Release Notes for Cisco 4000 Series ISRs, Cisco IOS XE Fuji 16.9.x

First Published: 2018-07-19

Last Modified: 2018-07-19

Cisco 4000 Series Integrated Services Routers Overview

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-X 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: 4 GB DDR3 up to 32 GB
- Hard Drive: 200 GB or higher (Optional). The hard drive is only required for running services such as Cisco ISR-WAAS.
- Flash Storage: 4 GB to 32 GB
- NIMs and SM-Xs: Modules (Optional)
- NIM SSD (Optional)

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

Note For more information on the Cisco WAAS IOS-XE interoperability, see the WAAS Release Notes: https://www.cisco.com/c/en/us/support/routers/wide-area-application-services-waas-software/products-release-notes-list.html.

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 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 4351 ISR	16.7(5r)	14101324

Cisco 4000 Series ISRs	Existing RoMmon	Cisco Field-Programmable Devices
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 https://cfnng.cisco.com/. 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 4000 Series ISR. 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 1000 reached for Crypto functionality with
securityk9 technology package license.
```

- The throughput encrypted traffic supports 250 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.

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 and Changed Information

New Hardware Features in Cisco IOS XE Fuji 16.9.2

The following hardware is introduces in Cisco IOS XE Fuji 16.9.2:

- Cisco 4461 ISR—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/routers/access/4400/hardware/installation/guide4400-4300/C4400_isr.html.

New Software Features in Cisco 4000 Series ISR Release Cisco IOS XE Fuji 16.9.2

There are no new features introduced for Cisco IOS XE Fuji Release 16.9.2.

New Hardware Features in Cisco IOS XE Fuji 16.9.1

No new hardware features were introduced for Cisco 4000 Series ISRs in Cisco IOS XE Fuji 16.9.1.

New Software Features in Cisco 4000 Series ISR Release Cisco IOS XE Fuji 16.9.1

The following features are supported by the Cisco 4000 Series Integrated Services Routers for Cisco IOS XE Fuji 16.9.1:

- For information on migrating from existing Cisco IOS XE 3S releases to the Cisco IOS XE Fuji 16.9.1 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.
- Address Range command for Object Group—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_zbf/configuration/xe-16-9/sec-data-zbf-xe-16-9-book/sec-zbf-ogacl.html.
- Aanalysis-module Monitoring for NAM/ vNAM—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book.html.
- Application Awareness Capability to ZBFW—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_zbf/configuration/xe-16-9/sec-data-zbf-xe-16-9-book/app-firewall-app-fw.html.
- BNG: Dumping Event-traces—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/isg/configuration/xe-16-9/isg-xe-16-9-book/isg-debug-enh.html#GUID-F2F71557-7CA9-405A-B30A-25C660603DB6.
- Candidate Config Support—For detailed information, see the following Cisco document: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/169/b_169_programmability_cg/configuring_yang_datamodel.html.
- Cellular Profile Configuration Support on Cisco 4000 Series ISRs—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/routers/access/interfaces/NIM/software/configuration/guide/4GLTENIM_SW.html#35936.
- CME - Support for Cisco IP Conference Phones 7832 and 8832—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucme/admin/configuration/manual/cmeadm/cmesoft.html.
- Show Command Improvement: show tech pki —For detailed information, see the following Cisco document:https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/en/us/td/docs/ios-xml/ios/security/s1/sec-s1-cr-book/sec-cr-t1.html.xml.
- DHCPv4 Client Pptions—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dhcp/configuration/xe-16-9/dhcp-xe-16-9-book.html.

- DMVPN Transit Vnet Supported on Azure—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/routers/csr1000/software/azu/b_csr1000config-azure.html.
- Event Trace for PFRv3 Errors and PFRv3 Channels—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/pfrv3/configuration/xe-16-9/pfrv3-xe-16-9-book/pfrv3-event-trace.html
- FlexVPN Enhancements—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/xe-16-9/sec-flex-vpn-xe-16-9-book/sec-cfg-ikev2-flex.html.
