. All routes corresponding to one of the 23 possible supernet mask lengths are removed.

  The router may now crash when doing **show ip route** command or when default route is updated.

  Workaround: There are two possible workarounds:

  1. Insure that not all 23 supernet mask lengths are populated by doing route filtering.
  2. If workaround #1 is not possible, then insure that at least one supernet route for all possible mask lengths exists at all times, for example by configuring summary routes that do not interfere with normal operation.

- CSCtx29557

  Symptoms: A standby crashes @ fib_fib_src_interface_sb_init.

  Conditions: All.

  Workaround: There is no workaround.

- CSCtx32628

  Symptoms: When a primary BGP path fails, the prefix does not get removed from the BGP table on the RR/BGP peer although a withdrawal message is received.

  Conditions: This symptom is observed on an L3vpn CE which is dual homed via BGP to a PE under the following conditions:

  - BGP full mesh is configured.
  - BGP cluster-id is configured.
  - **address family vpnv4** is enabled.
  - **address family ipv4 mdt** is enabled.
  - The sending peer is only mcast RD type 2 capable, the receiving peer is MDT SAFI and RD type 2 capable.

  Workaround: Remove the cluster-id configuration or hard-reset the BGP session on the affected Cisco router. However, removing the cluster-id does not guarantee protection.

- CSCtx34643

  Symptoms: MPLS pseudowire ping fails.

  Conditions: The symptom is observed when you configure MPLS with xconnect.

  Workaround: There is no workaround.

- CSCtx39936

  Symptoms: A Cisco 7600 router configured for MPLS TE with tunnel load-sharing may punt traffic to MSFC when multiple TE paths to a given destination exist.

  Conditions: The symptom is observed with a Cisco 7600 router that is running Cisco IOS Release 12.2(33)SRE4, configured with multiple MPLS TE tunnels with load-sharing.

  Workaround 1: In some cases, clearing the router may trigger proper reprogramming of the prefix in the hardware.

  Workaround 2: Remove load-sharing from the TE tunnels.

- CSCtx41296

  Symptoms: When you do a **clear crypto session** in 4k flexVPN cases, the memory of crypto IKEv2 shows that it is increasing.

  Conditions: The symptom is observed with session flapping.

  Workaround: There is no workaround.

- CSCtx42722

  Symptoms: Routed multicast traffic is not forwarded out to all interfaces in OIL.

  Conditions: The issue seen on 15.1 code.

  Workaround: Issue a **clear ip mroute** *group* for the group in the broken state.

  Further Problem Description: The issue can be verified by checking **show platform ip multicast group** *group* **detail**. If encountering the issue, ports will be missing from the OIF for the S,G entry:

```
me3600x#sh platform ip multicast groups 224.0.10.135 detail
GROUP_ADDR 224.0.10.135

NMDB (*, 224.0.10.135) nmdb->0xD7E82E4, entry->0xE53D134 magic 0x9E tcam
hdl:0x277 nh_rpf_p:0xC3D85F8 nh_rpf_f:0xC3D8498 fid_hdl:0x13FD4D3C
(idx=0xBEB1) rpf pass:cpuQ:4 rpf falied cpuQ:5
 flags: HW, pflags: SPT,

RPF INTERFACE-> intf 501 port count (1) p10

RPF pass OIF interface count 1 hw_cnt 1
intf 224 port count 1 flags=0x8
 p11 <<<--- Correct port information getting reflected

RPF failed OIF interface count 1 hw_cnt 1 intf 224 port count 1 flags=0x8
 p11

GROUP_ADDR 224.0.10.135
```

```
NMDB (10.0.2.70, 224.0.10.135) nmdb->0xD7E64B4, entry->0xE53A494 magic 0xB6
tcam hdl:0x298 nh_rpf_p:0xC3DE4D8 nh_rpf_f:0x0 fid_hdl:0x13FDF8CC(idx=0xBEED)
rpf pass:cpuQ:0 rpf falied cpuQ:6
 flags: HW, pflags:

RPF INTERFACE-> intf 501 port count (1) p10


RPF pass OIF interface count 1 hw_cnt 1
intf 224 port count 0 flags=0x8
                              <<<<<---- Missing port information
```

- CSCtx44060

  Symptoms: Flexvpn spoke-to-spoke tunnels do not come up.

  Conditions: None.

  Workaround: Once tunnels fail to come up, clear the NHRP cache on one spoke alone.

- CSCtx48010

  Symptoms: PIM neighbors on MDT tunnel continuously flap on a Cisco 7600 series router. Decapsulation path shows wrong rewrite index for flapping peers, instead of expected 7FFA recirculation index.

  Conditions: The symptom is observed with Cisco IOS Release 15.1(3)S1. ES20 card as core-facing.

  Workaround: Identifying the adjacency of the flapping peer and changing the rewrite index to 7FFA manually stops the flap:

  test mls cef adj 180262 4055 9238 7ffa 2608 20 multicast 001e.f741.e28d 0.0.0 0 0x5fa

- CSCtx49766

  Symptoms: GETVPN does not allow traffic in a Cisco HWIC-3G-CDMA-V modem.

  Conditions: This symptom is observed on a Cisco HWIC-3G-CDMA-V modem running Cisco IOS Release 15.1(4)M3.

  Workaround: Use Cisco IOS Release 15.1(3)T3 with the Cisco HWIC-3G-CDMA-V modem.

- CSCtx51935

  Symptoms: Router crashes after configuring “mpls traffic-eng tunnels”.

  Conditions: The symptom is observed with the following steps:

  interface gi1/2 mpls traffic-eng tunnels no shut

  router OSPF 1 mpls traffic-eng area 100 mpls traffic-eng router-id lo0 end

  show mpls traffic-eng link-management summary

  Workaround: There is no workaround.

- CSCtx54946

  Symptoms: CoA requests failing due to the error messages:

  CoA-NAK packet from host 10.10.10.14 port 1700, id=175, length=147 Reply-Message = "Push invoke failed Error-Cause = Unsupported-Service Cisco-Command-Code = "020;;turbo_button(in_p=3000000,out_s=3000000)" Cisco-Account-Info = "S18.0.23.175" Cisco-Account-Info = "$IVirtual-Access1.6017"

Conditions: The symptom is observed when you bring up 12K PTA sessions and send CoA request to all the sessions with VSA 252 0c attribute.

Workaround: There is no workaround.

- CSCtx55357

  Symptoms: Auto RP messages are permitted through "ip multicast boundary".

  Conditions: The symptom is observed when the ACL associated with the multicast boundary matches 224.0.1.39 and 224.0.1.40. It is seen on the Cisco ASR 1000 platform.

  Workaround: Use "no ip pim autorp" which will disable Auto RP completely from this device.

- CSCtx57584

  Symptoms: SIP basic call fails with 500 internal server error.

  Conditions: The symptom is observed with Cisco IOS interim Release 15.2(02.14) T.

  Workaround: There is no workaround.

- CSCtx61815

  Symptoms: IPsec sessions are not coming up.

  Conditions: The symptom is observed when 1000 sessions are configured. Only 50 IPsec sessions are coming up.

  Workaround: There is no workaround.

- CSCtx62215

  Symptoms: In the presence of ingress and egress marking, ingress exp marking stops working.

  Conditions: The symptom is observed only when you reload the router in the presence of ingress and egress marking.

  Workaround: Detach and reattach the ingress policy which does exp marking.

- CSCtx63034

  Symptoms: After a Cisco 7600 router is powered by PWR-2500-DC, PWR-4000-DC or PWR-6000-DC to Cisco IOS Release 15.2(1)S, the router logs the following error messages:

  %C7600_PWR-SP-3-PSUNKNOWN: Unknown power supply in slot 1 (idprom read failed). %OIR-SP-6-INSPS: Power supply inserted in slot 1 %C7600_PWR-SP-4-PSOK: power supply 1 turned on.

  The **show power** command shows that the power supply only provides 919W. Most of the line cards cannot be powered up.

  Conditions: This symptom is observed in Cisco IOS Release 15.2(1)S only. The problem does not occur in Cisco IOS Release 15.1(3)S1. PWR-4000-DC and PWR-6000-DC are confirmed to be affected by this problem.

  Workaround: There is no workaround.

- CSCtx63545

  Symptoms: Box will crash in case of all the configured radius servers are dead and tried to authenticate client against RADIUS in the Radius-proxy case.

  Conditions: This will happen only for Radius-Proxy senario and if all the configured radius servers are dead.

  Workaround: Configure one of the alive RADIUS Servers.

- CSCtx63716

  Symptoms: Traceback seen @ cmfib_lc_process_entry.

  Conditions: There are no specific conditions.

  Workaround: There is no workaround.

- CSCtx66011

  A vulnerability in the Internet Key Exchange (IKE) protocol of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a memory leak that could lead to a device reload.

  The vulnerability is due to incorrect handling of malformed IKE packets by the affected software. An attacker could exploit this vulnerability by sending crafted IKE packets to a device configured with features that leverage IKE version 1 (IKEv1).

  Although IKEv1 is automatically enabled on a Cisco IOS Software and Cisco IOS XE Software when IKEv1 or IKE version 2 (IKEv2) is configured, the vulnerability can be triggered only by sending a malformed IKEv1 packet.

  In specific conditions, normal IKEv1 packets can also cause an affected release of Cisco IOS Software to leak memory.

  Only IKEv1 is affected by this vulnerability.

  An exploit could cause Cisco IOS Software not to release allocated memory, causing a memory leak. A sustained attack may result in a device reload.

  Cisco has released free software updates that address this vulnerability. There are no workarounds to mitigate this vulnerability.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130925-ike

  Note: The September 25, 2013, Cisco IOS Software Security Advisory bundled publication includes eight Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the September 2013 bundled publication.

  Individual publication links are in “Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication” at the following link:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep13.html

- CSCtx67290

  Symptoms: A Cisco Session Border Controller crashes when receiving an oversize rtcp-fb element in the SDP.

  Conditions: The symptom is observed when there is an oversize rctp-fb element in the SDP.

  Workaround: There is no workaround.

- CSCtx67474

  Symptoms: Update message is sent with an empty NLRI when the message consists of 2byte aspath in ASPATH attribute and 4byte value aggregate attribute.

  Conditions: This can happen when there is a mix of 2byte and 4byte attributes in the update message and the message is sent from a 2byte peer and there is a 4byte aggregator attribute.

  Workaround: Move all the 2byte AS peers to a separate update-group using a non-impacting outbound policy like “advertisement-interval”.

- CSCtx68100

  Symptoms: On a system having SP-RP, the reload reason is not displayed correctly. Once the system crashes, in all subsequent reloads the last reload reason is displayed as crash.

  Conditions: The symptom is observed on a system having SP-RP. The reload reason is shown wrongly when the **show version** CLI is executed.

  Workaround: There is no workaround.

- CSCtx71618

  Symptoms: Router crash at process L2TP mgmt daemon.

  Conditions: The symptom is observed with a Cisco ASR 1006 (RP2) running Cisco IOS Release 15.1(2)S.

  Workaround: There is no workaround.

- CSCtx73452

  Symptoms: The following symptoms are observed:

  1. You send an ICMPv4 packet with IP option. It will be forwarded by Cisco ASR1001. IP options field includes "loose source routing" option.
  2. Cisco ASR 1001 receives the packet. ASR 1001 has "no ip source-route" setting in its configuration.
  3. ASR 1001 incorrectly overwrites the destination IP address of packet, which has source-route option set, and forwards it instead of dropping it.

  Conditions: The symptom is observed with the Cisco ASR 1001 (2.5G ESP).

  Workaround: There is no workaround.

- CSCtx76780

  Symptoms: DHCP relay does not work on Cisco ME 3600.

  Conditions: This issue is observed if you configure at the same time a "ip helper-address" and an xconnect under the VLAN interface. It is observed on ME 3600/ME 3800 platforms running Cisco IOS Release 15.1(2)EY1 or earlier.

  Workaround: There is no workaround.

- CSCtx87939

  Symptoms: When the **Mediatrace Poll** command is invoked using WSMA interface, the "hops response received notifications" message is displayed. This message corrupts the WSMA output for the command.

  Conditions: This symptom is observed when Mediatrace poll is used in a WSMA interface.

  Workaround: There is no workaround.

- CSCtx89538

  Symptoms: The following error message may appear on a Cisco ME 3800 that is running Cisco IOS Release 15.1(2)EY1a when attaching ingress policy with marking to a service instance:

  Qos:Out of internal resources %QOSMGR-3-LABEL_EXHAUST: Internal Error in resource allocation

  Conditions: The symptom is observed with:

  - A Cisco ME 3800.
  - Cisco IOS Release 15.1(2)EY1a.

Workaround: There is no workaround.

- CSCtx90299

  Symptoms: The DMVPN IPsec sessions might get torn down and unable to re- establish themselves after experiencing link-flap events.

  Conditions: In a scaled DMVPN environment, when physical-port link-state up/down events happen, there will be stormed IPSec events to tear down and/or re-negotiate the sessions; it might run into a bad state that it cannot establish new sessions. Hence, when those active sessions expire (by time period or volume based), it can no longer be re-created. After some period of time, no more active session remains on the router.

  Workaround: Reload the router.

- CSCtx92665

  Symptoms: Executing the **show mediatrace session stat** command causes a crash at *__be_sla_mt_route_data_print*.

  Conditions: This symptom is observed when **show mediatrace session stat** or **show mediatrace session data** is used.

  Workaround: There is no workaround.

- CSCtx93598

  Symptoms: An “ikev1 dpd” configuration erroneously affects IKEv2 flows.

  Conditions: The symptom is observed if we configured the IKEv1 DPD function with “crypto isakmp keepalive” while IKEv2 is enabled as well. The IKEv2 DPD function will be affected.

  Workaround: There is no workaround.

- CSCtx99544

  Symptoms: Exception occurs when using **no aaa accounting system default vrf** *VRF3* **start-stop group** *RADIUS-SG-VRF3*:

  router(config)# no ip vrf VRF3 router(config)# no aaa accounting system default vrf VRF3 start-stop group RADIUS-SG-VRF3

  %Software-forced reload

  Conditions: The symptom is observed with the following conditions:

  - Hardware: Cisco ASR 1001.
  - Software: asr1001-universalk9.03.04.02.S.151-3.S2.

