Release Notes for Cisco 4000 Series ISRs, Cisco IOS XE Everest 16.6

First Published: 2017-07-28

Last Modified: 2017-07-28

Cisco 4000 Series Integrated Services Routers Overview

Note Explore the Content Hub, the all new portal that offers an enhanced product documentation experience.

- Use faceted search to locate content that is most relevant to you.
- Create customized PDFs for ready reference.
- Benefit from context-based recommendations.

Get started with the Content Hub at content.cisco.com to craft a personalized documentation experience.

Do provide feedback about your experience with the Content Hub.

The Cisco 4000 Series ISRs are modular routers with LAN and WAN connections that can be configured by means of interface modules, including Cisco Enhanced Service Modules (SM-Xs), and Network Interface Modules (NIMs).

Note The Cisco IOS XE Bengaluru 17.4.1a is the first release for Cisco 4000 Series Integrated Services Routers in the Cisco IOS XE Bengaluru 17.4.1 release series.

The following table lists the router models that belong to the Cisco 4000 Series ISRs.

Cisco 4400 Series ISR	Cisco 4300 Series ISR	Cisco 4200 Series ISR
Cisco 4431 ISR	Cisco 4321 ISR	Cisco 4221 ISR
Cisco 4451 ISR	Cisco 4331 ISR	
Cisco 4461 ISR	Cisco 4351 ISR	

System Requirements

The following are the minimum system requirements:

Note There is no change in the system requirements from the earlier releases.

- Memory: 4GB DDR3 up to 16GB
- Hard Drive: 200GB or higher (Optional). (The hard drive is only required for running services such as Cisco ISR-WAAS.)
- Flash Storage: 4GB to 32GB

  Note There is no change in the flash storage size from the earlier releases. The flash storage size must be equal to the system memory size.

- NIMs and SM-Xs: Modules (Optional)
- NIM SSD (Optional)

For more information, see the Cisco 4000 Series ISRs Data Sheet.

Determining the Software Version

You can use the following commands to verify your software version:

- For a consolidated package, use the **show version** command
- For individual sub-packages, use the **show version installed** command

Upgrading to a New Software Release

To install or upgrade, obtain a Cisco IOS XE Gibraltar 16.12.1a consolidated package (image) from Cisco.com. You can find software images at http://software.cisco.com/download/navigator.html. To run the router using individual sub-packages, you also must first download the consolidated package and extract the individual sub-packages from a consolidated package.

Note When you upgrade from one Cisco IOS XE release to another, you may see *%Invalid IPV6 address* error in the console log file. To rectify this error, enter global configuration mode, and re-enter the missing IPv6 alias commands and save the configuration. The commands will be persistent on subsequent reloads.

For more information on upgrading the software, see the How to Install and Upgrade the Software section of the Software Configuration Guide for the Cisco 4000 Series ISRs.

Recommended Firmware Versions

Table 1: Recommended Firmware Versions, on page 3 provides information about the recommended Rommon and CPLD versions for releases prior to Cisco IOS XE Everest 16.4.1.

Table 1: Recommended Firmware Versions

Cisco 4000 Series ISRs	Existing RoMmon	Cisco Field-Programmable Devices
Cisco 4451 ISR	16.7(4r)	15010638 **Note** Upgrade CLI output has a typo and it would show the version incorrectly as 15010738 instead of 15010638. This does not impact the upgrade.
Cisco 4431 ISR	16.7(4r)	15010638 **Note** Upgrade CLI output has a typo and it would show the version incorrectly as 15010738 instead of 15010638. This does not impact the upgrade.
Cisco 4351 ISR	16.7(5r)	14101324
Cisco 4331 ISR	16.7(5r)	14101324
Cisco 4321 ISR	16.7(5r)	14101324
Cisco 4221 ISR	16.7(5r)	14101324

Upgrading the ROMMON Version on the Cisco 4000 Series ISR

For information about ROMMON compatability matrix, and ROMMON upgrading procedure, see the ROMMON Compatability Matrix and "ROMMON Overview and Basic Procedures" sections in the Upgrading Field-Programmable Hardware Devices for Cisco 4000 Series ISRs.

Upgrading Field-Programmable Hardware Devices

The hardware-programmable firmware is upgraded when Cisco 4000 Series ISR contains an incompatible version of the hardware-programmable firmware. To do this upgrade, a hardware-programmable firmware package is released to customers.

Generally, an upgrade is necessary only when a system message indicates one of the field-programmable devices on the Cisco 4000 Series ISR needs an upgrade, or a Cisco technical support representative suggests an upgrade.

From Cisco IOS XE Release 3.10S onwards, you must upgrade the CPLD firmware to support the incompatible versions of the firmware on the Cisco 4000 Series ISR. For upgrade procedures, see the Upgrading Field-Programmable Hardware Devices for Cisco 4000 Series ISRs.

Feature Navigator

You can use Cisco Feature Navigator to find information about feature, platform, and software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn . An account on cisco.com is not required.

Limitations and Restrictions

The following limitations and restrictions apply to all releases:

• Cisco Unified Threat Defense , on page 4

- Cisco ISR-WAAS and AppNav-XE Service, on page 4
- USB Etoken, on page 5

Acessing RSA Key and SSH

When you downgrade the Cisco 4000 Series ISR from IOS XE version 16.6.1 or a later release to a pre-16.6.1 release, including 16.3.X, the RSA key-pairs that are stored in private configuration storage are not accessible, and as a result, the SSH access is lost. This occurs because a secure storage feature was introduced and enabled by default starting with IOS XE version 16.6.1 which is not supported in pre-16.6.1 releases. After you downgrade, if you want to retain the access to RSA key-pair and SSH, use the **no service private-config-encryption** command in global configuration mode.

Smart Licensing

Ensure that the device is running the Cisco IOS XE Everest 16.6.1 version that supports the Smart Licensing mode.

For a more detailed overview on Cisco Licensing, go to https://cisco.com/go/licensingguide.

Cisco Unified Threat Defense

The Cisco Unified Threat Defense (UTD) service requires a minimum of 1 to 4 GB of DRAM.

Cisco ISR-WAAS and AppNav-XE Service

The Cisco ISR-WAAS/AppNav service requires a system to be configured with a minimum of 8GB of DRAM and 16GB flash storage. For large service profiles, 16GB of DRAM and 32GB flash storage is required. Also, Cisco ISR-WAAS requires a minimum of 200GB SSD.

IPsec Traffic

IPsec traffic is restricted on the Cisco ISR 4451-X. The router has the same IPsec functionality as a Cisco ISR G2. The default behavior of the router will be as follows (unless an HSECK9 license is installed):

- If the limit of 1000 concurrent IPsec tunnels is exceeded, no more tunnels are allowed and the following error message appears:

```
%CERM-4-TUNNEL_LIMIT: Maximum tunnel limit of 225 reached for Crypto functionality with
securityk9 technology package license.
```

- The throughput encrypted traffic supports 85 Mbps.
- The Cisco 4000 Series ISR does not currently support nested SA transformation such as:

```
crypto ipsec transform-set transform-1 ah-sha-hmac esp-3des esp-md5-hmac
crypto ipsec transform-set transform-1 ah-md5-hmac esp-3des esp-md5-hmac
```

- The Cisco 4000 Series ISR does not currently support COMP-LZS configuration.

CUBE–SRTP Calls

Cisco IOS XE Everest release 16.5.1 is not recommended for Cisco Unified Border Element deployment involving SRTP calls.

USB Etoken

USB Etoken is not supported on Cisco IOS XE Denali 16.2.1.

Unified Communication on Cisco 4000 Series ISR

- For T1/E1 clocking design and configuration changes, For detailed information, see the following Cisco document: T1/E1 Voice and WAN Configuration Guide.
- For Cisco ISR 4000 Series UC features interpretation with CUCM versions, For detailed information, see the following Cisco document: Compatibility Matrix .
- For High density DSPfarm PVDM (SM-X-PVDM) and PVDM4 DSP planning, For detailed information, see the following Cisco document: DSP Calculator for DSP planning .

Yang Data Models

Effective with Cisco IOS XE Everest 16.5.1b, the Cisco IOS XE YANG models are available in the form of individual feature modules with new module names, namespaces and prefixes. Revision statements embedded in the YANG files indicate if there has been a model revision.

Navigate to *https://github.com/YangModels/yang* > *vendor* > *cisco* > *xe* >*1651*, to see the new, main cisco-IOS-XE-native module and individual feature modules attached to this node.

There are also XPATH changes for the access-list in the *Cisco-IOS-XE-acl.yang* schema.

The *README.md* file in the above Github location highlights these and other changes with examples.

New Features and Important Notes About Cisco 4000 Series ISRs Release Everest 16.6

This section describes new features in Cisco IOS XE Everest 16.6 that are supported on the Cisco 4000 Series ISRs.

New and Changed Information

New Software Features in Cisco 4000 Series ISR Release Cisco IOS XE Everest 16.6.2

The following features are supported by the Cisco 4000 Series Integrated Services Routers for Cisco IOS XE Everest 16.6.2:

- Dying Gasp Suppport on Cisco 4000 Series ISRs—For detailed information, see the following Cisco document: Carrier Ethernet Configuration Guide.
- Encrypted Traffic Analytics—For detailed information, see the following Cisco document: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_eta/configuration/xe-16-6/sec-data-encrypted-traffic-analytics-xe-16-6-book.htmlandhttps://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Campus/CVD-Encrypted-Traffic-Analytics-Deployment-Guide-2017DEC.pdf .
- Enable Allowedlist Support for Encrypted Traffic Analytics—For detailed information, see the following Cisco document: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/xe-16-6/nf-xe-16-6-book/encrypted-traffic-analytics.html.
- Enable TLS Labels, App ID, and Multi Destination Support—For detailed information, see the following Cisco document: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/xe-16-6/nf-xe-16-6-book/encrypted-traffic-analytics.html.

New Hardware Features in Cisco IOS XE Everest 16.6.1

There are no new hardware features in this release.

New Software Features in Cisco 4000 Series ISR Release Cisco IOS XE Everest 16.6.1

The following features are supported by the Cisco 4000 Series Integrated Services Routers for Cisco IOS XE Everest 16.6.1:

- For information on migrating from existing Cisco IOS XE 3S releases to the Cisco IOS XE Everest 16.6.1 release, see Cisco IOS XE Everest 16.4.1 Migration Guide for Access and Edge Routers.
- Supported Technology Configuration Guides—When a technology is supported on Cisco 4000 series ISR, the corresponding technology configuration guide is displayed on the product landing page.
- BGP Feature Monitoring—For detailed information, see the following Cisco document: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/datamodels/configuration/xe-16/data-models-xe-16-book.html.
- Caller-ID and Directory Lookup for SIP Phones on Unified CME—For detailed information, see the following Cisco document: http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucme/admin/configuration/manual/cmeadm/cmedirs.html.
- HTTPS: UC Gateway Services API—For detailed information, see the following Cisco document: http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucme/CUCIS_API/CUCIS_API_Guide.html.
- IPv6 Support for Cisco Unified SIP SRST—For detailed information, see the following Cisco document: http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cusrst/admin/sccp_sip_srst/configuration/guide/SCCP_and_SIP_SRST_Admin_Guide/srst_overview.html.
- ISIS - SR OAM: ISIS FEC—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/seg_routing/configuration/xe-16-6/segrt-xe-16-6-book/oam-entropy-label-support.html.
- MLPPPoE on PPP Termination and Aggregation Router—For detailed information, see the following Cisco document:http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/wan_mlp/configuration/xe-16/wan-mlp-xe-16-book/wan-mlppp-eth-pta-xe.html.
- NID Support—For detailed information, see the following Cisco document: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cether/configuration/xe-16-6/ce-xe-16-6-book/ce-nid-support.html.
- NTT for NIM-BRI on Cisco 4000 Series ISR—Effective with Cisco IOS XE Everest 16.6.1 release, the ISDN switch type NTT on BRI network interface modules is supported on Cisco 4000 Series Integrated Services Routers, to enable seamless migration from Cisco G2 Series Integrated Services Routers.
- NGE TDM-IP (SIP) Support on Cisco 4000 Series ISR—Effective with Cisco IOS XE Everest 16.6.1, Next Generation Encryption (NGE) support is added for TDM-IP SIP in Cisco 4000 Series ISRs. NGE provides stronger encryption algorithm. With NGE, both signaling and media can be protected by the next generation cipher suites.
- QoS on GEC Portchannel on Cisco 4000 Series ISR—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_mqc/configuration/xe-16-6/qos-mqc-xe-16-6-book/aggregate-etherchannel-quality-of-service.html.
- Report Client-IP to Umbrella Cloud—For detailed information, see the following Cisco document:http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_utd/configuration/xe-16/sec-data-umbrella-branch-xe-16-book/sec-data-umbrella-branch.html.
- RESTCONF Programmability Interface Feature—For detailed information, see the following Cisco doucment: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/166/b_166_programmability_cg.html