- Guest Shell (On-Box Python)—The Guest Shell feature is supported on all Cisco 4000 Series Integrated Services Router platforms including the 4GB RAM SKUs.
- PHY Firmware Update—For detailed information, see the following Cisco document: https://www.cisco.com/c/en/us/td/docs/routers/access/interfaces/NIM/software/configuration/guide/vdsl2-and-adsl2-nim.html.
- IKEv2 Event Trace Enhancements—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/xe-16-9/sec-flex-vpn-xe-16-9-book/sec-cfg-ikev2-flex.html.
- IS-IS: Enhancements—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/ios/iproute_isis/command/reference/irs_book/irs_is2.html .
- IS-IS: Event Trace Improvements—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/ios/iproute_isis/command/reference/irs_book/irs_is2.html.
- IS-IS: Provide Per-Interface Statistics for CLNS/ISIS Traffic—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/ios/iproute_isis/command/reference/irs_book/irs_is2.html.
- IPSec VPN with DDNS—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnav/configuration/xe-16-9/sec-vpn-availability-xe-16-9-book/sec-realtime-ipsec.html.
- IPv6 TACACS on VRF—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/d1/sec-d1-cr-book.html.
- L2VPN Pseudowire Redundancies—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_l2_vpns/configuration/xe-16-9/mp-l2-vpns-xe-16-9-book/l2vpn-pseudowire-redundancy.html#GUID-90EA972B-1145-49F1-AE67-C2BF6B4C18AC.
- Monitor Event-trace Crypto PKI Event Command Enhancements—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/ion-en_US/ios-xml/ios/security/m1/sec-m1-cr-book.html
- PMIPv6 Enhancements for Cisco ISRs—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mob_pmipv6/configuration/xe-16-9/mob-pmipv6-xe-16-9-book/imo-pmipv6-multipath-support.html.
- PKI- Secure Device Provisioning—For detailed information, see the following Cisco document:https://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_pki/configuration/xe-16-9-1/sec-setup-sdp-piki.html#GUID-2F404010-76F1-42F5-AB84-7BA406475565

- ROMMON Protection On Cisco 4000 Series ISRs—For detailed information, see the following Cisco document:https://www.cisco.com/c/en/us/td/docs/routers/access/4400/software/configuration/xe-16-9/isr4400swcfg-xe-16-9-book/installing_the_software.html#concept_3F15D3B0CBA64CA9BADC3C84FE0C63FB
- Support for Secure SCCP Endpoints and VG on Cisco Unified Survivable Remote Site Telephony—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.
- UC Voice Module Support on Cisco 4461 ISR—For detailed information, see the following Cisco document:https://www.cisco.com/c/en_in/products/collateral/routers/4000-series-integrated-services-routers-isr/datasheet-c78-732542.html
- VXLAN support on IOS-XE—For detailed information, see the following Cisco document: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cether/configuration/xe-16-9/ce-xe-16-9-book/ce-vxlan-support.html
- vEdge on Cisco 4000 Series ISRs—For detailed information, see the following Cisco document:https://sdwan-docs.cisco.com/Product_Documentation/Getting_Started/Hardware_and_Software_Installation/Software_Installation_and_Upgrade_for_IOS_XE_Routers.
- Wide Area SDG Support on Cisco 4000 Series ISRs—For detailed information, see the following Cisco document:
- Web Root URL Filtering Enhancements—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-16-9/sec-data-utd-xe-16-9-book/web-filter.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 Fuji 16.9.1:
  - Day Zero Configuration
  - Open Shortest Path First (OSPF)
  - For information on how to access the Web User Interface, see Configure the Router for Web User Interface section.
- Candidate Configuration—A temporary configuration that can be modified without changing running configuration. You can then choose when to update the device's configuration with the candidate configuration, by committing and confirming the candidate configuration.
- 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/1691 . 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.