  Workaround: There is no workaround.

- CSCty00734

  Symptoms: OSPF failing over xconnect between CE-CE connected via xconnect.

  Conditions: The symptom is observed with a change in L3 adjacency.

  Workaround: Use the following command: **clear xconnect** *peer vcid*.

- CSCty02403

  Symptoms: EIGRP topo entry with bogus nexthop is created when more than one attribute is present in the route received from neighbors. It also tries to install one default route with bogus nexthop. So if you have a default route received from some neighbors, then that default route will also be flapped.

  Conditions: It can only occur when you have more then one attribute set in any route received from a neighbor.

Workaround: Do not set more then one attribute in the route.

- CSCty04213

  Symptoms: “Max aces 1000” is configured for an ACL and attached to a interface. Unconfiguring either ACL or ACEs under the ACL leads to a system crash.

  Conditions: The symptom is observed when an ACL configured with 1000 ACEs is attached to interface for ingress or egress packet processing and later when either the ACL is configured or one of the ACEs is unconfigured in the ACL, you will see a crash of the Cisco ME 3600/ME 3800 device.

  Workaround: There is no workaround unless you can configure the number of ACEs less than 1000 per ACL.

- CSCty06990

  Symptoms: Intercepted packets are not forwarded to MD.

  Conditions: The symptom occurs randomly after applying an LI tap on a Cisco 7600 with a SIP400 as the dedicated LI service card.

  Workaround: Remove and reapply TAP.

- CSCty12055

  Symptoms: A Cisco ASR 1000 6RU acting as IPsec-DMVPN hub with 4K sessions up on the router may unexpectedly reload at “IPSec background proc” within a few hours.

  Conditions: The symptom is observed on a Cisco ASR 1000 6RU acting as IPsec- DMVPN hub.

  Workaround: There is no workaround.

- CSCty15615

  Symptoms: Policy in direction A may disappear after removing policy from direction B. The policies no longer show up under the interface in **sh policy-map int** or **show running**.

  Conditions: The symptom is observed with policies on both input and output directions, and then you remove from one of the directions. Happens on Cisco 7200/7600 platforms.

  Workaround: There is no workaround.

- CSCty16623

  Symptoms: Traffic getting black holed because the VPN corresponding to the tunnel secondary VLAN gets programmed with punt adjacency.

  Conditions: The symptom is observed with unconfiguring-reconfiguring the VRF. (The issue is independent of time gap between the configuration change.)

  Workaround: There is no workaround.

- CSCty24707

  Symptoms: Standby RP continually reboots and never recovers.

  Conditions: The symptom is observed during an RP standby switchover with QoS applied to ISG sessions.

  Workaround: Shut down the virtual template interface and do a switchover.

- CSCty58300

  Cisco IOS Software contains a vulnerability in the Border Gateway Protocol (BGP) routing protocol feature.

  The vulnerability can be triggered when the router receives a malformed attribute from a peer on an existing BGP session.

Successful exploitation of this vulnerability can cause all BGP sessions to reset. Repeated exploitation may result in an inability to route packets to BGP neighbors during reconvergence times.

Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability. This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-bgp

Caveats for Cisco IOS Release 15.2(1)S

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats, and only select severity 3 caveats are included in this section.

In this section, the following information is provided for each caveat:

- Symptoms—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.

Note If you have an account on Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com and go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl. (If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)

This section consists of the following subsections:

Resolved Caveats—Cisco IOS Release 15.2(1)S2

Cisco IOS Release 15.2(1)S2 is a rebuild release for Cisco IOS Release 15.2(1)S. The caveats in this section are resolved in Cisco IOS Release 15.2(1)S2 but may be open in previous Cisco IOS releases.

- CSCti00319

  Symptom 1: The warning message “Fatal error FIFO” occurs repeatedly upon PPPoEoA Session teardown.

  Symptom 2: On the LC console, the message “Command Indication Q wrapped” keeps appearing.

  Conditions: This symptom is observed on a Cisco ASR1001 router and kingpin router chassis under the following conditions:

  1. High scale session counts.
  2. Range configuration with more than 100 virtual channels (VC).
  3. Back to back creation and deletion of multiple VCs with no time gap.

  Workaround: There is no workaround.

- CSCtj95685

  Symptoms: A router configured as a voice gateway may crash while processing calls.

  Conditions: The symptom is observed with a router configured as a voice gateway.

  Workaround: There is no workaround.

- CSCtq24557

  Symptoms: Router crash after deleting multiple VRFs. This happens very rarely.

  Conditions: The symptom is observed in a large scale scenario.

  Workaround: There is no workaround.

- CSCtq95384

  Symptoms: Even after the removal of NSR configurations, BGP still holds memory.

  Conditions: The symptom is observed after the removal of NSR configurations.

  Workaround: There is no workaround.

- CSCtr47317

  Symptoms: After a switchover, a Cisco Catalyst 6500 series switch may be replicating some spanned traffic indefinitely and flooding the network with the span copies.

  Conditions: The issue is seen after the following sequence:

  - An internal service module session for a FWSM or other service modules exists:

  ```
  UUT#show monitor session all
  Session 1
  Type  : Service Module Session
  ```

  - If you attempt to configure a span session with the session number already in use:

  ```
  UUT(config)#monitor session 1 source interface Gi2/7 , Gi2/40
  % Session 1 used by service module
  ```

  - The command seems to be rejected, but it is synchronized to the standby supervisor.
  - A switchover happens.

  Workaround: There is no workaround.

- CSCtr87070

  Symptoms: Enable login failed with error "% Error in authentication".

  Conditions: The symptom is observed with TACACS single-connection.

  Workaround: Remove TACACS single-connection.

- CSCts40043

  Symptoms: A Cisco router may crash due to a segmentation fault.

  Conditions: The symptom is observed when a fail-close ACL is applied to the Gdoi crypto map in GETVPN implementation.

  Workaround: There is no workaround.

- CSCts59564

  Symptoms: PIM neighbor over MDT tunnel goes down.

  Conditions: The symptom is observed with **hw-module reset** of access and core card, followed by an SSO.

  Workaround: There is no workaround.

- CSCts65564

  Symptoms: In a large scale DMVPN environment, a DMVPN hub router may crash in the IOS process under high scale conditions.

  Conditions: This only occurs if CRL caching is disabled (with the command **crl cache none** under the pki trustpoint configuration).

Workaround: Enable CRL caching (this is the configured default).

- CSCts72911

  Symptoms: In case of a GR/NSF peering, after an SSO switchover, the restarting router (PE, in this case) does not advertise RT constrain filters to the non-restarting peer (RR, in this case).

  Conditions: The symptom is observed after an SSO switchover in GR/NSF peering. Due to the RT constrain filters not sent by the restarting router after the SSO, the non-restarting router does not send back the corresponding VPN prefixes towards the restarted router.

  Workaround: There is no workaround.

- CSCts88817

  Symptoms: ASA-SM(s) and SCV-NAM3 in a Cisco Catalyst 6000 series switch may be reloaded by supervisor associated with the following syslogs reported by the switch:

```
%CPU_MONITOR-SP-6-NOT_HEARD: CPU_MONITOR messages have not been heard for 31
seconds [4/0]
%CPU_MONITOR-SP-6-NOT_HEARD: CPU_MONITOR messages have not been heard for 31
seconds [9/0]
%CPU_MONITOR-SP-6-NOT_HEARD: CPU_MONITOR messages have not been heard for 61
seconds [4/0]
%CPU_MONITOR-SP-6-NOT_HEARD: CPU_MONITOR messages have not been heard for 61
seconds [9/0]
%CPU_MONITOR-SP-6-NOT_HEARD: CPU_MONITOR messages have not been heard for 91
seconds [4/0]
%CPU_MONITOR-SP-6-NOT_HEARD: CPU_MONITOR messages have not been heard for 91
seconds [9/0]
%OIR-SP-3-PWRCYCLE: Card in module 4, is being power-cycled 'off (Module not
responding to Keep Alive polling)'
%C6KPWR-SP-4-DISABLED: power to module in slot 4 set off (Module not
responding to Keep Alive polling)
%OIR-SP-3-PWRCYCLE: Card in module 9, is being power-cycled 'off (Module not
responding to Keep Alive polling)'
 %C6KPWR-SP-4-DISABLED: power to module in slot 9 set off (Module not
responding to Keep Alive polling)
```

  Conditions: The lockup may occur if there are non-fabric cards in the chassis with the ASA or NAM3 card. Non-fabric cards have a model number of 61xx, 62xx, 63xx, and 64xx.

  Workaround: There is no workaround.

- CSCtt17762

  Symptoms: Mtrace does not show the IP address of RPF interface of a multicast hop.

  Conditions: The symptom is observed on an IP PIM multicast network.

  Workaround: There is no workaround.

- CSCtt26074

  Symptoms: Memory leak with IP SLAs XOS Even process.

  Conditions: The symptom is observed with IP SLA configured.

  Workaround: There is no workaround.

- CSCtt35379

  Cisco IOS Software contains a vulnerability in the Border Gateway Protocol (BGP) routing protocol feature.

  The vulnerability can be triggered when the router receives a malformed attribute from a peer on an existing BGP session.

Successful exploitation of this vulnerability can cause all BGP sessions to reset. Repeated exploitation may result in an inability to route packets to BGP neighbors during reconvergence times.

Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability. This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-bgp

- CSCtt39944

  Symptoms: The **show mls cef adjacency usage** is not showing the adjacency count correctly.

  Conditions: The symptom is observed in highly scaled networks. The platform code is not counting the last non-stats region allocation for adjacency usage.

  Workaround: There is no workaround.

- CSCtt46638

  Symptoms: A Cisco 7604 running Cisco IOS Release 12.2(33)SRE4/SRE5 crashes when changing the tunnel source and destination of an IPsec sVTI.

  Conditions: The symptom is observed once the IPsec session is up and traffic is flowing through. If the tunnel source or destination is changed, the router crashes. This does not occur with a plain GRE tunnel.

  Workaround: There is no workaround.

- CSCtu00699

  Symptoms: On a DMVPN hub router, the IOS processor memory pool can get fragmented due to memory allocated for “Crypto NAS Port ID”.

  Conditions: This happens when there is network instability potentially causing tunnels to flap frequently.

  Workaround: There is no workaround.

- CSCtu08608

  Symptoms: The standby RP crashes due to Voip HA Session App.

  Conditions: The Cisco ASR 1000 platform with redundant RPs and Cisco Unified Border Element Enterprise. The signature in the crashinfo is as follows:

  ```
  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = Voip HA Session App
  ```

  Workaround: There is no workaround.

- CSCtu26431

  Symptoms: Memory leaks pointing to “OER SAA MC PROB”.

  Conditions: The symptom is observed when running probes are deleted. This is a rare event.

  Workaround: There is no workaround.

- CSCtu32301

  Symptoms: Memory leak may be seen.

  Conditions: This is seen when running large **show** commands like **show tech-support** on the linecard via the RP console.

  Workaround: Do not run the show commands frequently.

- CSCtu35116

  Symptoms: VPDN session keeps on trying to come up with MPLS MTU higher than 1500.

Conditions: The symptom is observed when you upgrade a Cisco 7200VXR from the c7200-a3jk91s-mz.122-31.SB18 to the c7200-adventerprisek9-mz.122-33.SRE4 image.

Workaround: There is no workaround.

- CSCtu38244

  Symptoms: After bootup, the GM cannot register and is stuck in "registering" state. Issuing the **clear crypto gdoi** command is required for a successful registration to the keyserver.

  Conditions: The symptom is observed upon router bootup.

  Workaround: Either do a **clear crypto gdoi** after a reload, or configure a second keyserver entry. This does not have to be an existing keyserver, it can be just a dummy address.

- CSCtu60863

  Symptoms: IGMP reports do not get installed in the IGMP group list.

  Conditions: The symptom is observed when the port-security feature is enabled on the switchport which is part of the VLAN on which the IGMP reports are received.

  Workaround: Remove "switchport port-security" from ports associated with the VLAN on which the IGMP reports are received.

- CSCtu65655

  Symptoms: RP1 crash due to corrupted memory.

  Conditions: The symptom is observed with the following conditions:

  – Ixia -- CES (IPsec static crypto map) -- UUT (IPSec DVTI server).

  – UUT - 4RU(RP1/ESP10).

  – Scale 1000 IKE * 1 VRF * 4 IPsec, total 4K IPsec sessions.

  – CAC (30) enabled.

  – DPD (60/15/on-demand) enabled.

  – Reload CES (Cisco 7200 platform) every 10-15 minutes.

  – 60M bidirectional traffic.

  Workaround: There is no workaround.

- CSCtw45592

  Symptoms: The **ntp server** *DNS-name* command is not synced to the standby. When the **no ntp server** *hostname* command is issued later on the active, the standby reloads because the config was not added.

  Conditions: When the device is reloaded or when the DNS name is not resolved, the config is not added. After the standby SYNC failure, then issuing the **no ntp server** *hostname*.

  Workaround: Use IP/IPv6 addresses instead of the hostname for NTP configurations. The IP/IPv6 address can be found by pinging the hostname.

- CSCtw56439

  Symptoms: The **ip mtu** command that is configured on an IPsec tunnel disappears after a router reload.

  Conditions: The symptom is observed with IPsec and the **ip mtu** over a tunnel interface.

  Workaround: There is no workaround.

- CSCtw61872

  Symptoms: The router will crash when executing a complex sort on the flexible netflow cache from multiple CLI sessions.

  Conditions: The symptom is observed when executing a complex sort with top- talkers on a show command from multiple CLI sessions (note that normal show commands without top-talkers are fine):

  ```
  sh flow monitor QoS_Monitor cache sort highest counter packets top 1000
  sh flow monitor QoS_Monitor cache sort highest counter packets top 10000
  ```

  Workaround: Do not execute complex sorts with top-talkers on the show output from multiple CLI sessions.