- Radio Aware Routing—For detailed information, see the following Cisco document: http://www.cisco.com/c/en/us/td/docs/routers/access/4400/software/configuration/guide/isr4400swcfg/isr4400swcfg_chapter_010010.html.
- SD-AVC Auto-update Capability—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/configuration/xe-16-6/qos-nbar-xe-16-6-book.html.
- SD-AVC NBAR Export Capability—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/configuration/xe-16-6/qos-nbar-xe-16-6-book.html.
- Software Maintenance Upgrade—For detailed information, see the following Cisco document: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/config-mgmt/configuration/xe-16-6/config-mgmt-xe-16-6-book.html.
- Support for Idle URL for SIP Phones on Unified CME—For detailed information, see the following Cisco doucment:http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucme/admin/configuration/manual/cmeadm/cmelabel.html.
- Umbrella Connector on Cisco 4000 Series ISR/Interoperability of OpenDNS with IWAN—For detailed information, see the following Cisco document: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_utd/configuration/xe-16/sec-data-umbrella-branch-xe-16-book/sec-data-umbrella-bran.html
- UDF-ACL-Enhancement—For detailed information, see the following Cisco doucment:http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/lanswitch/configuration/xe-16-6/lanswitch-xe-16-6-book/lnsw-conf-erspan.html.
- Web User Interface—Supports an embedded GUI-based device-management tool that provides the ability to provision the router, simplifies device deployment and manageability, and enhances user experience. The following features are supported on Web User Interface from Cisco IOS XE Everest 16.6.1:
    - Cisco Umbrella Branch—The Cisco Umbrella Branch feature enables cloud-based security service by inspecting the Domain Name System (DNS) query that is sent to the enterprise DNS server through the Cisco 4000 Series Integrated Services Routers (ISR). The security administrator configures policies on the Cisco Umbrella Branch cloud to either allow or deny traffic towards the fully qualified domain name (FQDN). Cisco 4000 Series ISR acts as a DNS forwarder on the network edge, transparently intercepts DNS traffic, and forwards the DNS queries to the Cisco Umbrella Branch cloud.
    - Dyanamic Multipoint VPN—The Dynamic Multipoint VPN feature allows users to better scale large and small IP Security (IPsec) Virtual Private Networks (VPNs) by combining generic routing encapsulation (GRE) tunnels, IPsec encryption, and Next Hop Resolution Protocol (NHRP).
    - USB-LTE modem is supported on Web UI.
    - Snort IPS/IDS—The Snort IPS feature enables Intrusion Prevention System (IPS) or Intrusion Detection System (IDS) for branch offices on Cisco 4000 Series Integrated Services Routers and Cisco Cloud Services Router 1000v Series. This feature uses the open source Snort solution to enable IPS and IDS.
    - Zone-Based Firewall—Allows you to easily manage Cisco IOS unidirectional firewall policy between groups of interfaces known as zones.

      For information on how to access the Web User Interface, see Configure the Router for Web User Interface section.
    - YANG Data Models—For the list of Cisco IOS XE YANG models available with this release, navigate to https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/1661.

      Revision statements embedded in the YANG files indicate if there has been a model revision. The README.md file in the same github location highlights changes that have been made in the release

- Zero-Touch Provisioning (ZTP) —Supports HTTP file download along with TFTP file download

Configure the Router for Web User Interface

This section explains how to configure the router to access Web User Interface. Web User Interface require the following basic configuration to connect to the router and manage it.

- An HTTP or HTTPs server must be enabled with local authentication.
- A local user account with privilege level 15 and accompanying password must be configured.
- Vty line with protocol ssh/telnet must be enabled with local authentication. This is needed for interactive commands.
- For more information on how to configure the router for Web User Interface, see Cisco 4000 Series ISRs Software Configuration Guide, Cisco IOS XE 17.

Entering the Configuration Commands Manually

To enter the Cisco IOS commands manually, complete the following steps:

Before you begin

If you do not want to use the factory default configuration because the router already has a configuration, or for any other reason, you can use the procedure in this section to add each required command to the configuration.

Procedure

Step 1 Log on to the router through the Console port or through an Ethernet port.

Step 2 If you use the Console port, and no running configuration is present in the router, the Setup command Facility starts automatically, and displays the following text:

```
--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]:
```

Enter no so that you can enter Cisco IOS CLI commands directly.

If the Setup Command Facility does not start automatically, a running configuration is present, and you should go to the next step.

Step 3 When the router displays the user EXEC mode prompt, enter the **enable** command, and the enable password, if one is configured, as shown in the following example:

```
Router> enable
password password
```

Step 4 Enter config mode by entering the **configure terminal** command, as shown in the following example.

```
Router> config terminal
Router(config)#
```

Step 5 Using the command syntax shown, create a user account with privilege level 15.

Step 6 If no router interface is configured with an IP address, configure one so that you can access the router over the network. The following example shows the interface GigabitEthernet 0/0/0 configured.

```
Router(config)# interface gigabitethernet 0/0/0
Router(config-if)# ip address 10.10.10.1 255.255.255.248
Router(config-if)# no shutdown
Router(config-if)# exit
```

Step 7 Configure the router as an http server for nonsecure communication, or as an https server for secure communication. To configure the router as an http server, enter the **ip http server** command shown in the example:

```
Router(config)# ip http secure-server
```

Step 8 Configure the router for local authentication, by entering the ip http authentication local command, as shown in the example:

```
Router(config)# ip http authentication local
```

Step 9 Configure the vty lines for privilege level 15. For nonsecure access, enter the transport input telnet command. For secure access, enter the transport input telnet ssh command. An example of these commands follows:

```
Router(config)# line vty 0 4
Router(config-line)# privilege level 15
Router(config-line)# login local
Router(config-line)# transport input telnet
Router(config-line)# transport output telnet
Router(config-line)# transport input telnet ssh
Router(config-line)# transport output telnet ssh
Router(config-line)# exit
Router(config)# line vty 5 15
Router(config-line)# privilege level 15
Router(config-line)# login local
Router(config-line)# transport input telnet
Router(config-line)# transport output telnet
Router(config-line)# transport input telnet ssh
Router(config-line)# transport output telnet ssh
Router(config-line)# end
```

Resolved and Open Bugs

This section provides information about the caveats in Cisco 4000 Series Integrated Services Routers and describe unexpected behavior. Severity 1 caveats are the most serious caveats. Severity 2 caveats are less serious. Severity 3 caveats are moderate caveats. This section includes severity 1, severity 2, and selected severity 3 caveats.

The open and resolved bugs for this release are accessible through the Cisco Bug Search Tool . This web-based tool provides you with access to the Cisco bug tracking system, which maintains information about bugs and vulnerabilities in this product and other Cisco hardware and software products. Within the Cisco Bug Search Tool, each bug is given a unique identifier (ID) with a pattern of CSCxxNNNNN, where x is any letter (a-z) and N is any number (0-9). The bug IDs are frequently referenced in Cisco documentation, such as Security Advisories, Field Notices and other Cisco support documents. Technical Assistance Center (TAC) engineers or other Cisco staff can also provide you with the ID for a specific bug. 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

You can save searches that you perform frequently. You can also bookmark the URL for a search and email the URL for those search results.

Note 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.

We recommend that you view the field notices for the current release to determine whether your software or hardware platforms are affected. You can access the field notices from the following location:

http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html

Using the Cisco Bug Search Tool

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 .

Before You Begin

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.

Procedure

Step 1 In your browser, navigate to the Cisco Bug Search Tool .

Step 2 If you are redirected to a Log In page, enter your registered Cisco.com username and password and then, click Log In.

Step 3 To search for a specific bug, enter the bug ID in the Search For field and press Enter.

Step 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.

Step 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.

Step 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.

Resolved and Open Bugs in Cisco 4000 Series Integrated Services Routers

This section contains the following topics:

Open Caveats - Cisco IOS XE Everest 16.6.9

All resolved bugs for this release are available in the Cisco Bug Search Tool.

Caveat ID Number	Description
CSCvf86185	NIM-SSD: Inventory of disk0 and disk1 are interchanged on Polaris 16.x
CSCvt35331	Console port goes unresponsive, reboot required to restore it.

Resolved Caveats - Cisco IOS XE Everest 16.6.9

All resolved bugs for this release are available in the Cisco Bug Search Tool.

Caveat ID Number	Description
CSCvs48300	Arkenstone boot fail in Cisco 4221 ISR
CSCvv98528	Cisco 4000 Series ISR SER parity error checks continuing till router crashes
CSCvw56517	LMR Unable to hear first seconds of audio
CSCvw57860	Duplicate entries seen in MAC filter table.

Open Caveats - Cisco IOS XE Everest 16.6.8

All resolved bugs for this release are available in the Cisco Bug Search Tool.

Caveat ID Number	Description
CSCve01479	The e2e ping fails after configuring profiles qos-de and aaaauth1.
CSCvf50723	Packet-tracer error message % Error: Failed to collect packet information.
CSCvf86185	NIM-SSD: Inventory of disk0 and disk1 are interchanged on Polaris 16.x.
CSCvg62139	The "show voice lmr port_number " on Cisco 4000 Series ISRs do not show m-lead status
CSCvi37580	There is unexpected packets lost TCA reported on ISR4331 platform.
CSCvj17326	Cisco 4000 Series ISRs crashes in o2_cavm_pci_unlock when forwarding large packets for VPLS.
CSCvn22199	Cisco 4000 Series ISRs fails to authenticate users via dot1x following interface flap.
CSCvo84147	Cisco 4000 Series ISRTCP SEQ/ACK number wrongly inserted after OUT to IN NAT translation.
CSCvp49863	Incomplete arp in management interface.
CSCvp68166	The P-bit Sev Err Secs" increasing in patterns of 256 in SM-X-1T3/E3 on Cisco 4451 ISR.
CSCvr89973	NIM interfaces go into shutdown after router bootup.
CSCvt35331	Console port goes unresponsive, reboot required to restore it.
CSCvt55347	Cisco 4000 Series ISRs OID cwceLteCurrRsrq returning the wrong values.

Resolved Caveats - Cisco IOS XE Everest 16.6.8

All resolved bugs for this release are available in the Cisco Bug Search Tool.

Caveat ID Number	Description
CSCvo97985	The path-id discovery failure with "CENT throttle check fails, throttle type:0.
CSCvp23112	OBS: ping stop working on replacing MIP100 ->SIP40 >MIP100
CSCvp94050	cpp_bqs_srt_yoda_csr_tree_seid_initialize:1744 is not in "placed" state
CSCvq81620	Router crashes with ZBF HA sync.
CSCvq93850	Passive FTP will fail when going over NAT and either client or server are off a SM-X-ES3.
CSCvr00983	Unrecoverable Error with PVDM in 0/4 and Thule+dreamliner in 1/0 on Cisco 4300 ISR.
CSCvr01454	Punt fragment crash when receive EoGRE packets which have many fragments.

Caveat ID Number	Description
CSCvr15127	Cisco 4000 Series ISRs Calls fade to no-way audio due to media inactivity detection after 20 minutes.
CSCvr43037	The show macsec statistics interface and show macsec status interface does not show output
CSCvr58352	Prince: Keepalive pkts dropped when serial link congested with data traffic
CSCvr76534	Cisco 4000 Series ISRs : Crash seen at Process Exec.
CSCvr79751	Cisco 4331 ISR with BOOST License, the order of multicast packets reversed.
CSCvr89957	CFT crashed frequently.
CSCvs07447	Cisco 4000 Series ISRs Mgmt Gi0 up with speed 100Mbps
CSCvs28073	IOS-XE memory leak seen in 16.3.7 in IOSd due to update_sn_ao_state not deleting TDL bucket.
CSCvs53749	EVPN RMAC stale routes seen.
CSCvs55066	Cisco 4000 Series ISRs only: MGCP status remains Down and does not register with CUCM after a reboot or power cycle.
CSCvs75958	Cisco 4331 ISR/K9 Dialer cannot make calls suddenly.
CSCvs86573	Connect message is never forwarded to the calling side.

Open Caveats - Cisco IOS XE Everest 16.6.7

All resolved bugs for this release are available in the Cisco Bug Search Tool.

Caveat ID Number	Description
CSCvd65197	IOSd crashed when dialer disconnect the ISDN call.
CSCvf86185	NIM-SSD: Inventory of disk0 and disk1 are interchanged on XE 16.x.
CSCvg62139	"show voice lmr port_number " on Cisco 4000 Series ISRs do not show m-lead status.
CSCvi37580	There is unexpected packets lost TCA reported on Cisco 4331 ISR platform
CSCvj17326	Cisco 4400 ISR crashes in o2_cavm_pci_unlock when forwarding large packets for VPLS.
CSCvj55210	Memory leaks at __be_PKI_keypair_name_get.
CSCvo70549	CME SIP: BE4000 Smart Licensing - Extension Assigner temp registration uses endpoint license.
CSCvo84147	Cisco 4000 Series ISRs TCP SEQ/ACK number wrongly inserted after OUT to IN NAT translation.

Caveat ID Number	Description
CSCvp31671	Router crashes due to a call loop.
CSCvp49863	Incomplete arp in management interface.
CSCvp68166	"P-bit Sev Err Secs" increasing in patterns of 256 in SM-X-1T3/E3 on Cisco 4451 ISR.
CSCvp70211	Crash when running show crypto map.
CSCvp98673	Inband to OOB DTMF Fails to Be Passed On CUBE If Media Inactive Comes During Digit Processing
CSCvq43004	Need to check qfp ucode crash with RTCP traffic - chunk memory corruption in RTCP path.
CSCvq73281	TLS connections in WebEx between CUBE and iCP/CUSP breaks intermittently.
CSCvq75307	Crash due to watchdog after adding a prefix-list/ Route-map entry to existing route map.
CSCvq78692	mGRE L3VPN broken after reload.
CSCvq81620	Router crashes with ZBF HA sync.
CSCvq85913	FlexVPN with password encryption -- after MasterKey change password in profile is not working.
CSCvq90361	NHRP process crash on using same tunnel address on multiple spokes.
CSCvr00983	Unrecoverable Error with PVDM in 0/4 and Thule+dreamliner in 1/0 on Cisco 4300 Series ISRs.
CSCvr15127	Cisco 4000 Series ISRs Calls fade to no-way audio due to media inactivity detection after 20 minutes.
CSCvr15253	Router Crashes while Parsing and Printing Voice Packet IEs.
CSCvr17169	qfp ucode crash with media monitor.
CSCvr17670	The Cisco 4331 ISR crash and lost all config files.

