Release Notes for Cisco 4000 Series ISRs, Cisco IOS XE Fuji 16.7.x

First Published: 2017-11-17

Last Modified: 2017-11-17

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).

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.

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 2 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 4000 Series ISRs	Existing RoMmon	Cisco Field-Programmable Devices
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 3
- Cisco ISR-WAAS and AppNav-XE Service, on page 3
- USB Etoken, on page 4

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 Fuji 16.7

This section describes new features in Cisco IOS XE Fuji 16.7 that are supported on the Cisco 4000 Series ISRs.

New and Changed Information

New Hardware Features in Cisco IOS XE Fuji 16.7.1

No new hardware features were introduced for Cisco 4000 Series ISRs in Cisco IOS XE Fuji 16.7.1.

New Software Features in Cisco 4000 Series ISR Release Cisco IOS XE Fuji 16.7.1

The following features are supported by the Cisco 4000 Series Integrated Services Routers for Cisco IOS XE Fuji 16.7.1:

- For information on migrating from existing Cisco IOS XE 3S releases to the Cisco IOS XE Fuji 16.7.1 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.
- Assign Metrics to Routes Learned from DHCP—On a DHCP client, if the client receives static routes via option 121, the route can be added to the routing table with a configured route-distance value. Use the ip dhcp client route distance number command in interface configuration mode for the static routes to use the route metric from the configured value instead of the default value. If this command is not configured , the route distance would be considered as 254, which is the default value. Also, if the command is configured with its default value of 254, then the command would not be shown in the currently running configuration (show running-config command) as it is the default behavior.
- Anti-replay QoS/IPSec Packet Loss Avoidance—For detailed information, see the following Cisco document:http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dplane/configuration/xe-16-7/sec-ipsec-data-plane-xe-16-7-book/sec-ipsec-antireplay.html#GUID-C63760A0-ADC9-4234-AF59-8411260E0F35.
- Boost Performace License—For detailed information, see the following Cisco document:https://www-author3.cisco.com/c/en/us/td/docs/routers/access/4400/software/configuration/xe-16-8/isr4400swcfg-xe-16-8-book/installing_the_software.html#concept_EE11CBA65D814447BD6913EF89E8D0C3.
- Cisco Smart Licensing for Unified SRST—For detailed information, see the following Cisco document: https://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.
- 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-16-7/sec-data-encrypted-traffic-analytics-xe-16-7-book.html and https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Campus/CVD-Encrypted-Traffic-Analytics-Deployment-Guide-2017DEC.pdf.
- ETA - 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/sec_data_eta/configuration/xe-16-7/sec-data-encrypted-traffic-analytics-xe-16-7-book/sec-data-encrypted-traffic-analytics-xe-16-6-book_chapter_01.html .
- Enable Allowed list 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/sec_data_eta/configuration/xe-16-7/sec-data-encrypted-traffic-analytics-xe-16-7-book/sec-data-encrypted-traffic-analytics-xe-16-6-book_chapter_01.html.
- ETA Allowedlist Support— 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-16-7/

sec-data-encrypted-traffic-analytics-xe-16-7-book/sec-data-encrypted-traffic-analytics-xe-16-6-book_chapter_01.html.

- IOx Tracing and Logging— Allows a guest application to run separately on the host device that helps with reporting the logging and tracing of the data to the host. For detailed information, see the following Cisco document: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/167/b_167_programmability_cg.html.
- ISIS - Advertise Max SID Depth in LSPs and to LSLIB—For detailed information, see the following Cisco document: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/seg_routing/configuration/xe-16-7/segrt-xe-16-7-book/sr-ad-max-SID-depth-is-is-ospf-bgp-ls.html.
- Model-Driven Telemetry—Provides a mechanism to stream data from a Model-Driven Telemetry-capable device, to a destination. The data to be streamed is driven through subscription. The feature is enabled automatically, when NETCONF-YANG is started on a device.
- NBAR2 Support AVC on TSN Routers—For detailed information, see the following Cisco document: NBAR2 support – Support added in this release for Cisco Network-Based Application Recognition (NBAR2). NBAR2 analyzes network traffic and identifies the application source of the traffic. This enables application-based network policies, and is one part of Cisco Application Visibility and Control (AVC).
- OSPF-Redistribution to and from RIB—For detailed information, see the following Cisco document: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/seg_routing/configuration/xe-16-7/segrt-xe-16-6-book/sr-routing-info-base-support.html.
- OSPF - Advertise Max SID Depth in LSAs and to LSLIB—For detailed information, see the following Cisco document: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/seg_routing/configuration/xe-16-7/segrt-xe-16-7-book/sr-ad-max-SID-depth-is-is-ospf-bgp-ls.html.
- Secure Unified SRST on Cisco 4000 Series Integrated Services Routers—For detailed information, see the following Cisco document: https://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_secure_sccp_and_sip.html.
- Umbrella Resolver for IWAN DCA—For detailed information, see the following Cisco document: https://www-.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_utd/configuration/xe-16-7/sec-data-umbrella-branch-xe-16-7-book.html .
- Unified SRST with SIP Trunks (Unified SRST and Unified Border Element Co-location)—For detailed information, see the following Cisco document: https://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_sip_trunking.html.
- 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/1671. 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.
- 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 Fuji 16.7.1:
  - Configuring AAA Authentication
  - DHCP Enchancements
  - NetFlow Configuration