- CSCtw62310

  Symptoms: The **cells** keyword is added to “random-detect” whenever a policy-map is removed from an interface/map-class via “no service- policy”.

  Conditions: The symptom is observed when removing the policy-map from map-class.

  Workaround: There is no workaround.

  Further Problem Description: The CLI is technically valid if it has been manually configured as “cells” prior to the removal. The issue is that the template policy is being changed automatically to “cells” whenever the removal happens, regardless of what the original configuration was, and that is not the expected behavior.

- CSCtw71564

  Symptoms: Not all data packets are accounted for in the “show stats” output of the video operation.

  Conditions: The symptom is observed with heavy load on the responder caused either by many video sessions or other processes.

  Workaround: Reduce processor load on device running the responder.

- CSCtw78451

  Symptoms: A Cisco ASR 1000 series router may reload when multiple users are logged in running show commands.

  Conditions: This symptom is only seen when the Cisco ASR router is used as a DMVPN headend and there are hundreds of tunnels flapping.

  Workaround: There is no workaround. However, this appears to be a timing issue when there is instability in a large-scale environment.

- CSCtw86712

  Symptoms: RP crashes.

  Conditions: The symptom is observed when you apply certain tunnel configurations.

  Workaround: There is no workaround.

- CSCtw88094

  Symptoms: The standby management processor reloads during configuration sync when there is a mismatch in the IP SLA configuration.

  Conditions: This symptom occurs shortly after the “ip sla schedule X start specific_start_time” command is issued multiple times on the same probe instance. Hence, when the configuration is synced to the standby management processor, a PRC error occurs. The PRC error causes a reload of the standby management processor.

  Workaround: Unschedule the probe before rescheduling for a specific start time.

- CSCtw88599

  Symptoms: If "port acl" is configured, diagnostics for the port fail during bootup. If the port ACL is on a supervisor port then the router goes for a reload.

  Conditions: The symptom is observed when you configure "port acl" on a switch port and reload the router.

  Workaround: Disable diagnostics for the module.

- CSCtw94598

  Symptoms: Web authentication does not work after an upgrade. NAS-Port-Type = Async.

  Conditions: The symptom is observed when you upgrade to Cisco IOS Release 12.2 (58)SE2 or later or to the Cisco IOS 15.0(1)SE train.

  Workaround: Change NAS-Port-Type on AAA Server to match the new value.

- CSCtw98456

  Symptoms: A LAN-to-LAN VPN tunnel fails to come up when initiated from the router side, or when it is up (after being initiated by the peer). Incoming traffic is OK but no traffic is going out over the tunnel.

  Inspection of the IVRF routing table shows that there is a route to the remote destination with the correct next hop, but the route does not point to the egress interface (the interface with the crypto map in the FVRF).

  For example, the IVRF routing table should show:

  ```
  S        10.0.0.0 [1/0] via 192.168.0.1, GigabitEthernet1/0/1
  ```

  but instead it shows:

  ```
  S        10.0.0.0 [1/0] via 192.168.0.1
  ```

  where GigabitEthernet1/0/1 is the interface in the FVRF with the crypto map, and 192.168.0.1 is the next-hop in the FVRF through which the VPN peer is reachable.

  Consequently, no traffic from the IVRF is routed to the egress interface, so no traffic is hitting the crypto map and hence the encryption counters (in **show crypto ipsec sa**) remain at zero.

  Conditions: This has been observed on a Cisco ASR 1000 series router that is running Cisco IOS Release 15.1(3)S1. (Cisco IOS Release 15.0(1)S4 has been confirmed not to be affected.) Other IOS versions and other hardware platforms may be affected.

  Workaround: Configure a static route to the remote network. For example:

  ```
  ip route vrf IVRF 10.0.0.0 255.0.0.0 GigabitEthernet1/0/1 192.168.0.1
  ```

  where GigabitEthernet1/0/1 is the interface in the FVRF with the crypto map, and 192.168.0.1 is the next-hop in the FVRF through which the VPN peer is reachable.

- CSCtw99989

  Symptoms: During normal operation a Cisco ASR 1000 Series Aggregation Services router may show the following traceback:

  ```
  %FMANRP_ESS-3-ERREVENT: TC still has features applied. TC evsi
  ```

  Conditions: The symptom is observed during PPP renegotiation.

  Workaround: There is no workaround.

- CSCtx02522

  Symptoms: The router displays intermittent traceback errors.

  Conditions: Occurs when you configure REP.

  Workaround: There is no workaround.

- CSCtx29543

  Symptoms: A Cisco router may crash when an IPv4 default route update occurs or when doing the **show ip route** command.

  Conditions: This symptom occurs under the following conditions:

  1. At least one IPv4 route associated with each of the 23 possible supernet mask lengths exist.
  2. A default route exists.
  3. All routes corresponding to one of the 23 possible supernet mask lengths are removed.

  The router may now crash when doing **show ip route** command or when default route is updated.

  Workaround: There are two possible workarounds:

  1. Insure that not all 23 supernet mask lengths are populated by doing route filtering.
  2. If workaround #1 is not possible, then insure that at least one supernet route for all possible mask lengths exists at all times, for example by configuring summary routes that do not interfere with normal operation.

- CSCtx31175

  Symptoms: Framed-IP-Address added twice in PPP service-stop accounting record.

  Conditions: The symptom is observed with the following conditions:

  1. User session exists on ASR1001.
  2. Stop one user's session by using **clear subscriber session username xxx** on ASR1001.
  3. ASR1001 sends double "Framed-IP-Address" in service-stop accounting for one user's session.

  Workaround: Do not use **clear subscriber session** command to clear the session, instead use **clear pppoe**.

- CSCtx32628

  Symptoms: When a primary BGP path fails, the prefix does not get removed from the BGP table on the RR/BGP peer although a withdrawal message is received.

  Conditions: This symptom is observed on an L3vpn CE which is dual homed via BGP to a PE under the following conditions:

  - BGP full mesh is configured.
  - BGP cluster-id is configured.
  - **address family vpnv4** is enabled.
  - **address family ipv4 mdt** is enabled.
  - The sending peer is only mcast RD type 2 capable, the receiving peer is MDT SAFI and RD type 2 capable.

  Workaround: Remove the cluster-id configuration or hard-reset the bgp session on the affected Cisco router. However, removing the cluster-id does not guarantee protection.

- CSCtx35692

  Symptoms: On the Cisco ASR 1000 platform, while acting in a redundancy pair, when the standby ASR becomes active the dial-peers on the standby never change their state back to active causing all calls to fail. Calls that were active during the failover scenario will stay active in the new switchover. Only new calls are affected.

Conditions: The symptom is observed on an ASR 1000 series router CUBE with a box-to-box redundancy configured that is using OOD option pings in the dial- peers. Global configuration of option pings under voice service VoIP is only for IN-Dialog option pings.

Workaround: Disable option keepalives from the dial-peers.

- CSCtx39936

  Symptoms: A Cisco 7600 router configured for MPLS TE with tunnel load-sharing may punt traffic to MSFC when multiple TE paths to a given destination exist.

  Conditions: The symptom is observed with a Cisco 7600 router that is running Cisco IOS Release 12.2(33)SRE4, configured with multiple MPLS TE tunnels with load-sharing.

  Workaround 1: In some cases, clearing the router may trigger proper reprogramming of the prefix in the hardware.

  Workaround 2: Remove load-sharing from the TE tunnels.

- CSCtx48010

  Symptoms: PIM neighbors on MDT tunnel continuously flap on a Cisco 7600 series router. Decapsulation path shows wrong rewrite index for flapping peers, instead of expected 7FFA recirculation index.

  Conditions: The symptom is observed with Cisco IOS Release 15.1(3)S1. ES20 card as core-facing.

  Workaround: Identifying the adjacency of the flapping peer and changing the rewrite index to 7FFA manually stops the flap:

  ```
  test mls cef adj 180262 4055 9238 7ffa 2608 20 multicast 001e.f741.e28d 0.0.0 0 0x5fa
  ```

- CSCtx49073

  Symptoms: Free space check fails and IOS core dump never completes.

  Conditions: The symptom is observed when there is not enough storage media space for IOS core dump.

  Workaround: Make sure there is enough storage space for IOS core dump.

- CSCtx51935

  Symptoms: Router crashes after configuring “mpls traffic-eng tunnels”.

  Conditions: The symptom is observed with the following steps:

  ```
  interface gi1/2
  mpls traffic-eng tunnels
  no shut

  router OSPF 1
  mpls traffic-eng area 100
  mpls traffic-eng router-id lo0
  end
  ```

  Workaround: There is no workaround.

- CSCtx55357

  Symptoms: Auto RP messages are permitted through “ip multicast boundary”.

  Conditions: The symptom is observed when the ACL associated with the multicast boundary matches 224.0.1.39 and 224.0.1.40. It is seen on the Cisco ASR 1000 platform.

  Workaround: Use “no ip pim autorp” which will disable Auto RP completely from this device.

- CSCtx61815

  Symptoms: IPsec sessions are not coming up.

Conditions: The symptom is observed when 1000 sessions are configured. Only 50 IPsec sessions are coming up.

Workaround: There is no workaround.

- CSCtx67474

  Symptoms: Update message is sent with an empty NLRI when the message consists of 2byte aspath in ASPATH attribute and 4byte value aggregate attribute.

  Conditions: This can happen when there is a mix of 2byte and 4byte attributes in the update message and the message is sent from a 2byte peer and there is a 4byte aggregator attribute.

  Workaround: Move all the 2byte AS peers to a separate update-group using a non-impacting outbound policy like "advertisement-interval".

- CSCtx71618

  Symptoms: Router crash at process L2TP mgmt daemon.

  Conditions: The symptom is observed with a Cisco ASR 1006 (RP2) running Cisco IOS Release 15.1(2)S.

  Workaround: There is no workaround.

- CSCtx73452

  Symptoms: The following symptoms are observed:

  1. You send an ICMPv4 packet with IP option. It will be forwarded by ASR1001. IP options field includes "loose source routing" option.
  2. ASR 1001 receives the packet. ASR 1001 has "no ip source-route" setting in its configuration.
  3. ASR 1001 incorrectly overwrites the destination IP address of packet, which has source-route option set, and forwards it instead of dropping it.

  Conditions: The symptom is observed with the Cisco ASR 1001 (2.5G ESP).

  Workaround: There is no workaround.

- CSCtx73612

  Symptoms: A Cisco ASR 1000 may reload while reading IPsec MIBs via SNMP and write a crashfile.

  Conditions: The symptom is observed on a Cisco ASR 1000 that is running Cisco IOS Release 15.1(1)S1.

  Workaround: Do not poll or trap IPsec information via SNMP.

- CSCtx74342

  Symptoms: After interface goes down or is OIRed, in a routing table you can temporarily see IPv6 prefixes associated with the down interface itself (connected routes) as OSPFv3 with the next hop interface set to the interface that is down.

  Conditions: The symptom is observed with OSPFv3. The situation remains until the next SPF is run (5 sec default).

  Workaround: Configuring SPF throttle timer can change the interval.

  Further Problem Description: Here is an example of output after Ethernet0/0 goes down:

```
Routershow ipv6 route
IPv6 Routing Table - default - 2 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       l - LISP
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O   2001::/64 [110/10]
     via Ethernet0/0, directly connected
```

- CSCtx89260

  Symptoms: Re-adding the deleted port channel interface is not initializing the snmp-index.

  Conditions: The symptom is observed when re-adding the deleted port channel interface.

  Workaround: Reloading the standby and then doing an RP switchover or doing a double RP switchover corrects the configuration.

- CSCtx93598

  Symptoms: An “ikev1 dpd” configuration erroneously affects IKEv2 flows.

  Conditions: The symptom is observed if we configured the IKEv1 DPD function with “crypto isakmp keepalive” while IKEv2 is enabled as well. The IKEv2 DPD function will be affected.

  Workaround: There is no workaround.

- CSCtx99544

  Symptoms: Exception occurs when using **no aaa accounting system default vrf** *VRF3* **start-stop group** *RADIUS-SG-VRF3*:

  ```
  router(config)# no ip vrf VRF3
  router(config)# no aaa accounting system default vrf VRF3 start-stop group
  RADIUS-SG-VRF3

  %Software-forced reload
  ```

  Conditions: The symptom is observed with the following conditions:

  - Hardware: Cisco ASR 1001.
  - Software: asr1001-universalk9.03.04.02.S.151-3.S2.

  Workaround: There is no workaround.

- CSCty02403

  Symptoms: EIGRP topo entry with bogus nexthop is created when more than one attribute is present in the route received from neighbors. It also tries to install one default route with bogus nexthop. So if you have a default route received from some neighbors, then that default route will also be flapped.

  Conditions: It can only occur when you have more then one attribute set in any route received from a neighbor.

  Workaround: Do not set more then one attribute in the route.

- CSCty05150

  Symptoms: Default route is removed from stub area after SSO.

  Conditions: The symptom is observed when a PE router is configured as ABR for a stub area and generating a default route. After switchover the default route is withdrawn.

  Workaround 1: Move the default route generation to CE router.

  Workaround 2: Remove and reconfigure “area x stub no summary” on PE router.

- CSCty06191

  Symptoms: When an IPHC configuration is applied on a multilink bundle interface and the interface is flapped, the IPHC configuration does not apply successfully on a linecard.

Conditions: The symptom is observed with a multilink interface flap.

Workaround: Unconfigure and then reconfigure the IPHC configuration on the multilink interface.

- CSCty06990

  Symptoms: Intercepted packets are not forwarded to MD.

  Conditions: The symptom occurs randomly after applying an LI tap on a Cisco 7600 with a SIP400 as the dedicated LI service card.

  Workaround: Remove and reapply TAP.

- CSCty13647

  Symptoms: Symptoms vary from one image to another. The following symptoms have been mostly observed:

  1. Spurious memory access tracebacks from SPAN code even when SPAN is not configured.
  2. RP crash when unconfiguring a SPAN session with a particular session number.

  Conditions: Always seen on a particular SPAN session number.

  Workaround: Use a different a SPAN session number for SPAN configurations to avoid the router crash. (There is no workaround to avoid spurious memory access messages.)