Resolved Caveats - Cisco IOS XE Everest 16.6.7

All resolved bugs for this release are available in the Cisco Bug Search Tool.

Caveat ID Number	Description
CSCvd67904	Cisco 4000 Series ISRs does not run dot1x when a laptop wakes from sleep mode.
CSCve57810	Amur failing over w/o fail next-method or no-response next method.
CSCvg32153	"show interface port-channel" falsely reports output drops when there are no actual output drops.

Caveat ID Number	Description
CSCvh49874	FNF monitor download to DP failed after changing netflow record.
CSCvh79264	Change the punt cause of packets whose destination is virtual IP from SUBNET_BCAST to FOR_US.
CSCvh92659	BFD flaps everytime with dynamic tunnel creation in DMVPN.
CSCvi04907	T38 Packets are dropped by CUBE on ISR G2 in Multi VRF Scenario.
CSCvi22263	Crash when IOS is adapting shaping with Adaptive QoS over DMVPN configured.
CSCvj00317	Memory leak VOIP *MallocLite*.
CSCvj28921	High CPU due to Alignment Corrections - SMEF & IWAN.
CSCvj72294	memory leak @ CCSIP_SPI_CONTR.
CSCvj76866	Partial Power Failure in Stack Causes Interfaces to Become "shutdown".
CSCvk17998	Rekey Timer are same for both the Server and Client.
CSCvk47271	ICisco 4000 Series ISRscrashed in FXS-FXS non-hairpin call.
CSCvk51939	SSS Manager Traceback observer when test MLPPP.
CSCvm10850	Crash after CPUHOG in ISDN L2D SRQ Process.
CSCvm47690	Addition/Edits to numbered OG ACL using "access-list <>" command does not re-expand the ACL.
CSCvn00104	Software crash due to memory corruption after packet trace was enabled.
CSCvn01507	ISR not re-calculating the hash value correctly after payload change.
CSCvn02456	Router crashes when the calls doesn't establish after making 2 calls when we set "max-conn 2".
CSCvn03502	SR: CFLOW input intf index is 0xffffffff for Service-engine DSP module interface.
CSCvn23906	DHCP Server sends Renew ACKs to Clients with 00:00:00:00:00:00 MAC in L2 frame.
CSCvn45732	Device crashing if we unconfigure the NTP on the device.
CSCvn57892	High Memory utilization due to Wireless Manager IOSD process.
CSCvn61039	Cisco 4000 Series ISRs - control-plane host' feature was moved to APPX feature set.
CSCvn78961	Subscribers cannot re-login due to CoA time-out (lite-sessions in routed mode)
CSCvo03458	PKI "revocation check crl none" does not fallback if CRL not reachable.
CSCvo04856	DataPlane (DP) crash observed in MMOH call flow.

Caveat ID Number	Description
CSCvo06817	Router crash while executing show commands using '|' (pipe) to filter the output.
CSCvo10145	Memory overlay crash when using include-cui.
CSCvo10491	PnP Agent should detect image upgrade scenario and configure dialer to bring up cellular interface.
CSCvo11786	SCCP Application does not clear failed sockets leading to leak and socket pool exhaustion.
CSCvo12745	Packet drop occurs after acl permit configurations.
CSCvo12799	Call is not getting connected in Forking Re-INVITE scenario.
CSCvo21122	Memory leak at hman process.
CSCvo36031	WSMA crash formatting show command output.
CSCvo46138	Stuck CPP Thread while processing H323 packet.
CSCvo46405	QFP ucode crashed with sRTP traffic - chunk memory corruption.
CSCvo47376	Cisco REST API Container for IOS XE Software Authentication Bypass Vulnerability.
CSCvo55194	After RSP switchover label imposition was not programmed in Software on APS standby router.
CSCvo58098	CTS PACS not downloading to the devices.
CSCvo61610	FXS - no busy tone is generated on remote-onhook condition with call pickup scenario.
CSCvo66216	IPSec-Session count in "show crypto eli" reaches max causing VPN failure.
CSCvo71721	When sending account-logon ISG do not reply with ACK nor NACK.
CSCvo74486	IOS-XE ACL port information preserved after encapsulation.
CSCvo87827	Crash when polling IPForwarding MIB.
CSCvo90060	Wrong label programming leading to traffic drop.
CSCvo92514	SDP attribute list corruption causes voice gateway crash.
CSCvp24911	SRTP ROC Stress: CPP crash with 6000+ concurrent calls - g729.
CSCvp24981	When FQDN used for APN, IOS DNS resolves FQDN to IP, but GTP stays in DNS pending and IP 0.0.0.0.
CSCvp25052	Cisco 4000 Series ISRs: Router crash due to twice memory release.
CSCvp27220	Tail drops on IPSLA sender when using scaled udp-jitter probes.
CSCvp31779	Router Running IOS-XE 16 Crashes when Stopping EPC with ACL.

Caveat ID Number	Description
CSCvp33578	Crash at the moment of deleting a DVTI.
CSCvp34230	CUBE HA - Global bind is removed during interface flap.
CSCvp38317	MGCP GW does not reset SSRC/ROC on receiving MDCX with new IP/port/SDP parameter for SRTP call.
CSCvp39597	Crashes with GRE tunnels configured with QOS over Multilink Frame-relay interfaces.
CSCvp42709	Cisco 4000 Series ISRs NO_PUNT_KEEPALIVE kernel crash due to CP drivers stuck punt and IPC rings.
CSCvp47723	Cisco 4000 Series ISRs CME no way audio on calls across E1/PRI, reboot resolves for sometime.
CSCvp56596	Cisco 4000 Series ISRs crashes after voice register reset command is applied.
CSCvp63616	Crash due to too many DSPs.
CSCvp65151	CPP Stuck thread when processing IPv6 traffic.
CSCvp67530	Corrupt free block of memory with high availability config for Session Initiation Protocol.
CSCvp69393	Router crashes after snmpget to OID related to NHRP.
CSCvp70443	ISDN cause-location command support for switch-type primary-ntt.
CSCvp72220	Crash at sisf_show_counters after entering show device-tracking counters command.
CSCvp72379	IP dns primary command does not get removed.
CSCvp74674	QoS fails to apply to tunnel2 when underlying tunnel1 reachability change.
CSCvp86216	Router ucode crash with NAT with interface flap.
CSCvp87488	No login on-success log CLI does not persist across device reloads.
CSCvp92334	Crash after Media monitor look up.
CSCvp99884	CUBE not passing History-Info header in 181 Call is being forwarded.
CSCvq00263	Device crashed @ radius_io_stats_timer_handler due to dynamic-author.
CSCvq04828	VRF aware reverse DNS lookup not working.
CSCvq12723	DPDK: Performing Shut/No-Shut with traffic running can cause packets to silently drop on TX.
CSCvq18793	NIM-2FXS/4FXOP crashing due to DSP failed to reply properly.
CSCvq29575	Voice gateway crash due to segmentation fault in process CCSIP_DNS.
CSCvq39121	Cisco 4000 Series ISRs crash during packet inspection due to stuck thread.

Caveat ID Number	Description
CSCvq50202	Class-attributes duplicated after EAP reauthen. in ISG radius proxy scenario.
CSCvq57205	Recording failures with XMF media forking and SIP preservation timer.
CSCvq57862	Cable-detect command not reflecting proper status in Analog ports on IOS-XE platforms.
CSCvq58520	After reload dial-peers with ports that have the 'signal did' command show operational state none.
CSCvq72560	More connections are getting passthrough with reason SNG_OVERLOAD.
CSCvq75610	IWAN router crash after upgrading to 16.3.8.
CSCvq92102	VG450: SCCP crashing router while shutdown the process.

Open Caveats - Cisco IOS XE Everest 16.6.6

All resolved bugs for this release are available in the Cisco Bug Search Tool.

Caveat ID Number	Description
CSCvj72294	Memory leak happens at CCSIP_SPI_CONTR process for every trunk out-of-dialog message with "contact" header in it.
CSCvj56471	Memory leak under CCSIP_UDP_SOCKET / MallocLite
CSCvk51939	SSS Manager Traceback observer when test MLPPP
CSCvn01507	ISR not re-calculating the hash value correctly after payload change
CSCvo60849	Crash noticed when routes are getting imported twice(from vpnv4 to vrf to evpn) with route churn
CSCvo62122	IOS-XE Router may crash when attempting to Fragment Corrupted IPv4 Packet
CSCvo66216	IPSec-Session count in "show crypto eli" reaches max causing VPN failure
CSCvo74486	IOS-XE ACL port information preserved after encapsulation
CSCvo87827	Crash when polling IPForwarding MIB
CSCvp03110	After Configuring a New VRF Routes Are Not Imported From WAN Into l2vpn EVPN For Unrelated VRF

Resolved Caveats - Cisco IOS XE Everest 16.6.6

All resolved bugs for this release are available in the Cisco Bug Search Tool.

Caveat ID Number	Description
CSCuw36080	SNMP with Extended ACL.

Caveat ID Number	Description
CSCvg40746	mka policy MKA_POLICY" config lost after reload.
CSCvh57657	NAT MIB not populated when using traditional NAT.
CSCvj86876	Cisco 4000 Series ISR- IOS 16.8 - crypto-related issues seen with a single AF configured in VRF definition.
CSCvk32822	QoS stats process crash.
CSCvk62792	IKE Fragmentation payload incorrectly marked as critical.
CSCvm56670	ACL dropping packets after updating it - %CPPEXMEM-3-NOMEM.
CSCvm70471	hw-module subslot 0/2 reload' CLI does not activate the container after harddisk format.
CSCvm75066	MPLSoVPN: Change behavior of default route in NHRP. Must insert 0.0.0.0/0 instead of /32.
CSCvm94891	Crash caused by a "TLB Modification exception" after processing a null chunk in "IP Input" process.
CSCvn02419	Device running IOS-XE 16 Polaris Sees Crash When Performing NAT ALG on FTP Packet.
CSCvn14737	Crash with SIP call.
CSCvn17062	Cisco 4000 Series ISRs add SCCP MTP single-VRF support with a limitation no traffic from/to other VRF
CSCvn17530	Router Crashes When PKI-CRL-IO_0 Runs out of Stack Space During Failed DNS Lookup for CA Server.
CSCvn23226	NHRP process is crashing.
CSCvn27449	PBR does not work for dialer intf when it does not have fixed ip address.
CSCvn56017	Crash while processing ISIS updates when DiffServ-TE is enabled.
CSCvn78203	Router crashed when printing logs while constructing rekey packets (GETVPN).
CSCvn78349	FlexVPN with password encryption - keyring aaa LIST password 6 xxxxx encrypted again upon reload.
CSCvn82245	EIGRP session is not coming up if the dynamic PBR is applied on interface.
CSCvo09246	Cisco 4351 ISR communication down few minute after shutdown/no shutdown interface.
CSCvo19234	Memory corruption while freeing memory.
CSCvo22398	Cisco 4000 Series ISR with NIM-ES2 do not forward STP Uplink Fast dummy packet.
CSCvo24170	Crash due to chunk corruption in ISIS code.

Caveat ID Number	Description
CSCvo27553	PKI incorrect fingerprint calulation during CA authentication.
CSCvo47866	Crash at Process = SCCP Auto Config.

Open Caveats - Cisco IOS XE Everest 16.6.5

All resolved bugs for this release are available in the Cisco Bug Search Tool.

Caveat ID Number	Description
CSCus13106	IOS-XE - RSA key-gen: Error in generating keys:no available resources.
CSCvj89047	Quake-sessmgrd Huge Mem Leak After Master switchover.
CSCvk15062	Modification to ZBFW access-lists do not reflect in TCAM.
CSCvk22449	BGP Traceback/Crash seen with 20k IPv4 BGP scale after reload/clearing bgp.
CSCvk32822	QoS stats process crash
CSCvm25921	Signaling interface inactive on "show snmp mib ifmib ifindex de" on Cisco IOS 16.6.3.
CSCvm51112	The "clear crypto sa vrf MyVrf" triggers crash after updating pre-shared-keys.
CSCvm57021	Crash in CENT-MC-0 process after Doubly-linked list corruption.
CSCvm61279	Crash under AFW_application_process with shared-line configuration.
CSCvm70471	The hw-module subslot 0/2 reload CLI does not activate the container after harddisk format.
CSCvm76452	IPSec background crash while sending SNMP trap.
CSCvm78822	The config-sync failure aaa authorization commands.
CSCvm84742	Crash after issuing "no ip dhcp snooping VLAN <VLAN #>" command.
CSCvm91837	IOS and IOS-XE STCAPP service not updating DTMF RFC2833 payload when there is SCCP renegotiation.
CSCvn01507	Cisco 4000 Series ISR not re-calculating the hash value correctly after payload change.
CSCvn02419	Router crashes while running Dell software update.
CSCvn06127	Oneway audio issue is seen when CUBE use loopback interface for voice traffic that is coming on Multivrf.
CSCvn08136	Removing FNF config using the command "no vlan config 1-4094" causes watchdog forced crash.
CSCvn14454	iWAN router PDP crash.