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

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 bug that you have requested cannot be displayed, this may be due to one or more of the following reasons: the bug ID does not exist, the bug does not have a customer-visible description yet, or the bug has been marked Cisco Confidential.

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

Open Caveats-Cisco IOS XE Fuji 16.9.8

There are no open caveats in this release.

Resolved Caveats-Cisco IOS XE Fuji 16.9.8

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

Caveat ID Number	Description
CSCvt53563	Cisco IOS XE Software NETCONF and RESTCONF Authentication Bypass Vulnerability.
CSCvw25564	Cisco IOS and IOS XE Software IKEv2 AutoReconnect Feature Denial of Service Vulnerability.
CSCvx41294	High CPU usage caused by \"TCP Timer\" process.
CSCvv12527	Crash in SNMP Engine process while polling chassis ID in LLDP.
CSCvv78028	Cisco IOS XE Software Zone-Based Policy Firewall ICMP and UDP Inspection Vulnerability.
CSCvx16081	Cisco IOS XE Software H.323 Application Level Gateway Bypass Vulnerability.
CSCvx37176	Cisco IOS XE Software Rate Limiting Network Address Translation Denial of Service Vulnerability.

Open Caveats-Cisco IOS XE Fuji 16.9.7

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

Caveat ID Number	Description
CSCvm05934	RSA Keysize > 2048 may cause crash
CSCvt66541	DNAC Wolverine - Crypto PKI-CRL-IO_1 process crashed in crypto_send_pki_request,crypto_crl_io_proc
CSCvu57706	CUBE fails to send calls with below error after updating IOS to 16.9.5 Error (Resource busy)
CSCvv17488	Cisco 4000 Series ISR + SM-X-ES3-* module-Memory leak in iomd
CSCvv36247	Memory Leak in MallocLite / Crypto IKMP
CSCvw51738	Cisco 4000 Series ISR - NIM-ES2 module soft-reload leads to a memory leak in iomd
CSCvw74609	Cisco 4000 Series ISR LACP Configuration lost: channel-group X "mode active" gets removed on reload
CSCvw96723	CP process crashed while I95 driver was adding an IPC response to the receive ring
CSCvx23482	Cisco 4321 ISR reloading once NIM-1MFT-T1/E1 module is installed.

-

Resolved Caveats-Cisco IOS XE Fuji 16.9.7

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

Caveat ID Number	Description
CSCuv97577	Mishandling of dsmpSession pointer causes a crash
CSCvr50406	Cisco IOS XE IOx GuestShell USB SSD Namespace Protection Privilege Escalation Vulnerabiliy
CSCvr93458	Hub router crashed when run test_mpol_policy_qos_policy_template testcase
CSCvt70639	Device reload due to tunnel flapping
CSCvt74346	Router may unexpectedly be reloaded when collecting data from the interface using telemetry/Netconf.
CSCvu19733	Evaluation of CVE-2020-11868 for IOS
CSCvv02486	Random MPLS-TE tunnels with explicit-path stay down after egress interface is bounced.
CSCvv26538	Crash due to a NULL pointer while bringing down PPPoE sessions.
CSCvv51048	Memory leak "AAA SESS ATTR"
CSCvv58056	ACLs may be partially loaded into hardware resulting in unexpected drop or permit
CSCvv88621	GETVPN: All GM will crash when Primary KS recovers its COOP role after network outage
CSCvw06719	"platform ipsec reassemble transit" tail-drops unencrypted IPv4 Fragments with specific payload
CSCvw11902	Passive FTP doesn't work with NAT
CSCvw14836	ISR router running 16.9.6 crashes authenticating crypto certificate
CSCvw34157	APPNAV CFT Crashes
CSCvw48800	unable to transfer 1500 byte IP packet when using BRI bundled Multilink
CSCvw56517	LMR Unable to hear first seconds of audio
CSCvw57860	Duplicate entries seen in MAC filter table.