- CSCty37020

  Symptoms: Learned inside BGP prefixes are not getting added into MC database.

  Conditions: The symptom is observed with learned inside BGP prefixes.

  Workaround: There is no workaround.

- CSCty37445

  Symptoms: A DMVPN hub router with a spoke which is an EIGRP neighbor. The spoke receives a subnet from hub and then advertises it back to the hub, bypassing split horizon.

  Conditions: The symptom is observed when on the spoke you have a **distribute list route-map** command setting tags.

  Workaround: Once you remove that command EIGRP works normally.

- CSCty43582

  Symptoms: The **port-channel load-balance-hash-algorithm** CLI is not saved properly in the running-configuration.

  Conditions: The symptom is observed when the hash algorithm chosen is one of src-ip, dst-ip, or src-dst-ip.

  Workaround: There is no workaround.

- CSCty58300

  Cisco IOS Software contains a vulnerability in the Border Gateway Protocol (BGP) routing protocol feature.

  The vulnerability can be triggered when the router receives a malformed attribute from a peer on an existing BGP session.

  Successful exploitation of this vulnerability can cause all BGP sessions to reset. Repeated exploitation may result in an inability to route packets to BGP neighbors during reconvergence times.

Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability. This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-bgp

- CSCty58656

  Symptoms: A Cisco 7600 series router with ES+ module may crash.

  Conditions: The symptom is observed with the QoS policy map that has a name hash that is same as an existing policy used by the ES+ module and configuring a child policy or adding a child policy that is already in use.

  Workaround: Do not call a child policy map.

- CSCty60467

  Symptoms: SSM ID leak issues or SSM stats show unprovisioned segment counters. The leak can be observed with the command **show ssm stats**. Look for the following in the output:

```
Segment States Counters
  Type            Class           State           Count
  IP-SIP          SSS             Unprov          1050  <<< the count indicates the
IDs are getting leaked.
```

  Alarm: Counter reaches 1 Million: indicates you may be nearing ID exhaust state.

  Conditions: The symptom is observed with the following steps:

  1. Configure “ip dhcp ping packets 10” on an ISG.
  2. Initiate an L2-connected ISG DHCP session by triggering DHCP discover from the client.
  3. Start TCP traffic from the client immediately.
  4. The issue can be observed commonly on high CPS (greater than best practice).
  5. Observed in Cisco IOS XE Release 3.2 and XE 3.5.

  Workaround: Configuring “ip dhcp ping packets 0” will bring down the rate of SSM ID leak.

Resolved Caveats—Cisco IOS Release 15.2(1)S1

Cisco IOS Release 15.2(1)S1 is a rebuild release for Cisco IOS Release 15.2(1)S. The caveats in this section are resolved in Cisco IOS Release 15.2(1)S1 but may be open in previous Cisco IOS releases.

- CSCee38838

  Symptoms: A crashdump may occur during a two-call-per-second load test on a gateway, and the gateway may reload.

  Conditions: This symptom is observed on a Cisco 3745 that runs Cisco IOS Release 12.3(7)T and that functions as a gateway when you run a two-call-per-second load test that uses H.323, VXML, and HTTP. The crash occurs after approximately 200,000 calls.

  Workaround: There is no workaround.

- CSCsb53810

  Symptoms: A Cisco Catalyst 6500 series switch may not block traffic, which is supposed to be denied by an outbound ACL on a VLAN interface.

  Conditions: This issue is under investigation.

  Workaround: Reload the switch.

- CSCsg48725

  Symptoms: A TLB exception may occur on a Cisco platform that functions as a PE router in an MPLS environment, and the following error message may be generated:

  ```
  TLB (load or instruction fetch) exception, CPU signal 10 (BadVaddr : DEADBEF3)
  ```

  Conditions: This symptom is observed on a Cisco platform when TACACs accounting and authorization is enabled and when the TACACs server is reachable through the global routing table.

  Workaround: Disable AAA. If this not an option, there is no workaround.

- CSCtg57657

  Symptoms: A router is crashing at dhcp function.

  Conditions: This issue has been seen on a Cisco 7206VXR router that is running Cisco IOS Release 12.4(22)T3.

  Workaround: There is no workaround.

- CSCtg58029

  Symptoms: After switchover, aaa_acct_session_id iss not issued to new sessions.

  Conditions: This symptom occurs only after switchover.

  Workaround: There is no workaround.

- CSCtj33003

  A vulnerability exists in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause an affected device to reload. Affected devices must be configured to process SIP messages and for pass-through of Session Description Protocol (SDP) for this vulnerability to be exploitable.

  Cisco has released free software updates that address this vulnerability. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerability.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-sip

- CSCtj64807

  Symptoms: Router crashes while issuing the **show vlans dot1q internal** command.

  Conditions: The symptom is observed with the following conditions:

  1. One QinQ subinterface configured with inner VLAN as “any”.
  2. More than 32 QinQ subinterfaces configured with same outer VLAN.
  3. All subinterfaces are removed except subinterface configured with “any” inner VLAN.

  Workaround 1: For any Cisco 10000 series router which has had its first crash on any subinterface if the outer VLAN has second-dot1q VLAN as only “any”, immediately delete the sub-interface and recreate it. Then add a dummy VLAN/sub-interface to this outer VLAN.

  Workaround 2: On any outer VLAN (in array state) if they have less than 5 inner VLANs, add a dummy VLAN/subinterface.

  Workaround 3: For any Cisco 10000 series router which has not had a crash but has subinterface/outer VLAN with second-dot1q VLAN as only “any” and active sessions, add a dummy VLAN/sub-interface to this outer (tree state) VLAN.

- CSCtk00181

  Symptoms: Password aging with crypto configuration fails.

Conditions: The symptom is observed when Windows AD is set with “Password expires on next log on” and the VPN client is initiating a call to NAS. NAS does not prompt for a new password and instead gives an Auth failure.

Workaround: There is no workaround.

- CSCtk62763

  Symptoms: A Cisco 7600 router equipped with multiple DFC line cards may experience an unexpected reload because of increased IGMP activity.

  Conditions: This symptom is observed when IGMP joins and leaves (OIF churn) at approximately 160pps or more on DFCs with around 600 mroutes that have SVIs as OIFs.

  Workaround: There is no workaround.

- CSCtn02208

  Symptoms: Old PerUser ACL is not removed on applying new ACL.

  Conditions: This symptom occurs when applying a new PerUser ACL to an existing session. The old PerUser ACL that exists on the session is not removed.

  Workaround: There is no workaround.

- CSCtn40771

  Symptoms: The process ACL Header in the **show memory allocating- process totals** command output leaks memory with per-user ACLs and PPP session churn. This will also cause the SSS feature manager process in the **show process memory** command output to appear to have a leak.

  Conditions: This symptom occurs with IPv6 per-user ACLs and session churn.

  Workaround: There is no workaround.

- CSCto71671

  Symptoms: Using the **radius-server source-ports extended** command does not increase AAA requests source UDP ports as expected when Radius.ID has wrapped over, causing duplicate (dropped) requests on Radius, and forcing the Cisco ASR 1000 router to time out and retransmit.

  Conditions: This symptom is observed with a high AAA requests rate, and/or slow Radius response time, leading to a number of outstanding requests greater than 255.

  Workaround: There is no workaround.

- CSCtq59923

  Symptoms: OSPF routes in RIB point to an interface that is down/down.

  Conditions: This symptom occurs when running multiple OSPF processes with filtered mutual redistribution between the processes. Pulling the cable on one OSPF process clears the OSPF database, but the OSPF routes associated with the OSPF process from that interface still point to the down/down interface.

  Workaround: Configure “ip routing protocol purge interface”.

- CSCtr08680

  Symptoms: The following error messages are displayed on active and standby respectively:

  ```
  %ERROR: Standby doesn’t support this command BERT is running on this channel group,
  please abort bert first.
  ```

  Conditions: This symptom is observed when trying to create a channel after BERT has been started irrespective of whether BERT is running or completed.

  Workaround: There is no workaround.

- CSCtr45551

  Symptoms: T1/E1 controller does not get selected as network clock input source.

  Conditions: This symptom occurs when network-clock input source t1/e1 command is configured immediately after reload of the router or within 5 minutes from router bootup.

  Workaround: After the router reloads, wait for 5 to 6 minutes (until SETS gets initialized) and then configure T1/E1 as network clock input source.

- CSCtr47642

  Symptoms: On Cisco IOS Release 15.2(3)T that is running BGP configured as RR with multiple eGBP and iBGP non-clients and iBGP RR clients and enabling the BGP best-external feature using the **bgp additional-paths select best- external** command, a specific prefix may not have bestpath calculated for a long time.

  Conditions: The problem occurs on a certain condition of configuration of the below commands, and a few prefixes are withdrawn during the configuration time:

  1. Configure: **bgp additional-paths install** under vpnv4 AF
  2. Configure: **bgp additional-paths select best-external**

  Immediately disable backup path calculation/installation using the **no bgp additional-paths install** command.

  The problem does not appear if both of the above commands are configured with more than a 10-second delay as the commands will be executed independently in two bestpath runs instead of one.

  Workaround: Configure the **bgp additional-paths install** command and the **bgp additional-paths select best-external** command with a delay of 10 seconds.

- CSCtr88739

  Symptom 1: The routes may not get imported from the VPNv4 table to the VRF. Label mismatch may also be seen.

  Symptom 2: The routes in BGP may not get installed to RIB.

  Conditions: These symptoms are only observed with routes with the same prefix, but a different mask length. For example, X.X.X.X/32, X.X.X.X/31, X.X.X.X/30 ..... X.X.X.X/24, etc. These issues are not easily seen and are found through code walkthrough.

  For symptom 1, each update group is allocated an advertised-bit that is stored at BGP net. This issue is seen when the number of update groups increases and if BGP needs to reallocate advertised-bits. Also, this symptom is observed only with a corner case/timing issue.

  For symptom 2, if among the same routes with a different prefix length, if more specific routes (15.0.0.0/32) do not have any bestpath (for example, due to NH not being reachable or inbound policy denying the path, but path exists due to soft-reconfiguration), then even if a less specific route (15.0.0.0/24) has a valid bestpath, it may not get installed.

  Workaround for symptom 1: Remove import-route target and reconfigure route-target.

  Workaround for symptom 2: Clear ip route x.x.x.x to resolve the issue.

- CSCtr91106

  A vulnerability exists in the Cisco IOS Software that may allow a remote application or device to exceed its authorization level when authentication, authorization, and accounting (AAA) authorization is used. This vulnerability requires that the HTTP or HTTPS server is enabled on the Cisco IOS device.

  Products that are not running Cisco IOS Software are not vulnerable.

Cisco has released free software updates that address these vulnerabilities.

The HTTP server may be disabled as a workaround for the vulnerability described in this advisory.

This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai

- CSCts00341

  Symptoms: When executing a CLI that requires domain-name lookup such as **ntp server** *server.domain.com*, the command fails with the following message on the console:

  ```
  ASR1k(config)#ntp server server.domain.com         <<<    DNS is not resolved
  with dual RPs on ASR1k
  Translating "server.domain.com "...domain server (10.1.1.1) [OK]

  %ERROR: Standby doesn't support this command              ^
  % Invalid input detected at '^' marker.

  ASR1k(config)#do sh run | i ntp
  ASR1k(config)#
  ```

  Conditions: This symptom occurs on a redundant RP chassis operating in SSO mode.

  Workaround: Instead of using *hostname* in the command, specify the IP address of the host.

- CSCts13255

  Symptoms: Standby SUP720 crash is observed on the Cisco 7600 router in c7600s72033-advipservicesk9-mz.150-1.S3a.bin. This issue is random and recurring. Tracebacks are generated with the following error message:

  ```
  %CPU_MONITOR-STDBY-3-PEER_FAILED: CPU_MONITOR peer process has failed to receive
  heartbeats
  ```

  Conditions: This symptom is observed on the Cisco 7600 router with mistral based supervisors like SUP720. This issue is fairly uncommon, but affects all the versions after Cisco IOS Release 12.2(33)SRE, including Cisco IOS Releases 15.0S, 15.1S and 15.2S. This does not affect RSP 720.

  Workaround: There is no workaround.

- CSCts23882

  Symptoms: ISG calculates the radius response authenticator in CoA account- profile-status-query replies wrongly, resulting in an invalid response.

  Conditions: This symptom is observed when the CoA/WWW based session authentication is triggered via a CoA account logon using the “old” SSG command attributes.

  Workaround: Configure a fix “NAS-IP-Address” value with the **radius- server attribute 4** *x.x.x.x* command.

- CSCts38429

  The Cisco IOS Software Internet Key Exchange (IKE) feature contains a denial of service (DoS) vulnerability.

  Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-ike

- CSCts67465

  Symptoms: If you configure a frequency greater than the enhanced history interval or if the enhanced history interval is not a multiple of the frequency, the standby will reset.

  Conditions: The symptom is observed always, if the standby is configured as an SSO.

  Workaround: Remove enhanced history interval configuration before resetting the frequency.

- CSCts70790

  Symptoms: A Cisco 7600 router ceases to advertise a default route configured via "neighbor default-originate" to a VRF neighbor when the eBGP link between a Cisco 7600 router and its VRF eBGP peer flaps.

  Conditions: This symptom is observed when another VPNv4 peer (PE router) is advertising a default route to the Cisco 7600 router with the same RD but a different RT as the VRF in question. When the VRF eBGP connection flaps, the VRF default is no longer advertised.

  Workaround: Remove and re-add the **neighbor default- originate** command on the Cisco 7600 router and do a soft clear for the VRF neighbor.

- CSCts80643

  Cisco IOS Software and Cisco IOS XE Software contain a vulnerability in the RSVP feature when used on a device configured with VPN routing and forwarding (VRF) instances. This vulnerability could allow an unauthenticated, remote attacker to cause an interface wedge, which can lead to loss of connectivity, loss of routing protocol adjacency, and other denial of service (DoS) conditions. This vulnerability could be exploited repeatedly to cause an extended DoS condition.

  A workaround is available to mitigate this vulnerability.

  Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-rsvp

- CSCts85694

  Symptoms: The following error message is displayed:

  ```
  %FMANRP_ESS-3-ERREVENT: TC still has features applied. TC evsi (0x104C2E4)
  ```

  Conditions: This symptom is seen when clearing the sessions after a long time, and the memory leak increases incrementally. Leak is very slow.

  Workaround 1: Do not bring down all sessions together.

  Workaround 2: Do not tear down the sessions (scale numbers: 4k and above) together from different sources (say clearing PPP sessions and ISG sessions in lab; in field, clearing might happen via other triggers) simultaneously with no time gap between them.

  Workaround 3: Do not have accounting accuracy configured.

  Workaround 4: In this case, ISG Features are applied on TC and Session both. If we do not apply the features on the TCs, chances of this happening are less.

- CSCts97124

  Symptoms: Active crashes upon configuring a large number of TP tunnels with scale configurations either using copy paste or loading from a configuration file.

  Conditions: This symptom is not very consistent, not reproducible all the time, and happens only on adding tunnel TP configurations. The crash occurs when the protect-lsp is being configured.

  Workaround: Manually add the MPLS-TP tunnels through CLI instead of copying from a configuration or copy pasting a large configuration.

- CSCts97856

  Symptoms: PIM Assert is sent out from a router with metric [0/0], though the router has a less preferred path to reach the Source or RP.

  Conditions: This symptom occurs when an mroute is first created and its RPF lookup to the Source or RP is via BGP or Static, which involves recursive lookup, or there is no valid path to reach Source or RP. This issue only occurs in a small window in milliseconds. After the window, the metric [0/0] is corrected.

  Workaround: There is no workaround.

- CSCts97925

  Symptoms: IPv6 pings within VRF fail, where the next-hop (egress) is part of the global.

  Conditions: This symptom is observed only with IPv6, and not with IPv4.

  Workaround: Disable IPv6 CEF.

- CSCtt01056

  Symptoms: When a shell map configuration includes a parameter with no default value, that is, parameter1="", "<>", or "", then that parameter should be considered mandatory. During service activation of that shell map, if parameter1 is not provided by Radius, the activation should be rejected:

  - In case of service activation from Access-Accept, the session should be terminated.
  - In case of service activation from COA, the COA should be NAKed, and the services rolled back.

  Conditions: This symptom is observed with a shell map configuration when some parameters do not have the default value configured, such as param="", "<>", or "". This issue is seen with service activation with a missing mandatory parameter.

  Workaround: There is no workaround.

- CSCtt02313

  Symptoms: When a border router (BR) having a parent route in EIGRP is selected, “Exit Mismatch” is seen. After the RIB-MISMATCH code was integrated, RIB-MISMATCH should be seen, and the TC should be controlled by RIB-PBR, but they are not.

  Conditions: This symptom is observed when two BRs have a parent route in BGP and one BR has a parent route in EIGRP. The preferable BR is the BR which has a parent route in EIGRP. The BRs having BGP have no EIGRP configured.

  Workaround: There is no workaround.

- CSCtt02645

  Symptoms: CPUHOG is seen due to flapping of all NHRP.

  Conditions: This symptom is observed with scaling to 3k spokes on RP1.

  Workaround: There is no workaround.

- CSCtt04448

  Symptoms: There is a loss of IGMP snooping entries with a traffic drop at the pmLACP PoA boxes occurring.

  Conditions: This symptom is observed when removing/re-adding member links.

  Workaround: There is no workaround.

- CSCtt11210

  Symptoms: Routers enrolled to hierarchical PKI on different subordinate CAs, may be unable to establish tunnels using IKEv1/IKEv2.

  The “debug crypto isakmp” debugs will show that the certificate-request payload contains the issuer-name of the subordinate CA certificate, not the subject-name as it would be expected.

  Conditions: The symptom is observed when the router does not have the Root CA certificate installed.

  Workaround: Install the Root CA certificate in a separate trustpoint on all involved routers.

- CSCtt17785

  Symptoms: In the output of **show ip eigrp nei** *det*, a Cisco ASR router reports peer version for Cisco ASA devices as 0.0/0.0. Also, the Cisco ASR router does not learn any EIGRP routes redistributed on the Cisco ASA device.

  Conditions: This symptom is observed only when a Cisco ASR router is running on Cisco IOS Release 15.1(3)S and the Cisco ASA device is Cisco ASA Version 8.4(2).

  Workaround: Downgrade the Cisco ASR router to Cisco IOS Release 15.1(2)S.

- CSCtt17879

  Symptoms: The **bgp network backdoor** command does not have any effect.

  Conditions: This symptom occurs:

  - On 64-bit platform systems.
  - When the network is learned after the backdoor has been configured.

  Workaround: Unconfigure and reconfigure the network backdoor.

- CSCtt26643

  Symptoms: A Cisco ASR 1006 router that is running Cisco IOS Release 15.1(2)S2 or Cisco IOS Release 15.1(3)S0a crashes with Signal 11.

  Conditions: This symptom is observed on a Cisco ASR 1006 router that is running the asr1000rp1-adventerprisek9.03.04.00a.S.151-3.S0a.bin image. The **show version** command causes the “Last reload reason: Critical software exception” error.

  Workaround: There is no workaround.

- CSCtt28703

  Symptoms: VPN client with RSA-SIG can access a profile where the CA trustpoint is not anchored.

  Conditions: This symptom is seen with the use of RSA-SIG.

  Workaround: Restrict access by using a certificate-map matching the right issuer.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 3.5/3: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:S/C:P/I:N/A:N/E:POC/RL:W/RC:C No CVE ID has been assigned to this issue. Additional information on Cisco’s security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtt29615

  Symptoms: Any CLI command issued under af-interface mode in EIGRP router may lead to router crash.

  Conditions: This problem is observed in a Cisco router that is running Cisco IOS Release 15.2(1)S.

Workaround: There is no workaround.

- CSCtt31634

  Symptoms: Traffic drops.

  Conditions: This symptom occurs when the hw-module reloads the IM on active and posts which switchover is performed.

  Workaround: After switchover, use the **hw-module subslot reload** command to recover from the problematic state, and traffic will resume.

- CSCtt32165

  Symptoms: The Cisco Unified Border Element Enterprise on the Cisco ASR 1000 series router can fail a call with cause 47 immediately after the call connects.

  Conditions: This symptom is observed with a sufficient call volume and a call flow that redirects many calls. The Cisco ASR router can fail to provision the forwarding plane for the new call due a race condition where a prior call is not completely cleaned up on the forwarding plane before trying to use the same structure again.

  The **show voice fpi stats** command output indicates that a failure has occurred if the last column is greater than zero. For example:

  show voip fpi stats | include provisn rsp

  provisn rsp 0 32790 15

  Workaround: There is no workaround. However, Cisco IOS Release 3.4.1 is less impacted by these call failures due to a resolution of defect CSCts20058. Upgrade to Cisco IOS Release 3.4.1 until such time as this defect is resolved. In a fully redundant Cisco ASR 1006 router, you can failover the ESP slots to clear the hung entries in the forwarding plane. Other platforms will require a reload.

- CSCtt43843

  Symptoms: After reloading aggregator, PPPoE recovery is not occurring even after unshutting the dialer interface.

  Conditions: This symptom is occurring with a Cisco 7200 platform that is loaded with the Cisco IOS Interim Release 15.2(1.14)T0.1 image.

  Workaround: There is no workaround.

- CSCtt45536

  Symptoms: “FlowVar- Chunk malloc failed” messages are seen and this may be accompanied by slow console response.

  Conditions: The symptom is observed when a mix of IPv4 and IPv6 traffic is going through the router configured with QoS, VM, etc.

  Workaround: There is no workaround.

- CSCtt45654

  Symptoms: In a DVTI IPSec + NAT-t scaling case, when doing session flapping continually, several Virtual-Access interfaces are “protocol down” and are not deleted.

  Conditions: This symptom can be observed in a DVTI IPSec + NAT-t scenario when session flapping is done in the spoke side.

  Workaround: There is no workaround.

- CSCtt70585

  Symptoms: IPv6 traffic is not flowing.

Conditions: This symptom is seen with IPSec v6 tunnels.

Workaround: There is no workaround.

- CSCtt95846

  Symptoms: Changing the encapsulation of an Ethernet service instance which is set up for local switching to default encapsulation may cause an error in setting up switching, resulting in an inability to switch packets.

  ```
  PE1#show running-config | include local
  connect local Ethernet0/0 1 Ethernet1/0 1
  PE1#configure terminal
  ```

  Enter configuration commands, one per line. End with CNTL/Z.

  ```
  PE1(config)#interface Ethernet0/0
  PE1(config-if)#service instance 1 ethernet
  PE1(config-if-srv)#encapsulation default
  PE1(config-if-srv)#end
  PE1#show ssm id
  SSM Status: No switches
  ```

  Conditions: This symptom is observed if **no aaa new-model** is configured.

  Workaround: Unconfigure the local switching connection before changing the encapsulation of the service instance, then reconfigure the connection.

- CSCtu01172

  Symptoms: The Cisco ASR 1000 series router without an actual redundant router may crash when configured for CUBE HA based on the document "Cisco Unified Border Element High Availability(HA) on ASR platform Configuration Example."

  Conditions: This symptom is observed with the Cisco ASR 1000 series router.

  Workaround: Remove the application configuration, that is, "no application redundancy".

- CSCtu02286

  Symptoms: With pim-bidir in MVPN core, MVPN traffic might not flow if a PE is also a rendezvous point (RP) for the pim-bidir in core.

  Conditions: This symptom occurs with pim-bidir in MVPN core.

  Workaround: Use non pim-bidir modes.

- CSCtu12574

  Symptoms: The **show buffers** command output displays:

  1. Increased missed counters on EOBC buffers.
  2. Medium buffer leak.

  ```
  Router#sh buffers
  Buffer elements:
       779 in free list (500 max allowed)
       1582067902 hits, 0 misses, 619 created

  Interface buffer pools:
  ....
  Medium buffers, 256 bytes (total 89647, permanent 3000, peak 89647 @
  ```

```
00:01:17):
     273 in free list (64 min, 3000 max allowed)

EOBC0/0 buffers, 1524 bytes (total 2400, permanent 2400):
     0 in free list (0 min, 2400 max allowed)
     2400 hits, 161836 fallbacks
     1200 max cache size, 129 in cache
....
```

The leak is small. It is a leak of 64 bytes per buffer that is leaked, and the leak appears to be very slow.

Conditions: The **show buffers old** command output displays some buffers hanging on the EOBC buffers list for a really long time, such as weeks or even more. This issue is a corner case and the buffer leak rate is slow.

This DDTS tracks the leak specific to IPC application l3-mgr.

From the **show buffers old pack** output:

```
0A9C4ED8: 00200000 02150000 0202080B 01000000  . ............. --> IPC Header
0A9C4EE8: 97D49493 00081608 03493E4D 06927C9A  .T.......I>M..|.
0A9C4EF8: 00520002 00000000 00000000 000000    .R.............  --> ICC Header
            --  --
```

And, if we look at the ICC header at the underscored items 00520002:

```
0052   (represents the class name)             ----> L3_MGR_DSS_REQUESTS
0002   (represents the request name)          ----> L3_MGR_MLS_REQ
```

Workaround: Reload the system.

- CSCtu18201

  Symptoms: A Cisco router crashes due to low stack with the following display:

  ```
  %SYS-6-STACKLOW: Stack for process BGP Event running low, 0/6000
  ```

  Conditions: This symptom occurs with a low stack.

  Workaround: There is no workaround.

- CSCtu19450

  Symptoms: A system that is running Cisco IOS may reload when a large number of routes are simultaneously deleted at the same time that the inetCidrRouteTable is being walked.

  Conditions: This symptom is only likely to happen when there are large numbers of interfaces and routes within the system, and when large numbers of routes are being rapidly removed, and the system is loaded, at the same time that the inetCidrRouteTable is being walked.

  Routes may be deleted from the system both directly, and also indirectly for example, when a significant number of PPPoE sessions are removed.

  Workaround: Avoid walking the inetCidrRouteTable while significant numbers of routes are being removed from the routing system.

- CSCtu29729

  Symptoms: An attempt to create a frame-relay sub-interface on a serial interface may result in error. The serial interface can then not be configured as a frame-relay interface.

Conditions: This symptom is observed when a serial interface is configured as a multi-link frame-relay bundle link with a subsequent attempt to change the configuration to a frame-relay interface.

Workaround: There is no workaround.

- CSCtu31340

  Symptoms: The **show sip call called-number** crashes the router.

  Conditions: This symptom is observed when the call SIP state is DISCONNECT.

  Workaround: There is no workaround.

- CSCtu33956

  Symptoms: The dialer with PPP encapsulation is seen when DSL is the WAN interface. L2PT does not work.

  Conditions: This symptom is observed under the following conditions:

  - The PPPoE dialer client needs to be configured on the physical SHDSL interface.
  - The GRE tunnel destination interface should point to the dialer interface.
  - The MPLS pseudowire should go over the tunnel interface.
  - After the PPPoE session is set up, the GRE tunnel traffic gets dropped at the peer end of the PPPoE session.

  Workaround: There is no workaround.

- CSCtu35713

  Symptoms: IPv4 address saving: IPCP state change does not trigger session accounting update.

  Conditions: This symptom is observed under the following conditions:

  1. Enable IPv4 address saving on BRAS.
  2. Configure AAA periodic accounting using the **aaa accounting update periodic** *time in mins* command.
  3. Initiate IPCP negotiation from the client.
  4. After IPCP negotiation is complete, BRAS does not send an interim accounting update containing IPv4 address save VSA and the new IPv4 address assigned to the client.

  Workaround: Configure AAA accounting with the **aaa accounting update newinfo periodic** *time in mins*.

- CSCtu36674

  Symptoms: Packets stop being transmitted in the output direction on L2transport local connect PVC on the ATM interface.

  Conditions: This symptom is observed when local connect is configured and a new ATM subinterface is configured on the same ATM main interface as the one with local connect PVC.