Caveat ID Number	Description
CSCvn23906	DHCP Server sends Renew ACKs to Clients with 00:00:00:00:00:00 MAC in L2 frame.
CSCvn28017	Cisco 4331 ISR Routers may crash when "eigrp default-route-tag" Configured on IPv4 AF.
CSCvn49911	Stuck thread crash after executing 'clear ip nat translation vrf <VRFNAME>.

Resolved Caveats - Cisco IOS XE Everest 16.6.5

All resolved bugs for this release are available in the Cisco Bug Search Tool.

Caveat ID Number	Description
CSCty35807	INFO-2833 DTMF interoperability issue when Remote-Party-ID is configured.
CSCuy44786	Meet crypto recommendations in IKEv2 defaults.
CSCuz14861	IOS-XE Fails to correctly populate RTCP SSRC Field.
CSCvb03610	Watchdog crash after "% AAA/AUTHEN/CONT: Bad state in aaa_cont_login()."
CSCve31475	SNMP Error: OID not increasing: @ipAddressIfIndex.ipv6z.
CSCve76160	Transfer to voicemail not working because ephone-dn virtual/internal dial-peer is down.
CSCvf37923	Crash due to stack overflow.
CSCvf65079	CUBE reloaded with reason: RG-application reload on voice-b2bha RG.
CSCvf67313	CUBE does not honor codec under dialpeer when LTI and midcall-signaling block configured together.
CSCvg04712	ESP crash with cpp-mcplo-ucode core file.
CSCvg29037	Traceback is observed during mid-call media IP and port change.
CSCvg40893	Registration failed for REGISTER matching wrong voip dial-peer.
CSCvg42218	VRF failed to associate if binding is used in tenant.
CSCvg68773	Global bind disappears when bind interface flaps during an active call.
CSCvg69229	TAMS process crashes on Cat3k running 16.6.x code.
CSCvh49380	PFRv3 Incorrect reported value of TCA threshold in traffic-class router change history.
CSCvh77310	Wrong initial number of DPD incrementing error counter.
CSCvh84873	High CPU when enabling GETVPN Routing Awareness for BGP (crypto engine pr).
CSCvh92275	QoS Overrides loadbalancing to per prefix even with only session level policing applied.

Caveat ID Number	Description
CSCvh97101	NAT-HA on Cisco 2900s breaks if it is asymmetric routing.
CSCvi08303	Standby RP Reloads due to Config Sync Failure When Applied Service-insertion WAAS on Physical Int.
CSCvi52608	CLI show aaa clients detailed command triggered SSH to crash.
CSCvi65958	Standby RP crashes due to shortage of memory when running OSPF.
CSCvi83306	Crash with IOSXE-WATCHDOG: Process = IPv6 RIB Event Handler.
CSCvi83419	Router crash when removing route-target and with hard clear.
CSCvi92528	ZBFW HA: Configuring redundancy RII on virtual template auto-tunnel does not take effect.
CSCvi96450	Router crashed when lsp-mtu is changed.
CSCvi96965	Radius Automate Tester probe on feature is not working as expected.
CSCvj02910	Reload removing ipv6 VRRP group.
CSCvj22537	Standby switch crashes when flow-exporter destination configured with Hostname.
CSCvj25678	Crash after failing to modify xcode.
CSCvj43156	Crash in XDR process: "fib_rp_table_broker_encode_buf.size <= FIB_RP_TABLE_BROKER_ENC_BUF_SZ"
CSCvj45781	QFP CGM Memory depletion during ISG session churn.
CSCvj50005	Cisco 4000 Series ISR PPE ucode crash when processing ipsec traffic on CWS tunnel.
CSCvj60825	Redzone overlay copying SIP SDP data.
CSCvj67623	DNS ALG will not work when trying to match specific destination hosts.
CSCvj70568	FlexVPN / DHCP entries not flushing for ikev2 timed out reconnect sessions.
CSCvj71845	Backup path incorrect for ring topology where high ISIS cost is configured on 1 link.
CSCvj76285	Snmp v2 breaks due to Authentication failure, bad community string, 16.03.06.
CSCvj76316	subscriber template not cleared after idle time exceed as well as traceback generation
CSCvj76662	GetVPN TBAR failure does not generate syslogs.
CSCvj77688	Shimming have some issue over selecting idb.
CSCvj78083	Path of Last Resort Sending Probes in Standby State.
CSCvj78647	MTU cli is disappeared from show run when interface dialer shut/no shut.
CSCvj79542	Missing interface source template model.

Caveat ID Number	Description
CSCvj79694	sgt-map gets cleared for some of the end points for unknown reason.
CSCvj83551	SISF crash in IPV6 neighbor discovery packets.
CSCvj84104	PLR channel is not muted for some time.
CSCvj88138	VASI NAT: FTP ALG translation is sometimes failed.
CSCvj90089	Crashes while doing a conference call.
CSCvj90145	Zero Touch Provisioning (ZTP) fails to apply certain service instance configuration.
CSCvj90814	Crashes due to memory corruption in Cisco 4000 Series ISR.
CSCvj91448	PKI:-IP address parsing issue while printing the subject name if classless IP is used in Trustpoint
CSCvj94863	Channel with wrong label may be created on hub border.
CSCvj95361	Crashed due to process = IPSec background proc.
CSCvk02072	Hoot-n-holler multicast traffic marked with DSCP 0.
CSCvk07070	Observing bmalloc smd leaks at OBJ_WEBAUTH_LOGOUT_URL with webauth.
CSCvk07838	CUBE is using wrong source IP address to send SIP error.
CSCvk10633	BGP crashes while running show command and same time bgp peer reset.
CSCvk10909	ISRv: ONEP process crash during day0 bringup.
CSCvk12152	Unable to remove command ip nat inside destination.
CSCvk16771	ISIS for IP is enabled/installing routes in the RIB while IP routing is disabled.
CSCvk20003	Host limit of 32 for session monitoring sessions.
CSCvk20560	491 not sent in a multiple re-invites in DO2EO scenario.
CSCvk20589	SSH V2 crashes.
CSCvk27007	MGCP status remains Down after IOS upgrade caused by CSCvh70570.
CSCvk30939	Memory corruption at PKI session end.
CSCvk31115	Device-sensor does not send data off initial boot.
CSCvk37875	High Availability system with two Voice Gateways crashes.
CSCvk39041	SDA: IP phone latency in fabric is close to 4 secs.
CSCvk46664	DNA Center SWIM Upgrade fails and unable to upgrade manually.
CSCvk50734	Device Tracking - Memory leak observed with IPv6 NS/NA Packets.

Caveat ID Number	Description
CSCvk52495	IP SLA multicast appear as "Unknown".
CSCvk53405	Router crash - AFW_application_process.
CSCvk56331	Initial contact in IKEv1 phase 2 rekey (QM1) causes all crypto sessions to drop.
CSCvk58143	500~600 secs Increase in boot time when "ip domain lookup" configured.
CSCvk59419	Crash in xoslib code for onepk process when using yang-netconf.
CSCvk60184	Random crash of data plane with SRTP-SRTP / SRTP-RTP load tests.
CSCvk65072	Crash due ZBF + NAT.
CSCvk65354	Extension Mobility Not working when used with Greek locale on SIP CME.
CSCvk66880	CUBE incorrectly fomats SIP SDP.
CSCvk69075	No calls shown in output "show call active voice brief" on CUBE & stale entries are present.
CSCvk69093	CUBE is not responding to SIP INFO.
CSCvm00765	BFD crash on imitating traffic loss.
CSCvm01420	CUBE crashes at sipSPI_ipip_vcc_CheckCodecSetType.
CSCvm02627	Incorrect Contact port 5060 used instead of 5061 by CUBE in "302 Moved Temporarily" message.
CSCvm03744	"%FMFP-3-OBJ_DWNLD_TO_DP_FAILED:fman_fp_image:xxx" appears when configured "ip port-map" on Cisco 4000 Series ISR.
CSCvm08571	Rework need on CSCvj59170 to support SDP parsing.
CSCvm12196	Memleak (IP: RIB Alternate Preference): provides fix for CSCvk68355.
CSCvm19399	CRL file is getting overwritten when PKI server turns up after reload.
CSCvm21219	Crash is seen on Running "show vpdn tunnel summary" command.
CSCvm24689	One-way audio to IP phone if phone does hold/resume after 20 minutes on secure SIP gateway.
CSCvm32047	Device crashed when call-home is enabled and non-ascii characters in use in login banner.
CSCvm38891	PKI disabled stripping of trailing dot during server-id check.
CSCvm39894	False authorizations and authentications even without radius server for dot1x/mab.
CSCvm40441	CFD: PNP DNS discovery with trust pool flow uses IP address in PNP profile instead of FQDN.

Caveat ID Number	Description
CSCvm43071	[IBNS 2.0] aaa-available event is not being triggered when using authentication/authorization list.
CSCvm45068	IOS CUBE Ent does not show media anti-trombone in configuration.
CSCvm46814	cts_sga on 16.3.6 crashes.
CSCvm51739	SNMP v3 discloses password in the parser warning syslog trap.
CSCvm53491	SIP CME Crashes when Calling Shared Line.
CSCvm55465	BGP updates missing ISIS advertising-bits led to LDP label purge on peer.
CSCvm56592	Cisco CME: Corrupted config file for Auto Registered IP Phones after reload.
CSCvm58960	"VoIP dial-Peer <XX> is Busied out" printed in log every 2 minutes when destination is not reachable.
CSCvm59172	The "autoroute announce" and "loose" path not working on intra-area TE tunnel.
CSCvm59483	Host crashes the DSP if ipv6 commands are configured under Service-Engine [Purge ipv6 config option].
CSCvm63651	Memory leak due to authentication mac-move permit.
CSCvm65384	SNMP OID conflict.Trap being generated with wrong oid 6999.it should be 854.
CSCvm66103	Crash due to communication failure - IPC (Inter-Procedure Call) messages between DSP and RP.
CSCvm74894	PKI authentication should proceed even if GetCACaps return any http failure.
CSCvm76590	CUBE doesn't forward 200 OK in SRTP-RTP scenario with TCL script on Dial-peer.
CSCvm83720	Cisco 4431 ISRGateway crashed due to flex_dsprm_vtsp_close.
CSCvm86135	SMD crash after removing access-session attributes filter-list.
CSCvm91422	[MiFID] [Inbox-HA] VRF-ID is set to 65535 after switchover, call fails.
CSCvm92019	Media Ant-Trombone does not properly handle a Re-Invite utilizing a Replaces Header.
CSCvm93603	IP change on dialer-int does not trigger a correct "local cryto entpt"in DMVPN.
CSCvm96663	An IOS-XE router crashes after umbrella is configured.
CSCvm99036	CUBE Crash in CCSIP_SPI_CONTROL process.
CSCvm99045	IOS-XE PKI: Certificate with 4 dashes imported in trustpool gets lost after reboot.
CSCvn02171	Cisco IOS XE :HOLE is not created when acl default passthrough configured.
CSCvn07614	Out of Band DTMF Events Not Passing to CUCM via SCCP When Using IOS MTP.

Caveat ID Number	Description
CSCvn18712	CUBE incorrectly fomats SIP SDP with Content-Length > 1024.
CSCvn33961	SSRC-field in RTCP gets changes to 0 when going through TRP present in the media path.

Open Caveats - Cisco IOS XE Everest 16.6.4

All resolved bugs for this release are available in the Cisco Bug Search Tool.

Caveat ID Number	Description
CSCuy75886	Chunk memory leak about SNMP SMALL CHUN and SNMP MEDIUM CHU.
CSCvb72829	The **sh ipv6 neigh statistics** not updated post RPSO for entries synced.
CSCvc73961	OSPF BGP LS: When seg mpls is disabled on the NBR, the unnumbered links not withdrawn from LSLIB.
CSCvd20054	Traceback @mpls_ldp_cfg_interface while enabling ISIS.
CSCvd65197	IOSd crashed when dialer disconnects the ISDN call.
CSCve05486	ISDN switch-type configure issue for BRI leased-line.
CSCve12319	ISIS SRTE: When one of ECMP path for prefix is not enabled for SR, SRTE tunnel does not come up.
CSCve16269	IKEv2 CoA does not work with ISE.
CSCve32648	Traceback@cpp_mlp_bundle_stats_query_all_cmn on fp reload.
CSCve39101	OSPF SROAM: "%ARP-3-ARPADJ: Internal software error during updating CEF Adjacency" when box comes up.
CSCve39572	BGP net should have inlabel if bgp mpls-local-label is configured.
CSCve54914	NDSSO vrf ha table to be populated correctly.
CSCve96308	Observing memory leak in AAA_MALLOC_LITE.
CSCvf21341	CME: Pushing call from desk phone to SNR phone failing if media-renegotiate CLI is configured
CSCvf22725	OSPF SR/SIDredistribute: when SID configured > avbl SRGB, that sid should not be advertised in EPL.
CSCvf28564	Show details soft key is not functioning in a conference call.
CSCvf34848	License synchronized to SSMS despite being removed from SL Portal.
CSCvf37923	Crash due to Stack overflow.
CSCvf51917	The **dns-a-override** CLI not working due to breakage since 16.4 IOS.