CSCvw74609	Cisco 4000 Series ISR LACP Configuration lost: channel-group X "mode active" gets removed on reload

Open Caveats-Cisco IOS XE Fuji 16.9.6

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

Caveat ID Number	Description
CSCvu16200	Router may crash when a SSH session is closed after a TACACS configuration change.
CSCvu35559	Memory corruption crash when device is booting up.

Caveat ID Number	Description
CSCvu57706	CUBE fails to send calls with below error after updating IOS to 16.9.5 Error (Resource busy).
CSCvv17488	Cisco 4000 Series ISR with SM-X-ES3 Module- Memory leak in iomd.
CSCvv21125	Interface qlimit size decreases causing output / tail drops.
CSCvv26538	Crash due to a NULL pointer while bringing down PPPoE sessions.

Resolved Caveats-Cisco IOS XE Fuji 16.9.6

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

Caveat ID Number	Description
CSCvh24730	PfRv3: Crash while printing the same TCA message.
CSCvi22263	Crashes when IOS is adapting shaping with adaptive QoS over DMVPN configured.
CSCvi67613	Protocol type for GRE header does not work consistently with "cts sgt inline" enable over auto-tunnel.
CSCvm40582	Crashes when entering username with aaa common-criteria policy password.
CSCvm82184	Memory leak under Key Manager (keyman) process.
CSCvn02456	Router crashes when the calls does not establish after making 2 calls when we set "max-conn 2".
CSCvn33902	CPU spike is seen due to "VTEMPLATE BKG OW Process" when disconnecting PPP users 100 session/sec rate.
CSCvp46937	Sync failure and hung calls observed on standby.
CSCvp88044	Performance monitor crashes.
CSCvq39840	CiscoFlashFile - Get-Next request takes longer time for last file on directory.
CSCvq43004	Need to check qfp ucode crash with RTCP traffic - chunk memory corruption in RTCP path.
CSCvr10592	After putting caller on hold - caller call leg tx packets are increasing in CUBE.
CSCvr28935	IOS crash in DHCPd receives unnumbered interfaces.
CSCvr66463	With CRL fetch failed, stuck at failed to send the request. There is another request in progress.
CSCvr75640	LNS crash with Segmentation fault(11) in L2TP mgmt daemon.
CSCvr76593	Memory leak in CC-API_VCM and CCSIP_SPI_CONTROL.
CSCvr87906	Cisco 4461 ISR: Large un-fragmented IPSEC packets cause router to crash.

Caveat ID Number	Description
CSCvr89957	CFT crashed frequently.
CSCvs28073	IOS-XE device has memory leak in linux_iosd-imag.
CSCvs75958	Cisco 4331 ISR /K9 dialer cannot make calls suddenly.
CSCvs86573	Connect message is never forwarded to the calling side.
CSCvs88686	Cisco 4000 Series ISR crash in cpp_cp_svr due to watchdog timeout.
CSCvt05460	IOS-XE: NAT not work for Active FTP.
CSCvt33018	MACsec 128/256 XPN on 40g/100g, stop passing traffic for one of AN and interface link flap seen.
CSCvt42659	Possible regression Cisco 4000 Series ISR Management port ACL breakage or simply Day One Implementation as designed.
CSCvt48480	Flow monitor is removed from interface configuration on reload.
CSCvt54305	Device crashed after Boost license expire.
CSCvu04426	Cisco 4000 Series reloads with erroneous reload cause code.
CSCvu11115	IOS-XE MTP fails to interwork DTMF RFC2833 from payload 100 to payload 101.
CSCvu34009	Calls going through T1 are rejected with "no dsps found" Analog/TDM hairpin calls.
CSCvn31903	Cisco 4000 Series CUBE send first register with wrong ip address after reload - SIP-UA.
CSCvs00961	Memory leak under CCSIP_UDP_SOCKET / MallocLite.
CSCvs04194	Process = Exec crash seen on dmap longevity testbed with clear cry sa peer several times.
CSCvs08368	FlexVPN Hub Memory Leak in AAA process when IKEv2 sessions are being established
CSCvs12349	NeMo tunnel is down after cellular interface config is overwritten.