  Workaround 1: Perform shut/no shut on local connect.

  Workaround 2: Unconfigure/reconfigure local connect.

- CSCtu39819

  Symptoms: The Cisco ASR 1002 router configured as an RSVPAgent for Cisco Unified Communication Manager crashes under extended traffic.

Conditions: This symptom is observed on a Cisco ASR 1002 router configured as an RSVPAgent for CUCM End-to-End RSVP feature. The router crashes after 45 minutes of traffic run with 150 simultaneous up MTP-RSVP sessions.

The asr1000rp1-adventerprisek9.03.04.00a.S.151-3.S0a.bin image is used.

Workaround: There is no workaround.

- CSCtu41137

  Symptoms: IOSD Core@fib_table_find_exact_match is seen while unconfiguring tunnel interface.

  Conditions: The core is observed while doing unconfiguration.

  Workaround: There is no workaround.

- CSCtu43731

  Symptoms: On an RP1, RP switchover causes an RP reset.

  Conditions: This symptom is observed with RP switchover under the following conditions:

  - The router must be an RP1
  - The configuration of Flexible NetFlow (FNF) or equivalent must be applied to 4000 or more interfaces. In this case of testing, 4000 DVTI interfaces were in use.

  An equivalent of FNF is AVC or passive Video Monitoring. That is, those configured on a comparable number of interfaces will have the same effect.

  Workaround 1: Prior to doing a controlled switchover, such as ISSU, deconfigure FNF from some interfaces to take it well under the threshold at which the issue can occur.

  Workaround 2: Do not enable FNF monitoring.

- CSCtu87383

  Symptoms: CFM global configuration does not get applied to LC slots that are greater than 20 on LC OIR. This problem is specific to CPT platform where satellite box slot numbers go from 36 to 55.

  Conditions: This symptom occurs with satellite box OIR.

  Workaround: Disable and reenable CFM global configuration.

- CSCtu89771

  Symptoms: The Cisco ASR 1000 series router RP crashes while unconfiguring or removing the **no area 0 authentication ipsec spi <>** command.

  This behavior is not observed at the first few instances of unconfiguring the above CLI.

  Conditions: This symptom is observed only in automated tests where unconfiguring the authentication with the above CLI is executed multiple (approximately 3) times on the Cisco ASR 1000 series router. This leads to the RP crashes.

  Workaround: There is no workaround.

- CSCtu92213

  Symptoms: Console is stuck and irresponsive.

  Conditions: This symptom is seen when EVC with QoS is scaled, and traffic is being sent through many policy-maps with a large queue limit.

  Workaround: Configure a smaller queue-limit under each class on all egress policy-maps in use.

- CSCtu92289

  Symptoms: VCCV BFD on PW HE (routed pseudowire) is not working.

Conditions: VCCV BFD is not working on routed pseudowire but works fine on scalable EoMPLS.

Workaround: There is no workaround.

- CSCtu92673

  Symptoms: L2TP tunnels are not getting established with PPPoE relay.

  Conditions: This issue is seen on a Cisco 7200 router that is running Cisco IOS Interim Release 15.2(01.12)S.

  Workaround: There is no workaround.

- CSCtv19529

  Symptoms: Router crashes on unconfiguring the last available DHCP pool. Crash will also be seen on running the **no service dhcp**.

  Conditions: This crash can happen only if “DHCP Client” process is running on the router along with the DHCP relay processes (DHCPD Receive, DHCPD Timer, DHCPD Database).

  The client process can be started:

  1. from an DHCP autoinstall attempt during router startup (with no nvram config).
  2. if the **ip address dhcp** is run on one of the interfaces. 3) if the router was used for DHCP proxy client operations.

  The relay processes are started when a DHCP pool is created by the **ip dhcp pool** *pool* command.

  Workaround: Have a dummy DHCP pool created using the **ip dhcp pool** *dummy_pool* command, and never delete this pool. Other pools can be created and removed at will, the *dummy_pool* should not be removed. In addition, do not execute the **no service dhcp** command.

- CSCtw43640

  Symptoms: An IP ping/CFM session through Handoff FPGA fails.

  Conditions: This symptom is observed after switchover with IM in slot 5.

  Workaround: There is no workaround.

- CSCtw45055

  Symptom: A Cisco ASR router may experience a crash in the BGP Scheduler due to a segmentation fault if BGP dynamic neighbors have been recently deleted due to link flap. For example:

```
%BGP-5-ADJCHANGE: neighbor *X.X.X.X Up
%BGP-3-NOTIFICATION: received from neighbor *X.X.X.X (hold
time expired) x bytes
%BGP-5-ADJCHANGE: neighbor *X.X.X.X Down BGP Notification
received
%BGP_SESSION-5-ADJCHANGE: neighbor *X.X.X.X IPv4 Unicast
topology base removed from session  Neighbor deleted
%BGP_SESSION-5-ADJCHANGE: neighbor *X.X.X.X IPv4 Unicast
topology base removed from session  Neighbor deleted
%BGP-5-ADJCHANGE: neighbor *X.X.X.X Up

Exception to IOS Thread:
Frame pointer 0x3BE784F8, PC = 0x104109AC

UNIX-EXT-SIGNAL: Segmentation fault(11), Process = BGP Scheduler
```

The scheduler process will attempt to reference a freed data structure, causing the system to crash.

Conditions: This symptom is observed when the Cisco ASR router experiences recent dynamic neighbor removals, either because of flapping or potentially by manual removal. This issue only happens when BGP dynamic neighbor is configured.

Workaround: There is no workaround.

- CSCtw45168

  Symptoms: DTMF interworking fails when MTP is used to convert OOB---RFC2833 and vice versa.

  Conditions: This symptom is observed when MTP is used to convert OOB---RFC2833 and vice versa. This issue is seen starting from Cisco IOS XE Release 3.2S. Cisco IOS XE Release 3.1S should work fine.

  Workaround: There is no workaround.

- CSCtw46625

  Symptoms: The QL value is DNU although the four least significant bits of SSM S1 byte are pointing to PRC (bits: 0010).

  Conditions: This symptom is observed when SSM S1 byte is received on CEoPs SPAs or channelized SPA-1XCHSTM1/OC3.

  Workaround: Force the QL PRC value by executing the following command:

  ```
  network-clock quality-level rx QL-PRC controller SONET 1/2/0
  ```

- CSCtw48209

  Symptoms: High-end Cisco devices running Cisco IOS are likely affected. Active features at the time of this problem manifestation include any condition that leads to RSVP SNMP notification generation in Cisco IOS. BGP/MPLS TE instability, leading to changes to RSVP session status change, is observed in a test scenario while running Cisco IOS Release SXI4 and Cisco IOS Release SXI7. The issue is not reproducible consistently.

  Conditions: This symptom is observed with Cisco IOS Release 12.2(33)SXI4, Cisco IOS Release 12.2(33)SXI7, Cisco IOS Release 12.2SR, Cisco IOS Release 12.2SX, and Cisco IOS Release 15S.

  Workaround: Disable RSVP notification using the **no snmp-server enable traps rsvp** command.

- CSCtw50277

  Symptoms: Policy manager is getting apply config failed on standby while policy is activated through CoA. The router later crashes in policy code.

  Conditions: This symptom is seen when CoA activated policy install is failing on standby RP.

  Workaround: There is no workaround.

- CSCtw51134

  Symptoms: IMA interface configuration is lost post stateful switchover (SSO).

  Conditions: This symptom occurs after SSO.

  Workaround: There is no workaround.

- CSCtw52504

  Symptoms: WAN mode is not enabled on 10G IMs.

  Conditions: This symptom is observed when a 10G IM operates in LAN mode by default. The WAN mode supports SONET alarms to interface with SONET-like equipments.

  Workaround: There is no workaround.

- CSCtw52610

  Symptoms: Some of the TCes will switch to fallback interface, and the remaining TCes on primary interface will be in OOP state.

  Conditions: The issue is seen when primary link is considered OOP based on utilization despite using the **no resolve utilization** command.

  Workaround: There is no workaround if PfR policy with and without utilization is needed. If PfR policy based on utilization is not needed, then configure “max-xmit-utilization percentage 100”.

- CSCtw58395

  Symptoms: When executing the **clear crypto session** command in 4k FlexVPN cases, the memory of crypto IKEv2 is increasing.

  Conditions: This symptom is observed when the session is flapping.

  Workaround: There is no workaround.

- CSCtw58586

  Symptoms: IKEv2 CLI configuration currently requires to manually link the crypto IKEv2 profile default to the crypto IPSec profile default. This enhancement request will change the behavior and create an automatic anchorage.

  Conditions: This symptom is seen in IKEv2 usage.

  Workaround: There is no workaround.

- CSCtw64040

  Symptoms: Crash due to MPLS, which appears to be associated with load- balancing.

  Conditions: This symptom occurs when MPLS is configured.

  Workaround: There is no workaround.

- CSCtw68745

  Symptoms: A Cisco ASR 1000 router acting as DHPCv6 Relay standby crashes when there is high DHCPv6 incoming traffic and if DHCPv6 relay is configured on many (around 5k) interfaces.

  Conditions: This symptom occurs when there is high DHCPv6 incoming traffic and if DHCPv6 relay is configured on many (around 5k) interfaces.

  Workaround: There is no workaround.

- CSCtw73551

  Symptoms: Standby RP can crash due to a memory leak processing calls. The crashinfo file identifies the process as follows:

  ```
  UNIX-EXT-SIGNAL: Aborted(6), Process = Check heaps
  ```

  Conditions: This symptom is seen on CUBE enterprise on the Cisco ASR 1000 series router with redundant RPs and approximately 2.4 million calls processed from last start of the standby RP.

  Workaround: There is no workaround.

- CSCtw76044

  Symptoms: Need IGMP/MLD information to make IGMP/MLP snooping work.

  Conditions: The symptom is observed under all conditions.

  Workaround: There is no workaround.

- CSCtw79579

  Symptoms: Standby fails to be in standby HOT state after reload.

Conditions: This symptom is seen after removal of an IM and doing RSP stateful switchover (SSO) and then trying to bring up the standby RSP.

Workaround: There is no workaround.

- CSCtw85883

  Symptoms: The error "ace_add_one_map failed" occurs while adding an ACE to a crypto ACL that is being used by a crypto map.

  Conditions: This symptom is observed when the crypto map is applied to an interface and the crypto ACL being modified is also in use.

  Workaround: Remove the crypto map and apply the ACL changes to avoid the error.

- CSCtw94319

  Symptoms: Crash is seen at dhcpd_forward_request.

  Conditions: This symptom is seen when the IP DHCP Relay feature is used in scaled configuration.

  Workaround: Remove the **ip dhcp relay information option vpn** command, if possible. Otherwise, there is no workaround.

- CSCtw99290

  Symptoms: The source or destination group-address gets replaced by another valid group-address.

  Conditions: The symptom is observed during the NVGEN process if it suspends (for example: when having a huge configuration generating the running-config for local viewing or during the saving of the configuration or during the bulk sync with the standby and the NVGEN process suspends). The global shared buffer having the address gets overwritten by another process before the NVGEN completes.

  Workaround: There is no workaround.

- CSCtw99877

  Symptoms: IOMD process on 10G IM crashes upon booting standby.

  Conditions: This symptom is observed when the interface state is down on active.

  Workaround: There is no workaround.

- CSCtx01604

  Symptoms: Cisco IOS might crash on some 64-bit platform if CNS ID is configured as the IP address of some active network interface, and this IP address is changed in the middle of some critical CNS feature operations.

  Conditions: This problem presents a bad planning of bootstrapping a Cisco IOS device via an unreliable network interface whose IP address could be changed any time during the bootstrapping.

  Workaround: Do not use any dynamic network interface IP address as CNS ID.

- CSCtx05942

  Symptoms: The session to the service module from the Supervisor Fails. This can happen with SAMI, NAM, NAM-2 etc. modules.

  For example, if the SAMI card is in Slot 2, the **session slot** *2* **processor 0** command fails to create a telnet session and fails to give out the following messages:

  ```
  SUP#session slot 2 proc 3
  The default escape character is Ctrl-^, then x.
  You can also type 'exit' at the remote prompt to end the session
  Trying 127.0.0.33 ...
  ```

```
% Connection timed out; remote host not responding
```

Conditions: This symptom occurs with Cisco IOS Release 15.2(1)S release. It is not observed with Cisco IOS Release 15.1(3)S1 or lower version.

Workaround: Downgrading the Supervisor to Cisco IOS Release 15.1(3)S1 or lower version resolves this issue.

- CSCtx09614

  Symptoms: With the preconfigured ATM configuration, the standby RSP does not boot up.

  Conditions: This symptom is observed when one of the RSPs is up and the running configuration has the ATM configuration under the controller.

  Workaround: There is no workaround. Without an ATM configuration, the standby RSP goes to standby mode.

- CSCtx21206

  Symptoms: BFDv6 hardware offloaded sessions do not come up with all IPv6 source addresses.

  Conditions: This symptom is observed with interface source IPv6 addresses that have some specific bits in the 6th byte set like 6001:1:C::1..

  Workaround: Reconfigure the source IPv6 addresses to some address that will not match the criteria mentioned in the above Conditions.

- CSCtx29543

  Symptoms: A Cisco router may crash when an IPv4 default route update occurs or when doing the **show ip route** command.

  Conditions: This symptom occurs under the following conditions:

  1. At least one IPv4 route associated with each of the 23 possible supernet mask lengths exist.
  2. A default route exists.
  3. All routes corresponding to one of the 23 possible supernet mask lengths are removed.

  The router may now crash when doing **show ip route** command or when default route is updated.

  Workaround: There are two possible workarounds:

  1. Insure that not all 23 supernet mask lengths are populated by doing route filtering.
  2. If workaround #1 is not possible, then insure that at least one supernet route for all possible mask lengths exists at all times, for example by configuring summary routes that do not interfere with normal operation.