Caveat ID Number	Description
CSCvf76436	Combination of add-path, backup path and advertised-to leaves is not giving expected netconf values.
CSCvf86185	NIM-SSD: Inventory of disk0 and disk1 are interchanged on Cisco IOS XE 16.x.
CSCvf95739	Remove "dns-vrf-aware" CLI and make DNS vrf aware by default.
CSCvg06563	BE4K memory leak during bulk register request from portal.
CSCvg23363	Virtual-access interface MTU wrongly set when using ipsec ipv4.
CSCvg23820	CTS PAC download fails with VRF config on non-managenent interface.
CSCvg40893	BE4K Registration failed for REGISTER matching wrong voip dial-peer.
CSCvg42218	BE4K VRF failed to associate if binding is used in tenant.
CSCvg49910	BE4K OPTION messages not sent out with VRF+DNS.
CSCvg62139	The "show voice lmr port_number " on ISR4K do not show m-lead status.
CSCvg63956	BE4K Call failed to answer if SNr configured with no matching dial-peer.
CSCvg81772	VRF import config missing ipv4 unicast after no router bgp
CSCvg87102	BE4K group pickup failed when call xfered by AA with cause code 47.
CSCvh17679	BE4000/CME SNR call fails due to the extension COR list configuration.
CSCvh49364	PFRv3 Incorrect time-stamp in traffic-class router change history.
CSCvh57657	NAT MIB not populated when using traditional NAT.
CSCvh65955	CME: SIP Notify to clear NightService display message not sent to phones during de-activation.
CSCvh67422	IPSLA ICMP-jitter stats reporting some of the received packets as lost.
CSCvh67788	CME: COR functionality impacts CallFwd and SNR call flow scenarios.
CSCvh85031	Branch MC crashed@cent_send_syslog_on_violated_policies under stress test.
CSCvh93960	CME SIP: One way audio on consult transfer when SNR enabled on transfer target.
CSCvi06417	SIP stack matching the dial-peer when processing NOTIFY message causing call routing issues.
CSCvi10089	EXEC process stuck vty line where no exec is set.
CSCvi15955	Call failure after Bye-Also blind transfer from CUE requires failure indication.
CSCvi36351	The standby rp crash on removing member link from port-channel.
CSCvi37580	There is unexpected packets lost TCA reported on Cisco 4331 ISR platform.

Caveat ID Number	Description
CSCvi54372	%NHRP-3-PAKERROR | loop detected | Pak sanity failure.
CSCvi63425	Cisco 4400 ISR router cpp crashed when configured HSRP with PMIPv6.
CSCvi83419	Router crash when removing route-target and with hard clear.
CSCvi90729	IKEv2 CoA does not work with ISE (coa-push=TRUE instead of true).
CSCvi90964	Cisco 4331 ISR : Crash due to Segmentation fault(11), Process = Tunnel Security.
CSCvi92505	MWI info is not preserved on CME SIP phone after a reboot for unsolicited method.
CSCvi93431	CME/BE4k: Adding Support to allow whisper paging as a configurable option on SIP phones.
CSCvi93972	IWAN versions with prefix tracking only allow prefix splitting for internet and not enterprise.
CSCvi97233	CME radius accounting does not generate complete called number for EA.
CSCvj08942	SNMPwalk of cipslaPercentileLatestStatsTable does not give all the cipslaPercentileTypeVar types.
CSCvj09305	Slow convergence when configuring ha-mode sso for IPv6 peers.
CSCvj11263	NBAR: resource exhaustion might occur in FNF with vmware-vsphere and flow monitors.
CSCvj22081	Cisco 4331 ISR: Memory lock occurs when archive config and "wr" are executed at the same time
CSCvj25236	IPDT flapping after upgrade to 15.2(2)E7.
CSCvj26944	Cisco-IOS-XE-policy yang model does not support "set precedence"
CSCvj29514	CME: Toll fraud app not automatically trusting traffic from phones.
CSCvj35317	Ti-LFA Repair Path is not Loop-Free.
CSCvj44615	Ringback stops on REFER based xfer when CUBE receives 180 followed by 183 w/SDP media change.
CSCvj45781	QFP CGM Memory depletion during ISG session churn
CSCvj47270	IKEv2 sessions cannot establish due to CAC leakage.
CSCvj50644	Barge and cBarge failure on Incoming SIP trunk calls to BE4K.
CSCvj51929	Out of order ESP packets triggering IPSEC replay error message.
CSCvj57453	OSPF TILFA: tilfa repair path computation ALGORITHM fails with reason code BAD FH NBR.

Caveat ID Number	Description
CSCvj57487	OSPF TILFA: tilfa repair path computation ALGORITHM uses incorrect firsthop router-id.
CSCvj58359	SIP packets not sent out by BE4K when gig0/0/1 has vrf forwarding enabled.
CSCvj59152	Evaluation of all for May CPU Side-Channel Information Disclosure Vulnerabilities.
CSCvj60144	OSPF TILFA: tilfa ALGORITHM fails to get repair node n-sid label when vertex is beyond PGW node
CSCvj60749	Cisco 4000 Series ISRs handles MTU on Virtual-PPP interface differently and doesn't respect DF-bit on QFP level.
CSCvj64493	Standby switch crash whem removing kron scheduler command.
CSCvj66204	Initial SNMP traps take agent-addr from shutdown interface.
CSCvj67623	DNS ALG will not work when trying to match specific destination hosts.
CSCvj70568	FlexVPN || DHCP entries not flushing for ikev2 timed out reconnect sessions.
CSCvj72854	Router crash due to NHRP process Segmentation fault(11).
CSCvj74888	Kernel OOPS reporting ECC error.
CSCvj75853	Device crash after execute command "**show lldp neighbor [int] detail**".
CSCvj76285	Snmp v2 breaks due to Authentication failure, bad community string, 16.03.06.
CSCvj76316	Subscriber template not cleared after idle time exceed as well as traceback generation.
CSCvj76662	GetVPN TBAR failure does not generate syslogs.
CSCvj78876	CUBE: FPI Hung Sessions and Provisioning Failures observed in Standby CUBE.
CSCvj81382	IPv6 AAA Prefix Support for 3rd party PPP clients no password for -dhcpv6 Access-Request.
CSCvj82095	NBAR mismatch cisco video traffic.
CSCvj83551	SISF crash in IPV6 neighbor discovery packets.
CSCvj84104	PLR channel is not muted for some time.
CSCvj84121	Cisco 4321 ISR Radius Chap authentication does not work.
CSCvj84158	PfRv3: BR May Crash due to Channel Creation/Modification and Next-Hop State.
CSCvj88265	CBR8 After SUP failover, some BSOD clients have no service, L2VPN
CSCvj89345	AVC license should be activated only in case of smart licensing model.
CSCvj90089	Device crashes while doing a conference call.

Caveat ID Number	Description
CSCvj90814	Crash due to Memory corruption in Cisco 4000 Series ISRs.
CSCvj92548	FlexVPN: Spoke to Spoke: Implicit NHRP entry due to expired resolution request handling.

Resolved Caveats - Cisco IOS XE Everest 16.6.4

All resolved bugs for this release are available in the Cisco Bug Search Tool.

Caveat ID Number	Description
CSCsd58148	%SEC_LOGIN-4-LOGIN_FAILED does not show username in [user:].
CSCuv14856	WATCHDOG timeout crash during IPSEC phase 2.
CSCuv90519	Map does not get updated with socket change on local address change.
CSCuw90084	DS: Download should print alerts in case of unresolved variables.
CSCvb34443	The ikev2 fragmentation not working with aes-gcm encryption - hmac failure.
CSCvb69966	Memory leak under LLDP Protocol process.
CSCvb88867	Excess BGP Traps Generated just after upgrade.
CSCvd14310	IP TUNNELS: Overlapping Loopback Interface Causes Incorrect Forwarding Decision with AppNav and PfR.
CSCvd47657	Cisco 4000 Series ISRs routers may crashed with Segmentation Fault in AFW Application Process.
CSCvd50613	Cisco 4431 ISR crashes with UNIX-EXT-SIGNAL: Segmentation fault(11), Process = HTTP CP.
CSCvd90410	Router loses RSA keys upon boot with private-config encryption and config archive enabled.
CSCve11959	Memory leak occurs on DHCP client.
CSCve41775	Crash over CCSIP_SPI_CONTROL process due to null pointer / segmentation fault.
CSCve55004	OSPF GIR BASE: not all repair paths calculated for AS ext routes when routes rxed with maxmetric.
CSCve61143	CME SIP sip-ua do not send registration request when vrf forwarding is enabled.
CSCvf05864	BGP RR changes tunnel parameters for bgp evpn route type 3.
CSCvf06123	Route-map not checked when packet is flowing from OUT to IN with Static NAT.
CSCvf07153	SIP Date header format not in GMT Format.
CSCvf07576	Router reloaded when doing show BGP RT filter routes.

Caveat ID Number	Description
CSCvf16374	CME SNR Does not get ringback for PRI calls.
CSCvf19460	CTS Pac download fails with ISE reachability through loopback interface over vrf.
CSCvf23485	DS: Increase the size of command and prompt strings.
CSCvf26916	RTCP/RTP based Media Inactivity timers for MGCP GW do not work in newer releases.
CSCvf38050	Voice Gateway crash due to memory corruption while finding DN index during redirect.
CSCvf49126	Stub is not leaking the network as expected.
CSCvf51773	NHRP redirect overriding routing table.
CSCvf52766	Dual Ringback in Semi-consult transfer on CME.
CSCvf53053	Crash when issuing no dspfarm profile x stuck on DOWN_PENDING state.
CSCvf57090	CUBE automatically considers re-INVITE with a=silenceSupp:off - - - - as fax call.
CSCvf66030	OSPF SR: When SRGB range is changed, mapping server entries do not get re-installed.
CSCvf66860	IOS crash in SOCK TCP Test Server process.
CSCvf70383	Crash in SDP Passthru when T.38 as 1st mline in mid-call SDP.
CSCvf73693	Cisco 4321 ISR crash @ BGP Router for bfd bgp when sending traffic.
CSCvf80363	Rotate nginx access/error log files.
CSCvf81931	Loopback interface not appearing in RIB after upgrade.
CSCvf84528	False "voip_rtp_allocate_port:Possible port leak" errors.
CSCvf88705	Malformed GETVPN message %GDOI-4-COOP_KS_UNAUTH.
CSCvf89894	GETVPN // Primary KS sending rekey first to GM's and then to Secondary KS via scheduled rekey.
CSCvf96009	OSPF SR: When loopback isconfigured with prefix suppression, EPL should be withdrawn.
CSCvf96294	MIB counter for IPSec tunnels does not decrement under high tunnel scale and churn.
CSCvf97908	When NSSA ASBR is reloaded, ECMP to ext routes not installed in other routers.
CSCvf98378	IOSXE_INFRA-6-PROCPATH_CLIENT_HOG: IOS shim client fman stats bipc has taken xx msec.
CSCvg01774	OSPF SSPF: when seg area is disabled and enabled, mapping server EPL entries not re-generated.
CSCvg03444	Hub MC continues to send EIGRP SAF hellos after adjacency removed.

Caveat ID Number	Description
CSCvg05172	Crash in VOIP media loop detection.
CSCvg05452	IOS-XE router crash from memory corruption during CCB cleanup.
CSCvg06142	IPSM Tunnel Entry and Crypto IKMP memory leak due to IKE tunnel entry not deleted.
CSCvg08471	OSPF; process ospf segmentation fault when shut and no shut is performed in active RP.
CSCvg08768	OSPF BGP LS: After fail over, error msg seen: %LSLIB-4-EOD: Producer OSPF-0x0 did not send EOD.
CSCvg12605	Corrupted NOTIFY leads to %CRYPTO-4-IKMP_BAD_MESSAGE, stale ISAKMP SA and traffic failure.
CSCvg16234	ISR receives a control packet (CDP) with a CMD tag it should process it, not drop it
CSCvg18094	GETVPN: show crypto gdoi ks member summary missing last octet in IP address
CSCvg19259	MPLSoFlexVPN: Hub doesn't forward resolution req when default route is advertised to spokes
CSCvg25874	Toggling the switchport then default the interface, load-interval config reapplied
CSCvg30991	IOS-XE routers: Memory leak observed on process ivr: peer_item_t in AFW_application_process
CSCvg32701	Night-Service fails if it overlaps with FAC codes.
CSCvg32858	Snort control plane connectivity with Mgmt-intf is broken.
CSCvg33454	Pass load balancing information in IP header to container.
CSCvg34167	Unexpected reboot of voice gateway Cisco 4400 ISR.
CSCvg34986	Media recording on IOS-XE does not work if a refer is received immediately after the call is answered.
CSCvg36598	ISAKMP Fails When Multiple HSRP tunnel/SVTI Interfaces Configured.
CSCvg39082	Crash after TCP session timeout.
CSCvg41950	Cisco IOS XE Software Diagnostic Shell Path Traversal Vulnerability.
CSCvg43263	when shutting interface with no isis adjacency, local micro-loop avoidance blocks FRR recalculation
CSCvg44135	OSPF SRTE: prefix information is not provided to SRTE when it is learnt via mapping server.
CSCvg45950	packet drop seen intermittently if 40G traffic sent via cts interface
CSCvg47453	Default route redistributed into RIP from EIGRP is not removed from RIP database

Caveat ID Number	Description
CSCvg48470	ISIS l1-l2 redistribution prefix doesnt get redistributed till clear isis rib redistribution is done
CSCvg48492	BE4000 one way audio seen line to trunk side call with VRF enabled
CSCvg51358	DHCPNAK is not sent in roaming scenario.
CSCvg53159	%SNMP-3-RESPONSE_DELAYED: processing GetNext of cafSessionEntry.2 seen on catalyst switch
CSCvg54267	CDP Protocol can run device out of memory
CSCvg56088	Getting "HA Module DSP_MSP reported CALL_MODIFY RECREATE failure" in CUBE HA.
CSCvg56110	Error and pending objects when mma policy flap with egress monitor for multi-VRF case.
CSCvg58096	Increase of dampening penalty on route refresh.
CSCvg58599	Syslog: Logging host is truncating lines causing debug output to be cutoff in the middle of a msg.
CSCvg59604	Cube crashes intermittently multiple times within every two days.
CSCvg61219	Crash seen during Blind Transfer in CME video call
CSCvg67028	VRF deletion status <being deleted> after removing the RD
CSCvg67820	HIGH CPU observation on FMAN RP ESS EVENT TRACING
CSCvg68391	ISIS SR: When seg mpls is shut globally, ISIS SID entries not withdrawn from the entire network.
CSCvg71944	OSPF SR: When loopback is defined as /24 address, EPL should not be sent for the prefix.
CSCvg75315	ASR1K BGP scanner crash when change VRF and BGP configuration
CSCvg75419	ISIS SRTE: Explicit SRTE keeps flapping when ISIS is not the winning route in the RIB
CSCvg76664	OSPF SSPF: With SRTE tunnel, constrained bind of SID0 uses invalid old repair path in some cases
CSCvg76990	Missing LSP sending after configuration change
CSCvg78770	Router resets while processing fragmented/encrypted packet
CSCvg82855	OSPF SSPF: mapping-server strict SID is processed by images which are not strict spf capable
CSCvg84181	"CLID restrict" on outbound leg is setting "Privacy=Full" on inbound leg.