CSCvs29412	x509 SSH authentication incorrect UPN value selected.
CSCvs42075	Crash with shared-line command.
CSCvs46847	RTP/SRTP interworking fails when 180 and 183 have different to-tag.
CSCvs55066	Cisco 4000 Series ISR: MGCP status remains down and does not register with CUCM after a reboot or power cycle.
CSCvs70206	CUBE DNS cache clear should be limited only to the matched connection id.
CSCvs85642	Cisco 4000 Series router crashes when rtp-nte DTMF packet arrives at MTP + BDI.
CSCvs92848	Crash due to DHCP relay.

Caveat ID Number	Description
CSCvt02534	Cisco 4000 Series ISR- unexpectedly reboots with CENT-BR-0.
CSCvt04814	CPP crashes due to a long QoS policy and class name.
CSCvt08178	CUBE crashes when SIP call is forked with active SIP KPML subscription.
CSCvt10151	Multiple Cisco products Snort HTTP Detection Engine File Policy Bypass vulnerability UTD.
CSCvt21373	Unexpected reload in CPP ucode forced by nat 514 .
CSCvt33226	Cisco 4000 Series ISRS iwth CUBEs - call monitor crashed with Process = AFW_application_process.
CSCvt49705	Device Crash observed with NAT and once there is traffic from outside
CSCvt51433	Process sessmgrd crash due to clear radius sg-stats command.
CSCvt52825	Memory leak in SCCP TLS Client on unexpected deregister event.
CSCvt61876	IOS-XE FW feature crashes while inspecting TCP packet with incorrect session packet state.
CSCvt65588	FlexVPN IKEv2 Tunnel route removed after establishing new IKEv2 SA to another peer.
CSCvt73592	Missing/corrupt IOS-XE PKSC10 format.
CSCvt85954	IWAN routers Cisco 4000 Series ISR unexpected reload multiple times.
CSCvt89337	Incorrect Source IP when resolving DNS.
CSCvt91720	Router see http wsma request as coming from 192.168.1.5.
CSCvt99552	CUBE/LGW: Certificate Unknown Error is observed when cn-san-validate server is configured
CSCvu01690	CPUHOGS produced while executing the command - client fireall access-list.
CSCvu04665	CUBE keeps sending REINVITES to peer legs leading to high CPU and eventually crashes.
CSCvu11993	ZBFW drops selfzone generated packets from CPU to host with invalid reason in IOS XE 16.12.x routers.
CSCvu14823	Crash on IOS-XE router when authenticating expired IPSec peer certificate.
CSCvu20470	Memory leak in STUN/MallocLite on ISR G2 CUBE/SIP GW routers leading to memory exhaustion over time.
CSCvu27953	Crash due to a segmentation fault in the "IPsec background proc" process.
CSCvu40093	Crash when tearing down a PPPoE client session.

Caveat ID Number	Description
CSCvu43248	%IP-4-DUPADDR: Duplicate address issue at NAT-HSRP Cisco 4000 Series router.
CSCvu50302	Survivability.tcl recovery procedure fails on Ingress GW of CCE call flow.
CSCvu52218	Router crashes frequently on NBAR.
CSCvu87786	CUBE Segmentation Fault at sipSPIFreeOneSCB due to corrupt ccb.
CSCvu92620	Secure key agent memory leak in seen only in IOS XE 16.9 release.
CSCvv14026	Unexpected reload after running the **show voice dsp** command while an ISDN Call Disconnects.

Open Caveats-Cisco IOS XE Fuji 16.9.5

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

Caveat ID Number	Description
CSCvp45666	Kernel crash in netfilter.
CSCvq39840	CiscoFlashFile - Get-Next request takes longer time for last file on directory.
CSCvq84990	Remove show ip/ipv6 access-list from syncfd-<ewlc-SIT>17.1-Observed Traceback followed by IOSD crash.
CSCvq93850	Passive FTP will fail when going over NAT and either client or server are off a SM-X-ES3.