- CSCtx63034

  Symptoms: After a Cisco 7600 router is powered by PWR-2500-DC, PWR-4000-DC or PWR-6000-DC to Cisco IOS Release 15.2(1)S, the router logs the following error messages:

  ```
  %C7600_PWR-SP-3-PSUNKNOWN: Unknown power supply in slot 1 (idprom read
  failed).
  %OIR-SP-6-INSPS: Power supply inserted in slot 1
  %C7600_PWR-SP-4-PSOK: power supply 1 turned on.
  ```

  The **show power** command shows that the power supply only provides 919W. Most of the line cards cannot be powered up.

  Conditions: This symptom is observed in Cisco IOS Release 15.2(1)S only. The problem does not occur in Cisco IOS Release 15.1(3)S1. PWR-4000-DC and PWR-6000-DC are confirmed to be affected by this problem.

Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 15.2(1)S

This section describes possibly unexpected behavior by Cisco IOS Release 15.2(1)S. All the caveats listed in this section are open in Cisco IOS Release 15.2(1)S. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCtg68047

  Symptoms: The router reloads.

  Conditions: The symptom is observed if several tunnels with crypto protection are being shut down on the router console and the **show crypto sessions** command is executed simultaneously on another terminal connected to the router.

  Workaround: Wait until the tunnels are shut down before issuing the show command.

- CSCtj58706

  Symptoms: On executing ISSU runversion, the standby RP reloads multiple times before reaching hot-standby.

  Conditions: This symptom is observed during ISSU upgrade/downgrade with the iso1-iso2 image. This issue is seen with scaled configuration of 7000 L2VPN, 300 BGP, 300 EIGRP, and 8000 EVC sessions.

  Workaround: There is no workaround.

- CSCtk62763

  Symptoms: A Cisco 7600 router equipped with multiple DFC line cards may experience an unexpected reload because of increased IGMP activity.

  Conditions: This symptom is observed when IGMP joins and leaves (OIF churn) at approximately 160pps or more on DFCs with around 600 mroutes that have SVIs as OIFs.

  Workaround: There is no workaround.

- CSCtn83900

  Symptoms: After performing legacy mode or native mode subpackage ISSU with flexible NetFlow configured, the interface to monitor bindings may not be present on the newly active RP.

  Conditions: This symptom is observed when a legacy mode or native mode subpackage ISSU is performed with FNF configured.

  Workaround: Remove the FNF monitors prior to the subpackage ISSU. Add the monitors back to the interface configuration after the upgrade. Alternatively, use super-package ISSU, which does not have this limitation.

- CSCto71671

  Symptoms: Using the **radius-server source-ports extended** command does not increase AAA requests source UDP ports as expected when Radius.ID has wrapped over, causing duplicate (dropped) requests on Radius, and forcing the Cisco ASR 1000 router to time out and retransmit.

  Conditions: This symptom is observed with a high AAA requests rate, and/or slow Radius response time, leading to a number of outstanding requests greater than 255.

  Workaround: There is no workaround.

- CSCtq80891

  Symptoms: The Processor Pool for the Cisco IOS memory is used up with most of the buffers in the "IPv6 PIM input queue".

  Conditions: This symptom is observed with the following topology:

  IXIA [IPv6 Mcast Source] ------ TR1 (ASR1k) ------|500 IPv6 over IPv4 GRE

  Tunnels | ------ UUT (ASR1k) [IPv6 RP] ------ |500 IPv6 over IPv4 GRE

  Tunnels | ------ TR2 (7200) ------ IXIA [IPv6 Mcast MLD Hosts]

  - 500 IPv6 Sources sending Mcast traffic to 500 IPv6 Mcast groups
  - 500 PIM-RP on UUT
  - 500 PIM-RP Acl to make sure 1 Mcast-group/Tunnel
  - The GRE tunnels could be configured with tunnel protection or not.

  The reproduce procedure is as follows:

  1. Copy configurations (IPv6 over IPv4 GRE Tunnel Protections and IPv6 Mcast included) to TR1, TR2, and UUT.
  2. Launch Mcast traffic (500M) on IXIA.
  3. Hit the Cisco IOS memory depletion issue on UUT.

  Workaround: Configure the punt policer for PIM register packets as follows:

  platform punt-policer 55 limit-number
  platform punt-policer 55 limit-number high

  The limit-number above is a number between 1000-2000.

- CSCtr80274

  Symptoms: CISCO-LICENSE-MGMT-MIB does not populate.

  Conditions: This symptom occurs when the required license is installed on the Cisco ASR 903 router, but the SNMP query does not return any value.

```
NMS-RACK1-RUDY-1#show license
Index 1 Feature: metroaggrservices
        Period left: Life time
        License Type: Permanent
        License State: Active, In Use
        License Count: Non-Counted
        License Priority: Medium
Index 2 Feature: metroipservices
        Period left: 8  weeks 4  days
        License Type: Evaluation
        License State: Active, Not in Use, EULA not accepted
        License Count: Non-Counted
        License Priority: None
Index 3 Feature: metroservices
        Period left: 8  weeks 4  days
        License Type: Evaluation
        License State: Active, Not in Use, EULA not accepted
        License Count: Non-Counted
        License Priority: None
sw-mrrbu-nms-2:2> getmany 3.3.2.11 ciscoLicenseMgmtMIB
sw-mrrbu-nms-2:3>
```

Workaround: There is no workaround.

- CSCts05124

  Symptoms: A zero-byte crash file is generated upon a crash with TREX SPA.

  Conditions: This symptom is observed with a test crash on a SIP-400 line card with TREX SPA inserted.

  Workaround: There is no workaround.

- CSCts11715

  Symptoms: After shutting the tunnel, ISAKMP does not turn OFF.

  Conditions: This symptom is observed in a scaled DMVPN setup with more than 1k spokes.

  Workaround: There is no workaround.

- CSCts12499

  Symptoms: SPA firmware crash at one bay leads to SPA crash in another bay.

  Conditions: This symptom is observed when “test crash cema” is executed from the SPA console. leading to the SPA in the other bay to reload. Also, the crashinfo is not present in the RP disk.

  Workaround: There is no workaround.

- CSCts13255

  Symptoms: Standby SUP crash is observed on the Cisco 7609 router after upgrade to c7600s72033-advipservicesk9-mz.150-1.S3a.bin. This issue is random and recurring. Tracebacks are generated with the following error message:

  ```
  %CPU_MONITOR-STDBY-3-PEER_FAILED: CPU_MONITOR peer process has failed to receive
  heartbeats
  ```

  Conditions: This symptom is observed on the Cisco 7609 router after upgrade to c7600s72033-advipservicesk9-mz.150-1.S3a.bin. This issue is also seen with Cisco IOS Release 12.2(33)SRE.

  Workaround: There is no workaround.

- CSCts20632

  Symptoms: If subclassification and classification for the protocol is configured in a different class map, configuring the port map and assigning a different port (other than 80) for HTTP causes unexpected error messages to be displayed.

  Conditions: This symptom is observed when subclassification and protocol classification is configured for HTTP and a port map is configured for HTTP.

  Workaround: There is no workaround.

- CSCts47550

  Symptoms: When applying protocol attributes policy rules, traceback may be seen.

  Conditions: This symptom is not consistent and may or may not appear when applying the protocol attributes policy rules. The symptom is also not consistent with a specific protocol, but may appear with respect to different protocols.

  Workaround: There is no workaround.

- CSCts63426

  Symptoms: With 1K EoMPLS PWs, 6 percent performance drop is observed in Cisco IOS XE Release 3.5 compared to Cisco IOS XE Release 3.4 performance.

  Conditions: This symptom is observed with 1K EoMPLS PWs in Cisco IOS XE Release 3.5.

  Workaround: There is no workaround.

- CSCts63658

  Symptoms: Multicast traffic do not flow over EVCs on the port-channel.

  Conditions: This symptom is observed during router reload.

  Workaround: Reconfigure after the router reload. Configure regular EFPs before EFPs on the PC in the same BD.

- CSCts82598

  Symptoms: Incorrect IP from the NAT pool is chosen for translation, when one protocol exhausts all ports of all IPs and another protocol traffic is received.

  Conditions: This symptom occurs when one protocol (for example, TCP) exhausts all ports of all IPs in a pool, and only one IP from the pool is selected for translation, thus limiting the capacity of creating translations. This happens only when one protocol completely exhausts all ports and then another protocol traffic starts. This usually is not the case in customer environments that mostly see both TCP and UDP traffic hitting the box time.

  Workaround: There is no workaround.

- CSCts97925

  Symptoms: IPv6 pings within VRF fail, where the next-hop (egress) is part of the global.

  Conditions: This symptom is observed only with IPv6, and not with IPv4.

  Workaround: Disable IPv6 CEF.

- CSCtt01056

  Symptoms: When a shell map configuration includes a parameter with no default value, that is, parameter1="", "<>", or "", then that parameter should be considered mandatory. During service activation of that shell map, if parameter1 is not provided by Radius, the activation should be rejected:

  - In case of service activation from Access-Accept, the session should be terminated. - In case of service activation from COA, the COA should be NAKed, and the services rolled back.

  Conditions: This symptom is observed with a shell map configuration when some parameters do not have the default value configured, such as param="", "<>", or "". This issue is seen with service activation with a missing mandatory parameter.

  Workaround: There is no workaround.

- CSCtt02645

  Symptoms: CPUHOG is seen due to flapping of all NHRP.

  Conditions: This symptom is observed with scaling to 3k spokes on RP1.

  Workaround: There is no workaround.

- CSCtt04724

  Symptoms: On PPPoEoX, when activating multiple services from Access-Accept with long Cisco-SSG-Account-Info strings, if the aggregated string length exceeds the current limit of 256 characters, then the service activation fails, a traceback is seen, and the session is allowed to establish, no services will be applied in the ingress and/or egress directions.

  Conditions: This symptom is observed when the aggregated services string length exceeds the limit (256 characters).

  Workaround: The session should be terminated instead. In case of service activation from CoA, if the cumulative services string length exceeds the limit, then the last CoA should be NAKed, and the services rolled back to the previous state.

- CSCtt11210

  Symptoms: Routers enrolled to hierarchical PKI on different subordinate CAs, may be unable to establish tunnels using IKEv1/IKEv2.

  The “debug crypto isakmp” debugs will show that the certificate-request payload contains the issuer-name of the subordinate CA certificate, not the subject-name as it would be expected.

  Conditions: The symptom is observed when the router does not have the Root CA certificate installed.

  Workaround: Install the Root CA certificate in a separate trustpoint on all involved routers.

- CSCtt11558

  Symptoms: The Cisco ASR 1000 router displays the “INVALID_GPM_ACCESS” error message due to invalid GPM load. This may cause unexpected Embedded Services Processors (ESP) reload.

  Conditions: This symptom is observed when a small packet is sent from a BDI interface to an Ethernet service instance with either the **rewrite egress tag** command or the **rewrite ingress tag** command with the **symmetric** option present.

  Workaround: There is no workaround.

- CSCtt21257

  Symptoms: After a reload or switchover, all interfaces on one or more IMs may be down down. The state of the IMs is “ok, active”, which is shown in the **show platform** command output.

  Conditions: This symptom is occasionally observed after a reload or a switchover.

  Workaround: Power cycle the box.

- CSCtt26532

  Symptoms: With QoS policy-map configured on a BFD interface, modifying the QoS policy-map flaps the BFD session.

  Conditions: This symptom is observed when BFD and QoS policy-maps are configured on the same interface.

  Workaround: There is no workaround.

  Further Problem Description: QoS and BFD use a common flag that gets reset and set during QoS policy-map update, causing the BFD session to flap. BFD session flap leads to the OSPF session also going down.

- CSCtt33937

  Symptoms: Configure port 7 on the Gigabit IM as a port to forward traffic using IP routing.

  ```
  config t
  
  interface g0/0/7
  ```

```
ip address 10.0.0.1 255.255.255.0
```

Conditions: This symptom is observed when traffic is flowing well. When you perform a switchover, and once the standby becomes the new active, the traffic does not hit the ingress counter of the interface itself. On checking the links status using the registers, the SGMI link appears out of sync.

Workaround: There is no workaround. Reload the box when this symptom is observed.

- CSCtt34361

  Symptoms: During a soak test with 1800 PPPoE sessions flapping with the IPv4 Saving feature enabled + per-user ACLv4 and ACLv6, there is no ISG service. After 56 iterations, one memory snapshot is taken every four iterations, that is, roughly 270 seconds per iteration. The test duration is 4 hours, with total 100800 sessions established with an average of 7cps.

  Conditions: This symptom occurs under the following conditions:

  1. No active session is there in the router.
  2. Establish 1800 PTA dual-stack sessions with per-user ACL from Radius + IPV4 Saving feature.
  3. Wait till all sessions come UP.
  4. Take a memory leak snapshot “high”.
  5. Wait for all sessions to time out on the Idle timer (no traffic).
  6. Wait for all sessions to go DOWN.
  7. Take a memory snapshot.
  8. Loop back to 1.

  Workaround: There is no workaround.

- CSCtt45654

  Symptoms: In a DVTI IPSec + NAT-t scaling case, when doing session flapping continually, several Virtual-Access interfaces are “protocol down” and are not deleted.

  Conditions: This symptom can be observed in a DVTI IPSec + NAT-t scenario when session flapping is done in the spoke side.

  Workaround: There is no workaround.

- CSCtt45801

  Symptoms: The DMVPN HUB RP crashes with the default EIGRP timer when scaling to 4k spokes.

  Conditions: This symptom occurs when scaling to 4k spokes.

  Workaround: Changing the EIGRP timer to longer may reduce the chances of a crash.

- CSCtt70133

  Symptoms: The RP resets with FlexVPN configuration.

  Conditions: This symptom is observed when using the **clear crypto session** command on the console.

  Workaround: There is no workaround.

- CSCtt70346

  Symptoms: IOMD crash is seen when running the PTP session.

  Conditions: This symptom is observed when running the PTP session for a long time. Sometimes, this issue is seen when changing PTP packet rates. This issue is seen rarely.

  Workaround: There is no workaround.

- CSCtt70498

  Symptoms: After a reload or switchover, the state of F0 or F1 may become “disconnecting” instead of “ok, active/standby”, which is shown in the **show platform** command output. As a result, the corresponding RSP does not forward traffic.