Caveat ID Number	Description
CSCvg85146	OSPFv2 Encoding for local-id in LLS needs to be fixed.
CSCvg85879	BGP sets the wrong Local Preference for routes validated by RPKI server.
CSCvg89163	CUBE does not acknowledge Session-Expires header in UPDATE.
CSCvg91126	BE4K Group pickup failed if agent configured for cfwd no answer
CSCvg91169	3850 standby switch reloads due to configuration-mismatch after use "exception crashinfo" command
CSCvg94978	CUBE Router crashed - Critical software exception, Process = CCH323_CT
CSCvg95213	ISR4k: speed/duplex disappear from 'show run' after shut down & reload.
CSCvg96936	IOS-XE : PAT entry using the same port which is configured for static NAT
CSCvg97010	load-balance advanced moving traffic to fallback path when primary path are not over utilized
CSCvg97824	service-controller - mDNS API's did not free the ID's for mDNS SD HANDLES process.
CSCvg99559	OSPF SSPF/TILFA: TILFA ECMP tunnels are not created when the last segment is adjacency sid.
CSCvh00630	ISRv/QOS - service-policy defined in bootstrap config may not be applied
CSCvh01652	Multicast IPSLA UDP Jitter throws Socket open error if vrf interface is configured on responder
CSCvh02109	WSMA: Server responds with HTTP 404 on wsma-exec with http transport profile
CSCvh03359	EIGRP network statement reappearing after reboot
CSCvh03788	EIGRP Name mode Summary route is not being apply on Virtual-Access on HUB
CSCvh05611	IOSd crash while applying dial peer configuration
CSCvh06249	Crash when receiving EVPN NLRI with incorrect NLRI length field value
CSCvh09334	SDA-IPV6::SISF traceback @ar_relay_create_entry - L2 Binding tbl entry insertion failed
CSCvh09525	CME: BLF monitor function fails intermittently with TCP connection
CSCvh10607	ISG : IETF-Disc-Cause = 0 if DHCP SIP disconnect.
CSCvh15336	OSPF SSPF: ECMP combination of SRTE tunnels and MPLS-TE tunnels does not work properly sometimes.
CSCvh15484	ISIS SR: When the SRGB range is increased, the local SIDs which are in new range are re-installed.

Caveat ID Number	Description
CSCvh18001	Crash due to race condition caused by IOS radioactive trace code.
CSCvh18015	AppNav-XE cluster may cause router crash and reload.
CSCvh21564	AAA Attrbute list leak in Polaris 16.6.2
CSCvh21909	LISP: Overlapping prefix causes "probe-down" for map-cache entry
CSCvh21973	QFP crashed to while sending oversubscribe traffic.
CSCvh22278	OSPF Hello timer 10sec is not applied in network type non-broadcast
CSCvh22300	Update IOS XE OSPFv2 ELL private TLVs to IANA codepoints
CSCvh24315	Memory leak for CCSIP_TCP_SOCKET and CCSIP_UDP_SOCKET on CUBE
CSCvh25624	ISIS SR: When seg mpls is shut under ISIS, sid entries not cleared in the local router.
CSCvh26072	EIGRP SAF Adjacency doesn't form with /31 mask
CSCvh28323	ASR1002HX FP Crash post LNS path switchover
CSCvh29821	CME should send out a refer with notify_clear when night-service is manually disabled
CSCvh30968	ISIS BGP LS: When distribute link state changed from level 1 to level 2, entries not given to BGP LS
CSCvh32216	Sporadic Crashes Due to IPSec (during ISAKMP AAA interaction)
CSCvh32224	8800 KEM module not getting detected on 88XX phones with CME 12,11.6
CSCvh45744	CME Call Park: Dead air experienced on parked PSTN (TDM/FXO) calls
CSCvh48085	OSPF SSPF/SRTE: when we have ABR with multiple interfaces to backbone area, SPF keeps running.
CSCvh48610	IWAN router crash while updating pmi policy.
CSCvh49600	Output "sh sip-ua connections tcp tls detail" shows that CUBE has stuck connection ids.
CSCvh51038	[168] OSPF process crash on P router when router ospf <> is unconfigured on another PE or P router.
CSCvh53691	FP reload with IMGR deregister interface.
CSCvh53764	RP Unexpected reboot when using conditional debugging with CCSIP debug.
CSCvh54672	VRRP doesnt work over Port-channel L3 interface.
CSCvh56594	EIGRP offset-list still active if ACL used in offset-list is removed before offset-list.
CSCvh57061	Cisco 4000 Series ISRs-PPTP passthrough traffic not working with PAT, GRE packet consumed by router.

Caveat ID Number	Description
CSCvh57108	CPUHOG on QoS statistics collection for DMVPN. QoS crash with DMVPN/NHRP.
CSCvh57340	DMVPN: Crypto session stuck into UP-IDLE status after reconfiguring tunnel.
CSCvh57402	Ciso 4451-X ISR sometime drop the packet when volume -based rekey occurred.
CSCvh58909	OSPFv3 cost calculation not correct in some specific topology.
CSCvh61453	NULL remote_hostname from LAC.
CSCvh62532	System reload when clearing cts pac.
CSCvh62615	There is junk entry in route-import table on branch when shutdown/no shutdown WAN interface.
CSCvh63932	Noisy debugs in "periodic" tracelog.
CSCvh66033	IKEv2 - Crash with segmentation fault when debugs crypto ikev2 are enabled.
CSCvh66642	uIDB leaks at the DMVPN hub if the route to remote NBMA is not learned
CSCvh68228	CUBE Unsolicited NOTIFY returns 481 Subscription does not exist
CSCvh70297	Redundancy Mode None does not Sync.
CSCvh70557	CPP crash in MMA.
CSCvh70570	MGCP fallback mode remains ON after CUCM registered.
CSCvh71856	IOSd crash when enabling dot1q in a port-channel sub-interface.
CSCvh72700	CME: GUI user page doesn't load correctly. It is showing "View Window".
CSCvh73805	Explicit SRTE tunnels are not come up when a prefix is redistributed between levels.
CSCvh75132	CPP crash stuck thread detected multikey_hash_replace_int.
CSCvh77733	RR does not send VPNv4 routes to peer.
CSCvh79067	Call Park with standard FAC fails if phones extensions overlap with FAC codes.
CSCvh79640	Cisco 4000 Series ISRs: BDI unreachable when interface has HSRP-enabled subinterfaces.
CSCvh79942	Chunk corruption crash related to PNP or Guestshell.
CSCvh82112	Routers - Memory leak under process RECMSPAPP in IOSd.
CSCvh83215	IOS-XE Voice NIM/PVDM Service-Engine Admin Down leads to one-way audio.
CSCvh85788	Local LAN-only prefix present in master route-import table but not present in site prefix DB.
CSCvh88330	VAI Leaks with IKEv1 DVTI.

Caveat ID Number	Description
CSCvh88975	Performance-monitor does not report classification after tunnel shutdown.
CSCvh92130	Downloaded policies hit by traffics were all gone after the second SSO.
CSCvh92378	High CPU utlization with presence feature when reset is issued under voice register global.
CSCvh93071	Redistributing connected route with AIGP attribute is being continuously readvertised.
CSCvh96542	CCSIP_SPI_CONTRO holding memory increasing.
CSCvh96670	Cisco 4000 Series ISRs packet drop when shutdown or no shutdown interface.
CSCvh97246	Cisco 4000 Series ISRs - ucode crash with fw_base_flow_create.
CSCvh97691	Tacacs-server is missing keyword "key" in argument/option available.
CSCvh97818	The "show voice call <x/y/z>" missing print out dsp statistics in Cisco 4000 Series ISRs.
CSCvh99576	LACP Rate defaults to fast with no way to change it to normal.
CSCvh99651	AAA-Proxy errors in dmiauthd tracelogs.
CSCvh99949	Options Keepalive not triggered on applying profile to dial-peer.
CSCvi01558	iBGP dynamic peer using TTL 1.
CSCvi01650	SIP Out-of-Dialog OPTIONS Ping Group Shows Dial-Peers Marked as None.
CSCvi01805	Router with SIP traffic crashes at ccsip_free_kpml_info.
CSCvi02816	ZBF not able to identify the WAAS optimized flow and drops ACK.
CSCvi03339	[ECA-SIT] IOSd crash seen on xTR with baseline @ sisf_macdb_get_vlanid.
CSCvi04666	ISIS SRTE: SRTE tunnel not created due to R-flag set.
CSCvi05126	ISAKMP Notification messages carry unnecessary data.
CSCvi05408	Memory leak due to asnl.
CSCvi06312	Subsystem stopped: ios-emul-oper-db due to bgp table issue.
CSCvi06480	OSPF SSPF: EPL not sent for secondary addresses on loopback interfaces.
CSCvi06897	The dialpeer matching for inbound SIP profile fails with VRFs.
CSCvi07387	The ip dhcp excluded-address deletion issues via netconf.
CSCvi11123	FMFP-3-OBJ_DWNLD_TO_DP_FAILED error after modifying QoS policy.
CSCvi11665	Virtual-service guest IP accepts broadcast address.
CSCvi11970	Abnormal output for show pnp tech-support.

Caveat ID Number	Description
CSCvi13686	Cisco 4000 Series ISR - Outbound faxes originating from certain fax servers may fail to send.
CSCvi14656	Loss TCA is not generated for traffic with DSCP0 when 0-SLA enabled.
CSCvi15772	The ephone-dn with shared line sip in ESRST GW causing call incoming failure.
CSCvi15950	DTMF fails when mid-call renegotiation changes DTMF method.
CSCvi16306	Cube sends reinvite with annexb=yes even when it receives annexb=no.
CSCvi16454	Router crash due to PuntInject Keepalive Process - kmalloc failures.
CSCvi19685	ISDN - BRI - 'progress_ind command does not work.
CSCvi20882	Netconf IP-SLA udp-jitter case missing leaf codec.
CSCvi21288	PFRv3 RC FIA is not enabeld on interfaces with one of sub-interface with xconnect configuration.
CSCvi24515	IOS-XE - FTP closing connection as NAT device does not process the 230 reply message.
CSCvi26061	RP crash @policymap_associated_to_multiple_instances.
CSCvi26398	"%LISP-4-LOCAL_EID_RLOC_INCONSISTENCY" should be supporessed in SDA context.
CSCvi28362	Unexpected metric value for route redistribution from BGP to OSPF.
CSCvi34260	16.8.1:dot1x Clients stops responding (ping to clinet IP fails) after SSO (CSCvh68810) (PD changes).
CSCvi34314	Cisco ISR:interface down/up does not renew dhcp assigned ip address.
CSCvi35143	Repeatedly Tracebacks seen : %INFRA-3-INVALID_GPM_ACCESS: Invalid GPM Load.
CSCvi35232	CME/BE4K crashes when trying to check help command for new device type BEKEM.
CSCvi35960	VRF aware CUBE fails to send OOD OPTIONS pings.
CSCvi36290	Incorrect BDI configuration state shown by NETCONF on interface creation.
CSCvi38244	IPv6 VRRP Master is using using vlan BIA MAC while sending Neighbor advertisements (NA).
CSCvi38391	H.245 messages are not translated by NAT outside when H.323 video call is initiated from Out-2-In.
CSCvi38916	Persistent Telnet and SSH crashes when configured in 16.6.2.
CSCvi40033	802.1x authentications are failing if there was interface template config applied before.