CSCvr28935	IOS crash in DHCPd Receive with Unnumbered interfaces.
CSCvr76593	Memory leak in CC-API_VCM and CCSIP_SPI_CONTROL.
CSCvs00961	Memory leak under CCSIP_UDP_SOCKET / MallocLite.
CSCvs04194	Process = Exec crash seen on dmap longevity testbed with clear cry sa peer several times.
CSCvs10497	cpp_cp_svr fast memory leak when nbar custom protocol is configured.

Resolved Caveats-Cisco IOS XE Fuji 16.9.5

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

Caveat ID Number	Description
CSCvj29514	CME: Toll fraud app not automatically trusting traffic from phones.
CSCvp73666	DNA - LAN Automation does not configure link between Peer Device and PnP Agent due CDP limitation.
CSCvq41777	CUBE ha crash of standby unit after call hold from video endpoint.

Caveat ID Number	Description
CSCvq65366	Cube might crash when sending a SIP message over TLS.
CSCvq80928	CME/BE4K SNR: Crash when config changes are made while SNR call is active.
CSCvr31188	GETVPN gikev2 Secondary KS does not push new policy after merging split condition.
CSCvr33415	Router may crash unexpectedly with Segmentation fault(11), Process = DSMP.
CSCvr39932	IPSEC install failed IPSEC_PAL_SA shows "unexpected number of parents".
CSCvr42310	Removing and adding ACL to ASR1K is causing Tracebacks and download to DP failed errors.
CSCvr48349	ESP ucode crashed when running NAT with bpa (CGN).
CSCvr51860	Observed Traceback with SRTP-RTP call after hold/resume.
CSCvr57565	MGCP Calls with SRTP fail to connect with Cause Value=47 due to T.38 calls.
CSCvr58230	While signalling forking the CUBE is not Sending Re-INVITE for T.38 with the Authorized header.
CSCvr61217	GetVPN-ISR4461// Getvpn traffic is failing with Transport mode with all the versions.
CSCvr66754	CME-ISR4K: BLF working Inconsistently on 16.09.03 [Bad code fix was done in CSCvk49797]
CSCvr76534	Cisco 4000 Seris ISR: Crash seen at process execution.
CSCvr90926	CUBE is updating the resolved IP only after the REGISTER expires.
CSCvr96597	IOS-XE crash after doing a SCEP enrollment.
CSCvr99034	Cisco 4000 Series ISR router crash during updating the OpenDNS bypass whitelist.
CSCvs13960	IWAN High CPU and memory.
CSCvs29535	IWAN crash related to DCA channel.
CSCvs47682	Router crashed on removing trustpoint on dspfarm profile.

Open Caveats - Cisco IOS XE Fuji 16.9.4

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

Caveat ID Number	Description
CSCvh59431	Byte counters for physical interface and subinterface don't match.
CSCvj00317	Memory leak VOIP *MallocLite*
CSCvk39056	Memleak_detect script errors "can't use floating-point value as operand of -"

Caveat ID Number	Description
CSCvn02456	Router crashes when the calls doesn't establish after making 2 calls when we set "max-conn 2".
CSCvn46955	Memory leak found in CUBE after the test suite execution.
CSCvn76837	DMVPN Phase 2 shortcut triggered from a spoke behind PAT may end up in stuck DNX state.
CSCvn79227	QSIG - SIP - Connected Number Missing leading digit when decoding raw QSIG.
CSCvn82063	Input CRC counter increasing on Tengi interface.
CSCvo76620	Call drops on CUBE when Hold/Resume switches codec and with midcall-signaling passthru media-change.
CSCvp27158	CUE AA leg not cleared on ios after it does blind xfer to sip line.
CSCvp31671	Router crashes due to a call loop.
CSCvp45666	Kernel crash in netfilter.
CSCvp47723	Cisco 4000 Series ISRs: CME no way audio on calls across E1/PRI, reboot resolves for sometime.