  Conditions: This symptom is occasionally observed after a reload or a switchover.

  Workaround: Power cycle the box.

- CSCtt94147

  Symptoms: Nile manager crash is observed.

  Conditions: This symptom is observed with the following conditions:

  - VPLS in the core.
  - REP in the access.
  - The access-side REP segment flaps a few times.

  Workaround: There is no workaround.

- CSCtt94566

  Symptoms: The router crashes before all sessions come up.

  Conditions: This symptom occurs before all sessions come up.

  Workaround: There is no workaround.

- CSCtt95577

  Symptoms: After creating the 994th VC on a T1/E1 IM on Rudy, the traffic flow stops. Packets get dropped on the egress on Rudy.

  Conditions: This symptom is observed when ping starts to fail on all the pre-existing VCs upon adding the 994th VC. The working is unaffected till 993 VCs.

  Workaround: Delete the 994th VC to make the pre-existing VCs forward traffic.

- CSCtt97164

  Symptoms: If the router interface is flapped, the HSRP message may be dropped by the punt/inject path.

  Conditions: This symptom is seen if the router interface is flapped.

  Workaround: Disable the inject bypass.

- CSCtt97473

  Symptoms: After a reload or switchover, the RSP may reset during bootup.

  Conditions: This symptom is observed occasionally after a reload or switchover.

  Workaround: There is no workaround.

- CSCtt98574

  Symptoms: After a reload or switchover, the state of one or more IMs may become “out of service” instead of “ok, active/standby”, which is shown in the **show platform** command output. As a result, the corresponding interfaces do not come up.

  Conditions: This symptom is occasionally observed after a reload or a switchover.

  Workaround: Power cycle the box.

- CSCtt99235

  Symptoms: After a switchover, an IOMD process crashes because it has failed to establish LIPC connection.

  Conditions: This symptom is seen occasionally after a switchover.

  Workaround: Reload the box.

- CSCtu02280

  Symptoms: When running the PTP session for more than 12 hours, PTPD may crash.

  Conditions: This symptom occurs when running the PTP session for a long time.

  Workaround: There is no workaround.

- CSCtu02476

  Symptoms: An SSO followed by a change in the xconnect MTU results in the pseudowire in the redundant RP to go down. The pseudowire in the Active RP remains up and running. A subsequent SSO results in the pseudowire to go down.

  Conditions: This symptom is observed with “encapsulation default” at that end of the pseudowire where SSO is performed. An SSO followed by a change in the MTU value, and then a subsequent SSO, causes the pseudowire to go down. This issue is also seen in a setup with redundant pseudowires, where the primary and backup pseudowires configured under the service instance do not come up after changing the MTU with SSO.

  Workaround: Execute “no xconnect” under the service instance, and then reconfigure the pseudowire with the new MTU value under the service instance.

- CSCtu03699

  Symptoms: The Nile Manager crashes.

  Conditions: This symptom is observed when reloading the TP tunnel endpoint multiple times.

  Workaround: There is no workaround.

- CSCtu12574

  Symptoms: The **show buffers** command output displays:

  1. Increased missed counters on EOBC buffers.
  2. Medium buffer leak.

  ```
  Router#sh buffers
  Buffer elements:
       779 in free list (500 max allowed)
       1582067902 hits, 0 misses, 619 created
  Interface buffer pools:
  ....
  Medium buffers, 256 bytes (total 89647, permanent 3000, peak 89647 @
  00:01:17):
       273 in free list (64 min, 3000 max allowed)
  EOBC0/0 buffers, 1524 bytes (total 2400, permanent 2400):
       0 in free list (0 min, 2400 max allowed)
       2400 hits, 161836 fallbacks
       1200 max cache size, 129 in cache
  ....
  ```

The leak is small. It is a leak of 64 bytes per buffer that is leaked, and the leak appears to be very slow.

Conditions: The **show buffers old** command output displays some buffers hanging on the EOBC buffers list for a really long time, such as weeks or even more. This issue is a corner case and the buffer leak rate is slow.

The DDTS CSCtr34960 tracks the leak specific to IPC application l3-mgr.

From the **show buffers old pack** output:

```
0A9C4ED8: 00200000 02150000 0202080B 01000000  . ..............    -----> IPC
Header
0A9C4EE8: 97D49493 00081608 03493E4D 06927C9A  .T.......I>M..|.
0A9C4EF8: 00520002 00000000 00000000 000000    .R.............       ------>
ICC Header
            --  --
```

And, if we look at the ICC header at the underscored items 00520002:

```
0052   (represents the class name)             ----> L3_MGR_DSS_REQUESTS
0002   (represents the request name)          ----> L3_MGR_MLS_REQ
```

Workaround: Reload the system.

- CSCtu13806

  Symptoms: Upon switchover, the “red_switchover_process” process causes a crash on the old active RSP.

  Conditions: This symptom is observed upon switchover.

  Workaround: This crash is harmless as another RSP becomes active and works properly. Reboot the RSP to make it come up as standby.

- CSCtu13951

  Symptoms: Pending objects appear on the active and standby ESP.

  Conditions: This symptom occurs when the edge device to the core link is flapped multiple times for close to two days.

  Workaround: There is no workaround.

- CSCtu17006

  Symptoms: Mediatrace is not working because RSVP fails to select the output interface.

  Conditions: This symptom is observed only with PFR configuration.

  Workaround: Remove the PFR configuration.

- CSCtu17296

  Symptoms: Traffic failure occurs on 3 to 4 VLANs out of 1000.

  Conditions: This symptom is observed after reloading the UUT.

  Workaround: Remove and readd the service instance configuration for the affected VLANs.

- CSCtu17540

  Symptoms: IOMD core is generated on switchover for T1/E1 IM. After switchover, the IOMD process is aborted.

  Conditions: This symptom is observed with every switchover.

  Workaround: There is no workaround.

- CSCtu18150

  Symptoms: FP crash occurs due to a wrong FCID handling issue.

  Conditions: This symptom occurs due to a wrong FCID handling issue.

  Workaround: There is no workaround.

- CSCtu24765

  Symptoms: Under scale (28.8K PPPoX sessions), when executing "show policy-map session" from the CLI, both ESPs crash.

  Conditions: This symptom is observed with a large scale, that is, 28K PPPoE sessions established + ISG QoS services.

  Workaround: There is no workaround.

- CSCtu27601

  Symptoms: On ATM BRAS under scale (16K PPPPoEOA sessions + ISG services), the ESP crashes occasionally during sessions establishment.

  Conditions: This symptom is observed with a large scale (16K PPPPoEOA sessions + services).

  Workaround: There is no workaround.

- CSCtu28990

  Symptoms: RP crash is observed at SYS-6-STACKLOW: Stack for process XDR Mcast.

  Conditions: This symptom is observed when performing shut/no shut on interfaces on a configuration-rich system.

  Workaround: There is no workaround.

- CSCtu29047

  Symptoms: After a reload or switchover, the RSP may exhibit a kernel hang.

  Conditions: This symptom is observed occasionally after a reload or switchover.

  Workaround: Power cycle the box.

- CSCtu32913

  Symptoms: The system may crash when NBAR is continuously enabled/disabled.

  Conditions: This symptom is observed when NBAR is continuously enabled/disabled. This issue is seen after more than 12 hours of continuously enabling/disabling NBAR under traffic.

  Workaround: There is no workaround. The system works fine after reload.

- CSCtu32935

  Symptoms: IPv6 traffic loss of around 30 seconds is seen for routes learned from dynamic routing protocols upon RSP switchover with the Nonstop Forwarding (NSF) configuration. IPv6 CEF is not programmed on the standby RSP.

  Conditions: This symptom is observed with RSP switchover.

  Workaround: There is no workaround for the dynamic routing protocol. Problem will not be seen for static route.

- CSCtu33258

  Symptoms: LDP over MPLS-TP tunnel fails to get established upon router reload.

  Conditions: This symptom is seldom seen when the router is reloaded with scaled MPLS-TP tunnels that have LDP session established over the tunnels. Pinging traffic through the tunnel fails.

Workaround: There is no workaround.

- CSCtu34906

  Symptoms: All ptp sessions go down on the BC upon configuring more than 63 slaves to negotiate with it.

  Conditions: This symptom is observed on the BC when there are more than 63 slaves trying to negotiate with the master. This issue is not seen with lesser number of slaves. It was verified that the sessions are stable with 62 slaves. This issue is also not seen with the OC master, but only with the BC master.

  Workaround: This issue is not seen with lesser number of slaves. It was verified that the sessions are stable with 62 slaves. This issue is also not seen with the OC master.

- CSCtu35713

  Symptoms: IPv4 address saving: IPCP state change does not trigger session accounting update.

  Conditions: This symptom is observed under the following conditions:

  1. Enable IPv4 address saving on BRAS.
  2. Configure AAA periodic accounting using the **aaa accounting update periodic** *time in mins* command.
  3. Initiate IPCP negotiation from the client.
  4. After IPCP negotiation is complete, BRAS does not send an interim accounting update containing IPv4 address save VSA and the new IPv4 address assigned to the client.

  Workaround: Configure AAA accounting with the **aaa accounting update newinfo periodic** *time in mins* command.

- CSCtu41497

  Symptoms: The Nile Manager crashes.

  Conditions: This symptom is observed with a 256 rmep scale.

  Workaround: There is no workaround.

- CSCtu43120

  Symptoms: Service accounting start is not sent for L2TP sessions.

  Conditions: This symptom is observed with L2TP.

  Workaround: There is no workaround.

- CSCtu43731

  Symptoms: On an RP1, RP switchover causes an RP reset.

  Conditions: This symptom is observed with RP switchover under the following conditions:

  - The router must be an RP1.
  - The configuration of Flexible NetFlow (FNF) or equivalent must be applied to 4000 or more interfaces. In this case of testing, 4000 DVTI interfaces were in use.

  An equivalent of FNF is AVC or passive Video Monitoring. That is, those configured on a comparable number of interfaces will have the same effect.

  Workaround 1: Prior to doing a controlled switchover, such as ISSU, deconfigure FNF from some interfaces to take it well under the threshold at which the issue can occur.

  Workaround 2: Do not enable FNF monitoring.

- CSCtu53275

  Symptoms: Out to in traffic is not handled properly. The lookup on inside global is only done in the global routing table and not in the VRF routing table.

  Conditions: This symptom is observed with the following configuration on the Cisco ASR 1000 series router:

  ```
  ip nat inside source static 1.1.1.1 1.1.1.1 vrf test-pe1
  ```

  In to out traffic is handled properly.

  Workaround: A static route in the global routing table for each of these addresses (assuming they are unique) should provide a workaround for this issue.

- CSCtu98727

  Symptoms: ANCP shaping with Model F fails with BRR classes.

  Conditions: This symptom is observed with BRR classes, but works fine with LLQ (priority level) classes.

  Workaround: There is no workaround.

- CSCtv22685

  Symptoms: The ESP on the Cisco ASR 1000 router crashes or the GRE tunnel does not switch over when the destination interface is removed or the route changes, causing the tunnel interface to stop forwarding packets.

  Conditions: This symptom is observed when multiple GRE tunnels are configured on the same interface(s) with a high traffic rate across the tunnels.

  Workaround: Only configure one GRE tunnel per physical interface.

Resolved Caveats—Cisco IOS Release 15.2(1)S

All the caveats listed in this section are resolved in Cisco IOS Release 15.2(1)S. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCtj33003

  A vulnerability exists in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause an affected device to reload. Affected devices must be configured to process SIP messages and for pass-through of Session Description Protocol (SDP) for this vulnerability to be exploitable.

  Cisco has released free software updates that address this vulnerability. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerability.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-sip

- CSCtr28857

  A vulnerability in the Multicast Source Discovery Protocol (MSDP) implementation of Cisco IOS Software and Cisco IOS XE Software could allow a remote, unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition.

Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available. This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-msdp

- CSCts80643

  Cisco IOS Software and Cisco IOS XE Software contain a vulnerability in the RSVP feature when used on a device configured with VPN routing and forwarding (VRF) instances. This vulnerability could allow an unauthenticated, remote attacker to cause an interface wedge, which can lead to loss of connectivity, loss of routing protocol adjacency, and other denial of service (DoS) conditions. This vulnerability could be exploited repeatedly to cause an extended DoS condition.

  A workaround is available to mitigate this vulnerability.

  Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-rsvp

Related Documentation

The following sections describe the documentation available for Cisco IOS Release 15.2S. These documents include hardware and software installation guides, Cisco IOS configuration and command reference publications, system error messages, and feature modules.

Documentation is available online on Cisco.com.

Use these release notes with the resources described in the following sections:

- Platform-Specific Documents, page 417
- Cisco IOS Software Documentation Set, page 417
- Notices, page 418
- Obtaining Documentation and Submitting a Service Request, page 420

Platform-Specific Documents

Platform-specific information and documents for the Cisco 7600 series routers are available at the following location:

http://www.cisco.com/en/US/products/hw/routers/ps368/tsd_products_support_series_home.html

Platform-specific information and documents for the Cisco ME 3600X switch are available at the following location:

http://www.cisco.com/en/US/products/ps10956/index.html

Platform-specific information and documents for the Cisco ME 3800X switch are available at the following location:

http://www.cisco.com/en/US/products/ps10965/index.html

Platform-specific information and documents for the Cisco ME 3600X-24CX switch are available at the following location:

http://www.cisco.com/en/US/prod/collateral/switches/ps6568/ps10956/data_sheet_c78-708663.html

Platform-specific information and documents for the Cisco 7200 router are available at the following location:

http://www.cisco.com/en/US/products/hw/routers/ps341/index.html

Platform-specific information and documents for the Cisco 7301 router are available at the following location:

http://www.cisco.com/en/US/products/hw/routers/ps352/index.html

Cisco IOS Software Documentation Set

The Cisco IOS Release 15.2S documentation set consists of configuration guides, command references, and other supporting documents and resources. For the most current documentation, go to the following URL:

http://www.cisco.com/en/US/products/ps11793/tsd_products_support_series_home.html

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Original SSLeay License:

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section on page 417.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.