- Software Upgrade Enchancements
- For information on how to access the Web User Interface, see Configure the Router for Web User Interface section.

Configure the Cellular Back-off Operation

For a router with 3G/4G interface, sometimes service provider network might be busy, congested, in maintenance or in fault state. In such circumstances, service provider network rejects session activation request from the router by returning reject cause code 33 as a response of the activation request. After the router receives the reject cause, the router uses the back-off operation with the pre-defined timer value which could be carrier-specific. While back-off operation is in progress, no new session activation request is sent out from the router. After the back-off period is up, new session activation request is sent out from the router.

Note: There is no command to disable the cellular back-off feature on the router.

The following example shows how to configure the cellular back-off feature to stop continuous session activation requests back to the router:

```
Router#show cell 0/2/0 all
Profile 1, Packet Session Status = INACTIVE
Profile 2, Packet Session Status = INACTIVE
Profile 3, Packet Session Status = INACTIVE
.
.
.
Success rate is 0 percent (0/5)
Router#show cell 0/2/0 c
Profile 1, Packet Session Status = INACTIVE
Profile 2, Packet Session Status = INACTIVE
Profile 3, Packet Session Status = INACTIVE
RouterCall end mode = 3GPP
RouterSession disconnect reason type = 3GPP specification defined(6)
RouterSession disconnect reason = Option unsubscribed(33)
RouterEnforcing cellular interface back-off
 Period of back-off = 1 minute(s)
Profile 4, Packet Session Status = INACTIVE
...
Profile 16, Packet Session Status = INACTIVE

.
.
.
Profile 16, Packet Session Status = INACTIVE
```

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.
- You can use the Cisco IOS CLI to enter the necessary configuration commands. To use this method, see Entering the Configuration Commands Manually, on page 8.