CSCvp65151	CPP Stuck thread when processing IPv6 traffic.
CSCvp69393	Router crashes after snmpget to OID related to NHRP.
CSCvq08226	Cisco 4000 Series ISRs crashes when inserting LTE card.
CSCvq14832	CUBE Fails To Take the Accept Header Into Account When Receiving Option Pings.
CSCvq25297	BRI leased line can't come up automatically after remove/insert one side's cable.
CSCvq26821	Shaper of the internal crypto interface is incorrectly programmed.
CSCvq29575	Voice gateway crash due to segmentation fault in process CCSIP_DNS.
CSCvq30306	IOSXE: IOMD / TDL leak seen with tdl_response_xcode_stat_side_t
CSCvq31129	AppNav: Optimization failed with Asymmetrical traffic, VRF, FNF and NBAR.
CSCvq31871	Router crashes with ZBF HA sync.
CSCvq39787	Support status of Restapi container for CSR has not been documented.
CSCvq43004	Need to check qfp ucode crash with RTCP traffic - chunk memory corruption in RTCP path.
CSCvq49000	Supervisor reloaded due to cpp_cp_svr process crashing.
CSCvq50202	Class-attributes duplicated after EAP reauthen. in ISG radius proxy scenario.
CSCvq57205	Recording failures with XMF media forking and SIP preservation timer.

Caveat ID Number	Description
CSCvq57862	Cable-detect command not reflecting proper status in Analog ports on IOS-XE platforms.
CSCvq57996	RADIUS attribute 4 (NAS-IP-Address) is not honored.
CSCvq58144	cpp_cp_svr crash in cpp_bqs_rm_yoda_select_sch_exponent
CSCvq58237	Supervisor reload due to cpp_cp_svr crash.
CSCvq58520	After reload dial-peers with ports that have the 'signal did' command show operational state none.
CSCvq63570	CME SIP: Add custom SK templates support back to 7832/8832 conf phones.
CSCvq65366	Cube might crash when sending a SIP message over TLS.
CSCvq67003	CPP microcode core file generated due to HW interrupt.
CSCvq71864	Crash after executing **show archive config differences**.
CSCvq72298	Router crashed on running show policy-map interface <> output command.
CSCvq73575	TCP traceroute - response ICMP TTL exceeded packet dropped by ZBFW with NAT enabled.
CSCvq74418	Connectivity is broken on ingress-replication L2DP/VXLAN.
CSCvq75610	IWAN router crash after upgrading to 16.3.8.
CSCvq78529	Seg Fault 11 crash at cts_ip_sgt_binding_sync on CTS enabled SDA fabric-edge switch stack.
CSCvq81620	Router crashes with ZBF HA sync.
CSCvq85329	NEAT/CISP:authenticate SVI interface for Supplicant switch in NEAT port when spanning-tree disabled.
CSCvq85913	FlexVPN with password encryption -- after MasterKey change password in profile is not working.
CSCvq87063	getvpn suiteb:KS sends delete payload to gm's while scheduled rekey after primary KS dead/readded.
CSCvq90343	Secure SIP trunk between SIP-GW/CUBE and CUCM with multiple nodes not coming in to service.
CSCvq90361	NHRP process crash
CSCvq91789	When issuing ip helper-addresss x.x.x.x command, **show run** and **show run all** show differently.
CSCvq92102	VG450: SCCP crashing router while shutdown the process.
CSCvq93197	Hostname is not accepted as a part of "snmp-server host" command.

Caveat ID Number	Description
CSCvq93830	IOS XE: RSA Keys randomly getting wiped out after rebooting.
CSCvq94679	[SDA] Crash due to Segmentation fault(11), Process = ARP Input.
CSCvq95517	Segmentation Fault in IP RIB Update following Virtual-Access Interface flap.
CSCvq95756	IPSec SA creation failure causes crash in fman-fp-image.
CSCvq97906	"DHCPD Receive" process crash.
CSCvq98095	Gi0/0/0 interface stays up/up and LED green after cable removed.