Caveat ID Number	Description
CSCvi41050	PFRv3 route-control is inconsistently set to "Disabled" on BR devices.
CSCvi41465	All router mcast is removed by "no ipv6 mld router" in specific timing.
CSCvi42002	CDP packets not getting encapsulated over multipoint GRE tunnel.
CSCvi44298	Cisco 4451 ISR Installs 2 IPsec SAs with different peers having same proxy identities.
CSCvi44476	IS-IS unnecessarily updates RIB when in metric-style narrow.
CSCvi48837	Ensure load-balance internet TCs do not match class DEFAULT if configured.
CSCvi50061	Evaluate NTP February 2018 Vulnerabilities.
CSCvi52659	Incorrect "Hop count" obsearbed in IPv6 EIGRP
CSCvi54878	Memory leaks seen at PKI_name_list_add(0xa139cc0)+0x3e
CSCvi55920	ISR 4K Crashes issuing "show call active voice"
CSCvi56463	Unexpected Reset, Crypto IKMP Segmentation fault with IPSec AAA Configuration
CSCvi56919	Radius source interface command is not taking effect on ISR 4k
CSCvi57096	MATM RP Shim Process memory leak @aaa_attr_list_alloc make_a_sublist_max
CSCvi58526	CPUHog and crash on DNS-SRV-1 process
CSCvi61745	Crash when running MPLS Tunnel protection command
CSCvi64534	Remove stack 1+1 CLI for WS-C3850-48XS
CSCvi67613	Protocol type for GRE header doesn't work consistently with "cts sgt inline" enable over auto-tunnel
CSCvi71376	OSPF SSPF: tilfa ALGORITHM fails to compute repair path, reports incorrect reason of too many labels
CSCvi72996	NMR TTL is wrongly considering eid-record of 0.0.0.0/0 for its calculation
CSCvi74088	link local multicast packets are received when the SVI is in down state
CSCvi75086	Rapid TDL memory leak in SMD process leads to crash of active switch in stack for ipv6 clients
CSCvi76084	Device-tracking entry stuck in TENTATIVE for certain Mac Pro hosts configured with static IP
CSCvi77760	SNMP cafSessionMethodState not unsupported after Denali 16.3.3 upgrade on 3850
CSCvi79948	OSPF TILFA: tilfa ALGORITHM preference rules does not pick repair path with lowest number of labels
CSCvi86983	ZBFW HA: active router stuck in cold standby state after shut no shut the wan interface

Caveat ID Number	Description
CSCvi91714	IPv6 address not assigned or delayed when RA Guard is enabled
CSCvi92571	On IOSXE neighbor command under pseudowire interface is rejected
CSCvi93967	EEM: event mat mac-address not triggered on router with NIM-ES2-8-P
CSCvi94425	TBAR issues on KS after running "clear crypto gdoi ks coop role"
CSCvi95775	Reverse-tunnel routes under PMIPv6 MAG config not using configured distance metric
CSCvi96874	ASR1001 has crashed with cgm_avlmgr_find_node
CSCvi96933	mac-move doesn't work on IBNS 2.0 unless you disable it then enable it back
CSCvi97411	Average queue depth calculation tops out prematurely
CSCvi97590	AppNav-XE cause delays for locally source traffic on router
CSCvj00858	CPP Microcode Crash during sRTP Call Encryption
CSCvj01098	Evaluation of IOS-XE and IOS for OpenSSL CVE-2018-0739 and CVE-2018-0733
CSCvj02955	ISR4221 16.6.2 - SIP NAT ALG not sending packets out of WAN interface
CSCvj03263	H225 gatekeeper request dropping under "ALG PARSER" with ZBF
CSCvj04717	OSPF SSPF: With SRTE tunnel scale, SRTE SID0 constraint Label Bind fails with LABEL_BROKER error msg
CSCvj05446	Initial Trustpool installation not successful before PKI is ready
CSCvj06388	Type 7 password parsed incorrectly in dot1x credentials causing auth failure.
CSCvj06909	Reverse-route configuration is unsupported under gdoi crypto map.
CSCvj09541	Cisco 4000 Sereis ISR IOS-XE PBR fails when next hop is recursive over tunnel.
CSCvj14521	Web redirect clients do not get redirected, Create IO ctx, too many intercepted connections.
CSCvj16818	Cisco 4431 ISR crashing immediately following auto-CA certificate renewal.
CSCvj16825	"VoIP dial-Peer is Up" incorrectly log prints at every up interval when server-group is configured.
CSCvj20302	Cisco 4000 Series ISR MTP not performing RFC2833 payload type conversion.
CSCvj21692	UNIX-EXT-SIGNAL: Segmentation fault(11), Process = ACCT Periodic Proc.
CSCvj23301	IOS: Crypto Ruleset fails to get deleted.
CSCvj24940	Voice VRF with No Bind OPTIONS Ping response not sent.
CSCvj27172	Crash during Generic Call Filter Module cleanup

Caveat ID Number	Description
CSCvj27526	BGP attribute map for aggre address can not set attribute.
CSCvj29126	RADIUS client on network fails to solicit PAC key from CTS even though the device has a valid PAC.
CSCvj30023	DNS Debug seen without enabling any debug.
CSCvj38384	%PMIPV6-5-TUNNELDELETE:
CSCvj39346	OSPF SSPF: When sid 0 is removed, wrong implicit-null label used for inter-area prefix.
CSCvj41224	Crash when doing SNMP walk and applying QOS over a GRE tunnel.
CSCvj41550	Default channel operation state changing from I/O to D/O failed when zero-sla enabled.
CSCvj42152	No Audio for SRTP enabled calls in Cisco 4000 Series ISRs.
CSCvj49476	Telnet Sessions Hang/Become unavailable at execution of "show run".
CSCvj50410	Cisco 4331 ISR no collisions count up on duplex mismatch condition.
CSCvj52231	ACEs after an object-group reference not being processed in software if ACL has more than 13 ACEs.
CSCvj52681	Dynamic VLAN assignment causes all sisf entires under the port to be deleted.
CSCvj57502	Memory leak@CENT-BR-0 when change the path label frequently.
CSCvj61603	"dtmf-interworking rtp-nte" command breaking software MTP.
CSCvj65296	"ip rsvp bandwidth" max value llimitation to 10GE

Open Caveats - Cisco IOS XE Everest 16.6.3

All open bugs for this release are available in the Cisco Bug Search Tool.

Caveat ID Number	Description
CSCvf84528	False indication of RTP port leak on Cisco 4000 Series ISRs.
CSCvf89894	GETVPN/Primary KS sending rekey first to GM's and then to Secondary KS via scheduled rekey.
CSCvf96294	MIB counter for IPSec tunnels does not decrement under high tunnel scale and churn.
CSCvg16234	Cisco ISR receives a control packet (CDP) with a CMD tag it should process it, not drop it.
CSCvg43408	IOS-XE Router crashed unexpectedly with critical process fault, fman_fp_image, fp_0_0, rc=134.

Caveat ID Number	Description
CSCvg60185	Cisco 4000 Series ISR discards private RSA key after upgrade and reload with WAAS module.
CSCvg79608	PFR: Overlapping Loopback Interface Causes Incorrect Forwarding Decision with AppNav and PfR.
CSCvh05611	IOSd crash while applying dial peer configuration.
CSCvh09525	CME: BLF monitor function fails intermittently with TCP connection.
CSCvh09620	Continuous crash in "/kernel/mki/src/free" after upgrade to version 15.5(3)S6.
CSCvh24730	PfRv3: Crash while Printing the Same TCA message.
CSCvh26241	Crash after crypto map removal.
CSCvh32216	Sporadic Crashes Due to IPSec (during ISAKMP AAA interaction).
CSCvh32224	8800 KEM module not getting detected on 88XX phones with CME 12,11.6.
CSCvh48610	IWAN router crash while updating pmi policy.
CSCvh49600	Output "sh sip-ua connections tcp tls detail" shows that CUBE has stuck connection ids.
CSCvh50515	Cisoc 4331 ISR crashed due to SA creation failure
CSCvh52882	Memory Leak due to nbar configuration.
CSCvh53691	FP crash with scaled IKE sessions.
CSCvh57108	CPUHOG on QoS statistics collection for DMVPN. QoS crash with DMVPN/NHRP.
CSCvh59195	Ciosc 4000 Series ISR: QFP crashed due to NAT memory leak.
CSCvh66445	Cisco 4000 Series ISR router crashes during status check on WAAS Express.

Resolved Caveats - Cisco IOS XE Everest 16.6.3

All resolved bugs for this release are available in the Cisco Bug Search Tool.

Caveat ID Number	Description
CSCua00661	Memory leak seen while creating vlans using Tclsh.
CSCvc60745	Memory leak - refcount not reduced when packet dropped.
CSCvd04871	Crash after IWAN does a recalculation in the RIB.
CSCvd64670	SCEP enrollment failing with HTTP/1.1 500.
CSCvd97768	Cisco 4000 ISR crashes at sstrncpy using voice.
CSCve08418	IPsec/IKEv2 Installation sometimes fails with simultaneous negotiations.

Caveat ID Number	Description
CSCve32330	A pseudo-random number was generated twice in succession.
CSCve55089	BGP crashes at bgp_ha_sso_enable_ssomode.
CSCve64341	Mid Point LSP creation failure after reload with latest polaris Image.
CSCve66601	Crash is seen in CISCO-SLB-EXT-MIB code.
CSCve75919	In-dialog options ping received post ACK (call completion) cause cube to change codec and no audio.
CSCvf31368	Router crash after EEM-wanfailover script triggered.
CSCvf36269	Cisco IOS and IOS XE Software Plug-and-Play PKI API Certificate Validation Vulnerability.
CSCvf39474	GETVPN: TBAR sync "timer is not running" after KS upgrade causing anti-reply drops and GM outages.
CSCvf48159	Router crash during T38 fax bitrate negotiation.
CSCvf60862	Cisco IOS and IOS XE software IOS daemon Cross-Site scripting vulnerability.
CSCvf68261	Crash when printing IPSEC anti-replay error.
CSCvf84349	Router crash on polling cEigrpPeerEntry.
CSCvg05896	IWAN EIGRP SAF - seq number mismatch after branch reload.
CSCvg07428	PfRv3 triggers List Header leak in FN.F
CSCvg09010	KS merge fails for groups with TBAR due to PST update failure on primary KS.
CSCvg14256	Crash at cc_detect_mute_call.
CSCvg22515	After upgrade of IOS, SSH passwords longer than 25 characters do not work.
CSCvg29183	Cisco 4000 Sereis ISR: XE 16.3.4 - SIP-TDM GW - FLEXDSPRM-3-TDM_CONNECT errors and unexpected reboot.
CSCvg30722	EAPTLS:- Session manger crashing with MKA/EAPTLS session bring up with newly installed certificates.
CSCvg31607	IPv4 PLU mtrie lookup return invalid oce_chain_p.
CSCvg34731	IOS-XE MOS scores always show 4.x even with massive packet loss.
CSCvg38307	CME/BE4000 crash occurs when call is made to invalid SNR destination.
CSCvg40430	Cisco 4431 ISR QFP crashes by a LLC packet received in a serial interface.
CSCvg40784	Session not comming up after certificate expired.
CSCvg52560	Traceback: OCSP creates a large number of lists and triggers a memory problem.

Caveat ID Number	Description
CSCvg60288	Device IP address AV pair replaced with 192.168.1.5
CSCvg71566	"no cdp enable" is rewritten to "no cdp tlv app" after reload.
CSCvg74048	PKI: All SCEP requests fail with "Failed to send the request. There is another request in progress".
CSCvg76912	PnP configuration upgrade failed when IFS returns size 0 for all TFTP files.
CSCvg84039	Traceback: Crash on WAAS menu prompt for WAN Interface.
CSCvg84989	List Header leak with PfR enabled.
CSCvg90226	Crypto Traceback: Router crash at 'Crypto Support' segmentation fault.
CSCvg94908	Mgig stack keeps crashing while configuring with Radius commands
CSCvg98890	IOS-XE GM router might crash after the rekey method is changed from unicast to multicast.
CSCvh00038	Device IP address AV pair replaced with 192.16X.1.X.
CSCvh17481	PKI: Device crash during crl download with multiple CDP URI.
CSCvh32416	Evaluation of all for CPU Side-Channel Information Disclosure Vulnerabil
CSCvh54813	Output Qos policy is removed from Dialer interface after reloading the device if input policy exists.
CSCvh60525	CLI 'aaa common-criteria' not available on IPBASEK9 license.

Open Caveats - Cisco IOS XE Everest 16.6.2

All open bugs for this release are available in the Cisco Bug Search Tool.

Caveat ID Number	Description
CSCvc23012	Ciso 4300 and 4400 ISR Silently Crashes with "Reload Reason:Localsoft" and No Core / Crashinfo File.
CSCvd65197	IOSd crashed when dialer disconnect the ISDN call.
CSCve18549	CME/BE4000 Intermittently Crash when making configuration changes.
CSCve54914	NDSSO vrf ha table to be populated correctly.
CSCve78446	[1661]- Switch number is missing in stack merged logs.
CSCvf33947	CUBE cannot handle mid-call re-invite when midcall-signalling passthrough mediachange is configured.
CSCvf39868	Cisco 4431 ISR crashes while verifying IPv6 CEF scalability.
CSCvf65079	CUBE 1K reloaded with reason: RG-application reload on voice-b2bha RG.