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 Fast Ethernet 0 configured.

```
Router(config)# int FastEthernet0
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 Fuji 16.7.2

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

Caveat ID Number	Description
CSCve08418	IPsec/IKEv2 Installation Sometimes Fails With Simultaneous Negotiations
CSCve94399	router crash when importing BGP routes - EVPN
CSCvf89894	GETVPN // Primary KS sending rekey first to GM's and then to Secondary KS via scheduled rekey.
CSCvg05599	Router does not recalculate UDP checksum after NAT
CSCvg09010	KS merge fails for groups with TBAR due to PST update failure on primary KS
CSCvg90226	Crypto Traceback: Router crash at 'Crypto Support' segmentation fault
CSCvg98890	IOS-XE GM router might crash after the rekey method is changed from unicast to multicast
CSCvh32216	Sporadic Crashes Due to IPSec (during ISAKMP AAA interaction) .
CSCvh57061	Cisco 4000 Series ISRs:PPTP passthrough traffic not working with PAT, GRE packet consumed by router. .
CSCvh59195	Cisco 4000 Series ISRs: QFP crashed due to NAT memory leak.
CSCvi16454	Router crash due to PuntInject Keepalive Process - kmalloc failures.
CSCvi32156	Router crashes when DMVPN tunnel moves accoss ports.
CSCvi70934	SYS-3-INVMEMINT: Invalid memory action prior crash with MoH + route list.
CSCvi90964	Cisco 4331 ISR: Crash due to Segmentation fault(11), Process = Tunnel Security.
CSCvj02955	Cisco 4221 ISR - SIP NAT ALG not sending packets out of WAN interface .
CSCvj27172	Crash during Generic Call Filter Module cleanup.
CSCvj29593	Debug platform condition start causes keepalive failures with Vasi interface.
CSCvj37428	LPCOR FAC on ISR 4K throws Traceback for call.

Caveat ID Number	Description
CSCvj46153	Memory corruption after non zero REFCOUNT during IPSEC sibling allocation.
CSCvj56471	Memory leak under CCSIP_UDP_SOCKET / MallocLite.

Resolved Caveats - Cisco IOS XE Fuji 16.7.2

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

Caveat ID Number	Description
CSCuv90519	Map does not get updated with socket change on local address change.
CSCuv91356	IOS XE for Cisco 4000 ISR Routers Privileged EXEC Mode Root Shell Access Vulnerability.
CSCvb34443	IKEV2 fragmentation not working with aes-gcm encryption - hmac failure.
CSCvd04871	The device crashes after IWAN does a recalculation in the RIB.
CSCvd90560	Incorrect channel next-hop for branch to branch traffic.
CSCve15722	The second and later PfRv3 VRF configurations are missing after reload.
CSCve55089	BGP crashes at bgp_ha_sso_enable_ssomode.
CSCvf07576	Router reloads when doing show BGP RT filter routes.
CSCvf16626	IWAN router unexpectedly reboots while updating pmi policy.
CSCvf29213	PFRV3: Site Prefix shows unreachable after removing and adding the specific route for the prefix
CSCvf51773	NHRP redirect overriding routing table
CSCvf59201	IP SLA tracks are down, but IP reachability is up
CSCvf63541	BGP w/global import/export crashes when several nbrs deleted simultaneously
CSCvf70383	Crash in SDP Passthru when T.38 as 1st mline in mid-call SDP
CSCvf71358	NBAR First Packet Classification fails with AppNav enabled
CSCvf73693	isr4321 crash @ BGP Router for bfd bgp when sending traffic
CSCvf84349	Router crash on polling cEigrpPeerEntry
CSCvf93129	Mid-call failure because all available Crypto is not Offered in SDP
CSCvf98378	IOSXE_INFRA-6-PROCPATH_CLIENT_HOG: IOS shim client 'fman stats bipc' has taken 278 msec
CSCvg02533	router crashed after triggers with debug

Caveat ID Number	Description
CSCvg03981	IOS-XE NAT: IP header of tunneled traffic is translated twice (in inner and outer header)
CSCvg05172	Crash in VOIP media loop detection
CSCvg05452	IOS-XE router crash from memory corruption during CCB cleanup
CSCvg05896	IWAN EIGRP SAF - seq number mismatch after branch reload
CSCvg07428	PfRv3 triggers List Header leak in FNF
CSCvg08471	OSPF; process ospf segmentation fault when shut and no shut is performed in active RP.
CSCvg09138	Interface duplex and flow-control settings are not getting displayed
CSCvg14256	Crash at cc_detect_mute_call
CSCvg16234	ISR receives a control packet (CDP) with a CMD tag it should process it, not drop it
CSCvg19259	MPLSoFlexVPN: Hub doesn't forward resolution req when default route is advertised to spokes
CSCvg28614	ISR4k dialer interface traceroute is abnormal although communication is OK
CSCvg30991	IOS-XE routers: Memory leak observed on process ivr: peer_item_t in AFW_application_process
CSCvg31373	ISR4k Error Msg (SYS-2-CHUNKEXPANDFAIL: Could not expand chunk pool for ASR1000 SPA TDL)
CSCvg31607	IPv4 PLU mtrie lookup return invalid oce_chain_p
CSCvg31929	Extended the retries on UCSE before NGIO control packet loss is detected
CSCvg32099	Active call status is displaying as 0 when resume in remote for the first time
CSCvg32105	Memory Leak in fman_fp_image when NBAR is configured
CSCvg33403	Incoming call fails with 'Lower layer disconnected call cause=47' error caused by T.38 calls
CSCvg33454	Pass load balancing information in IP header to container
CSCvg34167	Unexpected reboot of voice gateway 4400ISR
CSCvg34731	IOS-XE MOS scores always show 4.x even with massive packet loss.
CSCvg36246	SM-X-ES3's port connected to Ethernet-Internal x/0/0 always become block port.
CSCvg38307	CME/BE4000 crash occurs when call is made to invalid SNR destination.
CSCvg38872	Crash observed while sending 40K 4Kb pkt size html session with ETA configured on ESP 100.

Caveat ID Number	Description
CSCvg40085	Cisco 4000 Series ISR - IOSd crash with SIGABRT with CCVPM_HTSP.
CSCvg45247	Site-prefix learning: Unexpected Reboot in 'IP RIB Update' Process after 'no domain default'
CSCvg48492	BE4000 one way audio seen line to trunk side call with VRF enabled
CSCvg52560	Traceback: OCSP creates a large number of lists and triggers a memory problem.
CSCvg54149	TCP socket flap due to keepalive timeout with message stuck in queue for Multi-VRF dual BR setup.
CSCvg59604	Cube crashes intermittently multiple times within every two days.
CSCvg60721	Cisco 4451 ISR crashes when MobileIP receives SNMP trap.
CSCvg61219	Crash is seen during Blind Transfer in CME video call.
CSCvg62161	Prefix SID delete after SSO.
CSCvg74048	PKI: All SCEP requests fail with "Failed to send the request. There is another request in progress".
CSCvg76706	BGP does not take into account the lowest IP NH for duplicate MAC RT 2 with same seq # for BP calc.
CSCvg78665	Cisco 1100 ISR Pause frame generation not working.
CSCvg84989	List Header leak with PfR enabled.
CSCvg85879	BGP sets the wrong Local Preference for routes validated by RPKI server.
CSCvg94908	Mgig stack keeps crashing while configuring with radius commands.
CSCvg94978	CUBE Router crashed - Critical software exception, Process = CCH323_CT.
CSCvg95213	Cisco 4000 Series ISR: speed/duplex disappear from 'show run' after shut down and reload.
CSCvg97010	Load-balance advanced moving traffic to fallback path when primary path are not over utilized.
CSCvh02294	Cisco 4000 Series ISR SW MTP configured as TRP does not relay sRTCP messages.
CSCvh04245	TDM-IP, QoS marking is varying to 0 and EF for the same RTP stream.
CSCvh05575	Cisco 4000 Series SCCP Process Does Not Wait for All PVDM Modules to Come Up Before Registering
CSCvh05611	IOSd crash while applying dial peer configuration.
CSCvh06249	Crash when receiving EVPN NLRI with incorrect NLRI length field value.
CSCvh17481	PKI: Device crash during crl download with multiple CDP URI.

Caveat ID Number	Description
CSCvh21973	QFP crashed to while sending oversubscribe traffic.
CSCvh24315	Memory leak for CCSIP_TCP_SOCKET and CCSIP_UDP_SOCKET on CUBE.
CSCvh26277	T38 faxes fail is going IP to PRI when it is cooming from A BDI with DOT1Q tagging.
CSCvh28859	Interoperability failure between some Fortitude Ports and some SmartJack cards.
CSCvh47443	Spoke-to-spoke site-prefix reachability checking should be removed.
CSCvh48610	IWAN router crashes while updating pmi policy.
CSCvh51038	OSPF process crashes on P router when the router ospf is unconfigured on another PE or P router.
CSCvh57050	IGMP multicast SSM-map with DNS does not work with IGMPv3. .
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	Cisco 4451-X ISR sometime drop the packet when volume -based rekey occurred.
CSCvh58909	OSPFv3 cost calculation not correct in some specific topology.
CSCvh66033	IKEv2 - crashes with segmentation fault when debugs crypto ikev2 are enabled.
CSCvh69641	Cisco 4000 Series ISR Core file seen @cvmx_pow_work_response_async.
CSCvh70557	CPP crashes in MMA. .
CSCvh79640	Cisco 4000 Series ISRs: BDI unreachable when interface has HSRP-enabled subinterfaces.