Caveat ID Number	Description
CSCvf68261	Crashes when printing IPSEC anti-replay error.
CSCvf70383	Crashes in SDP Passthru when T.38 as 1st mline in mid-call SDP.
CSCvf71066	Router crash due to memory corruption in PKI.
CSCvf84349	Router crashes on polling cEigrpPeerEntry.
CSCvf89399	Flexible NetFlow crash.
CSCvf93129	Mid-call failure because all available Crypto is not Offered in SDP.
CSCvg05452	IOS-XE router crash from memory corruption during CCB cleanup.
CSCvg09010	KS merge fails for groups with TBAR due to PST update failure on primary KS.
CSCvg15158	DMVPN session get stuck in NHRP and UP-NO-IKE state without active IKEv2 session until rekey.
CSCvg16357	Copying file larger than 2GB to FTP destination fails with "Invalid argument."
CSCvg19259	MPLSoFlexVPN: Hub doesn't forward resolution req when default route is advertised to spokes.
CSCvg28614	Cisco 4000 Series ISR traceroute is abnormal although communication is OK.
CSCvg29183	Cisco 4000 Series ISRs - XE 16.3.4 - SIP-TDM GW - FLEXDSPRM-3-TDM_CONNECT errors and crash.
CSCvg30928	Management ARP entry disappears after a period of time.
CSCvg33403	Incoming call fails with 'Lower layer disconnected call cause=47' error.
CSCvg34685	IKEv1 Stuck Virtual-access interface&RRI 15.4(3)s6.
CSCvg34889	IKEv2 VPN tunnel does not establish when destiantion ip address changes during the AUTH exchange.
CSCvg38307	BE4K crashed @ContactingDest_SnrOtherDestroyDone
CSCvg40430	4431 QFP crashes by a LLC packet received in a Serial Interface

Resolved Caveats - Cisco IOS XE Everest 16.6.2

All resolved bugs for this release are available in the Cisco Bug Search Tool.

Caveat ID Number	Description
CSCuv47069	DHCP crashed when configure a manual binding in an interface.
CSCux22473	IPv6 Tracking for route learned from IBGP Neighbor is Down.
CSCuy09470	ISIS hello stops to be sent after RSP switchover.

Caveat ID Number	Description
CSCvc78492	DMVPN : IOS-XE - Unable to pass traffic if spoke to spoke fails to build in phase 2.
CSCvd16501	High CPU due to SNMP ENGINE when polling mplsTunnelHopEntry.
CSCve00909	16.6 : Ping failure on re-add of ip address to Dialer Interface.
CSCve07263	IPSec Tunnel stuck in Up/Down state after shut/no-shut - VPN Interop.
CSCve09104	Command "segment-routing mpls" under router isis 1 not getting NVGEN'd.
CSCve13491	Router might crash due watchdog when creating a new swidb at if_index_allocate_index.
CSCve15722	The second and later PfRv3 VRF configs are missing after reload.
CSCve23090	16.6 OBS: Local LFA is used incorrectly when TI-LFA Node Protection enabled.
CSCve35209	16.6:Kignpin @ Kernal errors kernel-source/kernel/softirq.c:150 __local_bh_enable_ip+0x3b/0x9c().
CSCve47826	Memory leak Crypto IKEv2 at ikev2_ios_psh_set_route_info.
CSCve51657	Slow convergence with scale after a core link flaps.
CSCve53984	Cisco 4300 ISR crashed while importing certificate.
CSCve54486	Crash when attempting to assign nonexistent/shutdown VLAN to 802.1x port.
CSCve57788	Web authentication clients do not receive redirect URL and HTTP Intercept, Invalid appl_id error smd.
CSCve62353	Startup-config missing after power outage.
CSCve64336	RSP1-Continous ESMC tracebacks observed after IMA8T OIR followed by SSO.
CSCve66119	Router crash due to process "Crypto Support" segmentation fault.
CSCve68911	Nested Enhanced Route Refresh requests triggers Stale Prefixes.
CSCve76827	NAT policy-map that is large takes long time to download.
CSCve76945	:Router crashed when a sh bgp command was executed.
CSCve77011	SSL handshake failure when validating certification with name-constraints.
CSCve78101	Inconsistent Behavior on Link states with different SFP's plugged into the module.
CSCve81985	Subscriber session not synced to standby while assigning static ip in DHCP.
CSCve89668	Router crashed when "clear ip bgp vpnv4 u update-group <nei>.
CSCve90812	Cisco 4431 ISR drops all received packets due to CRC error after power off/on.
CSCve94399	Router crash when importing BGP routes - EVPN.

Caveat ID Number	Description
CSCve95243	Internal interface missing from L2FIB output list.
CSCve97061	Unable to remove 'mpls tp' configuration from Router.
CSCve98056	ESP ucode crash with ALG for PPTP traffic and PAP is enabled.
CSCve98223	Two PW-Group switchover notifications are triggered from PI to PD for a single event.
CSCvf02131	IP SLA can trigger crash when used with MPLS probe.
CSCvf03810	Cisco 4221 ISR boot loop when Gig0/0/0 up
CSCvf05616	Traffic drop, on reconfiguring l2vpn sessions after sso on peer.
CSCvf11237	Memory leak seen@crypto_init_show_instance.
CSCvf11776	VRRPv3 with VRRS remains NOT READY after shutdown Port-channel IF.
CSCvf12746	Cisco 4331 ISR packet drop when shut/no shut interface that not transport traffic.
CSCvf16448	No all IPv6 GRE crypto tunnels may come up or recover from flapping at scale.
CSCvf18162	Crash observed in Mlpp-Bacd scenario.
CSCvf18470	IOS-XE CUBE HA crash.
CSCvf19607	Cisco 4000 Series ISR not correctly handling forked 18X responses with SDP.
CSCvf24607	Ipsec Session Fail After Up/down Link Between Dmvpn Tunnel.
CSCvf24713	Stale path message for that prefix is noticed when dampening is configured.
CSCvf27072	NBAR not working on 16.5.1a in switch if name-server is configured.
CSCvf29213	PFRV3: Site Prefix shows unreachable after removing and adding the specific route for the prefix.
CSCvf30703	Watchdog crash at sla_resp_config_command when executing the "show run" command.
CSCvf30772	Cisco 4331 ISR - ATM - T1 CAS - One Way Audio: Dropping Packets due to Tail Drop
CSCvf33443	FEW Inter xTR roam scale 400/sec hit on CSR1KV-Map server causes delay in L2&L3 lisp updates to xTR.
CSCvf33570	Crash while BGP-RR Unconfiguration.
CSCvf34835	IOS-XE GETVPN KS crashes while sending cgmGdoiKeyServerRegistrationComplete trap after GM reg.
CSCvf35507	Crash in SSH Process due to SCP memory corruption.
CSCvf40147	C9300: ASIC Ballot failed message seen on during bootup in overnight reload test

Caveat ID Number	Description
CSCvf40983	TSN-H: Sometimes boot C1111-8PLTEW and see the DHCPD receive traceback in the log
CSCvf41539	CAT3K SDA border/LISP crashed with segmentation fault
CSCvf42300	ISIS SR: segmentation fault in ISIS when "no seg mpls" command is given.
CSCvf44501	ISR4K slow responsiveness when interface state goes from UP to DOWN compared to Cat6880X
CSCvf44638	Numbered extended IP ACLs break config sync
CSCvf51341	Crash after show ip ospf database summary command
CSCvf54314	Crashes due to a null pointer dereference on htsp structure.
CSCvf59923	DNS : Split DNS reg-expression issue in IOS-XE (16.x).
CSCvf62916	Router crashes when doing "show ip bgp neighbor" on a flapping BGP neighborship.
CSCvf63541	BGP with global import/export crashes when several nbrs deleted simultaneously.
CSCvf64377	Ping fail with many ACL rules and dialer profiles configured when using ISDN DDR on Cisco 4000 Series ISR.
CSCvf65643	Unicast ping stops working when "ip pim sparse-mode" removed from SVI.
CSCvf68602	E1r2-Cas is not working when adding "invert-abcd 1 0 0 0"
CSCvf69272	SNMP ENGINE high CPU usage observed with 1.3.6.1.2.1.185.1.1.1(mgmdHostInterfaceEntry).
CSCvf73320	Cisco 4431 ISR crashes while finding NDR with max oif number per multicast grp at scale.
CSCvf74154	SGACL: cpp_sp_svr crash during CFM EDIT request with reseq_enable = TRUE.
CSCvf74829	CRL download fails due to "failed to create getcacert message".
CSCvf76512	Option 82 circuit-id-tag restricted by 6 bytes.
CSCvf76535	B2B NAT HA: Stale NAT translations stuck on primary router after communication loss with standby.
CSCvf80495	IPv6 BGP network advertized not seen in the peer.
CSCvf80757	NETCONF-YANG/RESTCONF edit config fails silently, subsequent get config reports false-positive.
CSCvf88590	After disabling http server/https server on netconf, IP-Adm-V4-Int-ACL-global delete.
CSCvf89608	Missing ip route to cellular interface after router reload or modem power cycle.
CSCvf92057	CUBE is unable to send PRACK to Skype server for inbound calls.

Caveat ID Number	Description
CSCvf94948	Cisco 4331 ISR: Input policy-map classify traffic incorrectly.
CSCvf95077	Stale Mac entry in MLRIB.
CSCvf95141	ZBF crashes on standby.
CSCvf96035	ISIS redistribute connected not working for IPV6 routes.
CSCvg03498	The "copy run start all" makes the router stuck.
CSCvg06514	BE4K crashed due to CS_Placecall_Sharedln.
CSCvg08979	Martian check for distance command needs to be removed.
CSCvg13049	ISR G2: dot1p marking fails if service-policy applied on the Dialer.
CSCvg31493	Stale Mac entry in MLRIB.
CSCvg31495	NMR calculation is wrongly considering eid-record of 0.0.0.0/0 in SDA.

Open Caveats - Cisco IOS XE Everest 16.6.1

All open bugs for this release are available in the Cisco Bug Search Tool.

Caveat ID Number	Description
CSCve95037	Traceback found for PLATFORM_INFRA-5-IOS_INTR_OVER_LIMIT part 2
CSCvf23190	IPSec install failing with dynamic crypto map scale.
CSCve90812	Cisco 4431 ISR drops all received packets due to CRC error after power **OFF** and **ON**.
CSCvf12746	Cisco 4331 ISR packet drops when the **shut/no shut** interface does not transport traffic.
CSCve92165	Packet drop issue is seen on Cisco 4000 Series ISR with EVC configuration.
CSCve62353	Startup configiration is missing after the power outage.
CSCvf24588	Cisco 4331 ISR Fman_Fp crashes with just a single tunnel configured.
CSCvf27563	Cisco 4000 Sereies ISR crashes in fman_fp during IPSec flow deletion.
CSCvf02875	Reducing the memory utilized by ISR-WAAS-200.
CSCve45274	A Cisco router may crash when issuing the **'show dmvpn detail | in Virtual-Access** with up/down|INTF.
CSCuv90519	Map doesn't get updated with socket change on local address change.
CSCvf16626	IWAN router crash while updating pmi policy.
CSCvc46230	PfRv3: Unexpected reload while evaluating/moving TC's between channels.

Caveat ID Number	Description
CSCvf18856	Cisco 4000 Series ISR with SM-X - Switch module does not recover gracefully following bcm crash.
CSCve99492	DMVPN Ph-2: spoke to spoke traffic drops, NHRP entry incomplete, if crypto session fails to come up.
CSCve89095	Cisco 4221 ISR router crashed on fw_icmp6_get_ntuple.
CSCve69182	Logs filled with conn_array_empty messages
CSCvc89226	Connection goes down randomly on Cisco 4321 ISR/K9.
CSCvf27566	OpenDNS local-domain bypass on Cisco 4000 Series ISR stop working after reboot.

Resolved Caveats - Cisco IOS XE Everest 16.6.1

All resolved bugs for this release are available in the Cisco Bug Search Tool.

Caveat ID Number	Description
CSCuu68879	Cisco 4300 ISR shows abnormal large RTT/jitter value in IP SLA udp-jitter v2/v3.
CSCvd19860	OSPFv3 AUTH breaks IPv6 traffic intermittently
CSCve71068	The **show platform software cerm-information** command is not displaying the statistics information.
CSCve47826	Memory leak Crypto IKEv2 at ikev2_ios_psh_set_route_info.
CSCve20522	The **show crypto map** command displays incorrect wildcard mask for crypto access-list.
CSCvf11237	Memory leak is seen at crypto_init_show_instance.
CSCve63482	Phase1 comes up and DPDs being exchanged even if the tunnel interface is shut down.
CSCvc79296	Redundancy inter-device is not working with security ipsec.
CSCve66119	Router crash due to process Crypto Support segmentation fault.
CSCvd97524	Fixed versions for CSCuz15131 crash when traffic with maximum size is on wire.
CSCve14080	Error message "LID: Handle 0x0 is invalid" filling console logs
CSCve77011	SSL handshake failure when validating certification with name-constraints
CSCve74862	Crash due to memory corruption when using PNP feature
CSCve76827	large NAT policy-map takes long time to download

Related Documentation

Platform-Specific Documentation

For information about the Cisco 4000 Series ISRs and associated services and modules, see:

Documentation Roadmap for the Cisco 4000 Series ISRs,Cisco IOS XE 16.x .

Cisco IOS Software Documentation

The Cisco IOS XE Everest 16.x software documentation set consists of Cisco IOS XE Everest 16.x configuration guides and Cisco IOS command references. The configuration guides are consolidated platform-independent configuration guides organized and presented by technology. There is one set of configuration guides and command references for the Cisco IOS XE Everest 16.x release train. These Cisco IOS command references support all Cisco platforms that are running any Cisco IOS XE Everest 16.x software image.

See http://www.cisco.com/en/US/products/ps11174/tsd_products_support_series_home.html

Information in the configuration guides often includes related content that is shared across software releases and platforms.

Additionally, you can use Cisco Feature Navigator to find information about feature, platform, and software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn . An account on cisco.com is not required.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

© 2017 Cisco Systems, Inc. All rights reserved.