CSCvh82112	Memory leak under process RECMSPAPP in IOSd.
CSCvh91443	Cisco 4000 Series ISR crashed due to CPUHOG Net background.
CSCvh92378	High CPU utlization with presence feature when reset is issued under voice register global.
CSCvh97818	The show voice call <x/y/z> missing print out dsp statistics in Cisco 4000 Series ISR.
CSCvi01558	iBGP dynamic peer using TTL 1.
CSCvi02816	Zone-based Firewall not able to identify the WAAS optimized flow and drops ACK.
CSCvi05408	Memory leak due to asnl.
CSCvi06312	Subsystem stopped: ios-emul-oper-db due to bgp table issue.
CSCvi06897	Dialpeer matching for inbound SIP profile fails with VRFs.

Caveat ID Number	Description
CSCvi08470	OSPF: process crashed when the interface priority is configured for 0.
CSCvi08933	Crash processing MMA punt records.
CSCvi11884	Cisco 4000 Series ISR: After issuing RELOAD command, inerfaces keep up for tens of seconds.
CSCvi34314	Cisoc 1100 ISR: interface down/up does not renew dhcp assigned ip address.
CSCvi35232	CME/BE4K crashes when trying to check help command for new device type BEKEM.
CSCvi35609	Cisco 4431 ISR do not update mac address after STP topology changed.
CSCvi35960	VRF aware CUBE fails to send OOD OPTIONS pings.
CSCvi38923	Cisco 4300 Series ISR dataplane crash during packet drop.
CSCvi44988	Cisco 1111 IS -8P: random commands may trigger TACACS+ to crash
CSCvi54878	Memory leaks seen at PKI_name_list_add(0xa139cc0)+0x3e.
CSCvi55920	Cisco 4000 Series ISR crashes issuing **show call active voice** command.
CSCvi74088	Link local multicast packets are received when the SVI is in down state.
CSCvi81216	Cisco 4000 Series ISR: LISP Ping src Looback(lo is EID) has been dropped after reloading.
CSCvi83419	Router crash when removing route-target and with hard clear.
CSCvi97411	Average queue depth calculation tops out prematurely .
CSCvj11198	Threat Defense screen is not displayed in Web GUI.
CSCvj16818	Cisco 4431 ISR crashing immediately following auto-CA certificate renewal.
CSCvj17682	MAC filtering incorrectly set on builtin ports of Cisco 4300 ISR.
CSCvj23301	IOS: Crypto Ruleset fails to get deleted.

Open Caveats - Cisco IOS XE Fuji 16.7.1

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

Table 2:

Caveat ID Number	Description
CSCvg79164	RP_0_iomd crash @ iomd_ipc_send
CSCvf80101	CM JM procedure is not triggered on dm814x.

Caveat ID Number	Description
CSCvg03981	IOS-XE NAT: IP header of tunneled traffic is translated twice (in inner and outer header).
CSCvg34783	Voice-port command compand-type is remove during a reboot.
CSCvg39934	SL mode, unthrottled configuration and relaod without saving puts the system in inconsistent state.
CSCvg46819	SVTI tunnel,unthrottled configured,sending 65 byte PKT, IPsecTail Drops are seen with QFP util at 95

Resolved Caveats - Cisco IOS XE Fuji 16.7

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

Caveat ID Number	Description
CSCuu86175	Cisco 4000 Series ISRs: CUBE and Zone-based Firewall interoperability issues are seen when co-located on the same router.
CSCvb29204	BenignCertain on IOS and IOS-XE.
CSCvf24607	Ipsec Session Fail After Up/down Link Between Dmvpn Tunnel.
CSCvf68261	Crash when printing IPSEC anti-replay error.
CSCvf69191	UTD: iosd crash Process = Connected Apps CLI Print Server.
CSCvf74829	CRL download fails due to "failed to create getcacert message".
CSCvf76535	B2B NAT HA: Stale NAT translations stuck on primary router after communication loss with standby
CSCvf80268	IKEV2 ipsec proposal response/accept can fail validation.
CSCvf82376	Crash when removing "crypto map ipv6" and then related IPv6 ACL.
CSCvf94948	Cisco 4331 ISR Input policy-map classify traffic incorrectly.
CSCvf95141	ZBF crashes on standby.
CSCvg06722	CRETE/RSP3: IPSec tunnels goes down after lifetime expiry even with ReKey enbaled.
CSCvg29183	Cisco 4000 Series ISR: XE 16.3.4 - SIP-TDM GW - FLEXDSPRM-3-TDM_CONNECT errors and crash.

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 Fuji 16.x software documentation set consists of Cisco IOS XE Fuji 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 Fuji 16.x release train. These Cisco IOS command references support all Cisco platforms that are running any Cisco IOS XE Fuji 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.