Resolved Caveats - Cisco IOS XE Fuji 16.9.4

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

Caveat ID Number	Description
CSCuy75886	Lots of chunk memory leak about SNMP SMALL CHUN and SNMP MEDIUM CHU.
CSCva76745	Show running-config | format with DHCP pool results in a reload.
CSCvc78492	DMVPN : IOS-XE - Unable to pass traffic if spoke to spoke fails to build in phase 2.
CSCvg40933	MoH not heard when conf initiator drops from conference [specifically when Holdee xfers the call].
CSCvg83770	Traceback seen on COOP KS.
CSCvh11088	Crash on OPF_CSR32_OPF_LOGIC_ERR_LEAF_INT__INT_START_OF_BURST_MARKER_ERR
CSCvh66339	Linux shell prompt format changed with cEdge image.
CSCvh79264	Change the punt cause of packets whose destination is virtual IP from SUBNET_BCAST to FOR_US.
CSCvi60411	SNR call flows hardening with Media Renegotiate Flow.
CSCvi86071	Crash seen after configuring SCP path under archive.
CSCvj17326	Cisco 4000 Series ISRs crashes in o2_cavm_pci_unlock when forwarding large packets for VPLS.
CSCvj76866	Partial Power Failure in Stack Causes Interfaces to Become **shutdown**
CSCvj78876	CUBE: FPI Hung Sessions and Provisioning Failures observed in Standby CUBE.
CSCvj82585	CCSIP_REGISTER memory leak@__be_voice_reg_bulkreg_initialize
CSCvj84601	Called-Station-Id attribute not included in Radius Access-Request.
CSCvj90089	Crash while doing a conference call.

Caveat ID Number	Description
CSCvk03388	After enabling fac standard, cancel call waiting *1 scenario is not working properly.
CSCvk32783	Standard IPSec support in IOS-XE SDWAN software.
CSCvk42239	Service code when dialed in from sip phone does not toggle ephone 1 status.
CSCvk58112	Router crash after binding virtual template to IWAN domain.
CSCvk74443	Multicast IPv6 ping within VRF return % No valid source address for destination.
CSCvk75838	Netconf/yang or telemetry retrieval of /trustsec-state/cts-rolebased-policies breaks.
CSCvm06775	ATOM CW is not exchanged after node reload.
CSCvm07861	Process = VTEMPLATE Background Mgr crashed in flexvpn session.
CSCvm11235	SRTP to RTP call through IOS-XE CUBE produces static with jitter present.
CSCvm17348	Callq periodic notification timer needs update after CSCve91511 commit [No functionality impact]
CSCvm19435	Crypto not updated post standby IP address change.
CSCvm22142	Critical Authentication affected if Voice VLAN not configured.
CSCvm24689	One-way audio to IP phone if phone does hold/resume after 20 minutes on secure SIP GW.
CSCvm39485	Small clock changes or time drifts can cause GETVPN TBAR drops (GDOI/IPSEC-PI).
CSCvm47675	Stale entry in shared line database on executing no voice register dn.
CSCvm47690	Addition/Edits to numbered OG ACL using "access-list <>" command does not re-expand the ACL.
CSCvm47984	Cisoc 4331 ISR: XE 16.9.1: snmpwalk error - OID not increasing.
CSCvm56135	IOS-XE block CLI "tunnel protection ipsec profile <name> shared" on Virtual-template type tunnell.
CSCvm58777	CUBE Gets Stuck In 491 Request Pending When Using TLS.
CSCvm77162	FED logs overrun 20,000 times with same trace.
CSCvm80443	IOSd memory leak within DSMIB Server within xqos_malloc_wrapper
CSCvm91642	MACsec SAP 128 Bits doesn't work with network-essentials license.
CSCvn00104	Software crash due to memory corruption after packet trace was enabled.
CSCvn03502	SR: CFLOW input intf index is 0xffffffff for Service-engine DSP module interface.
CSCvn03895	Using MTR in redundant RP systems will reload the standby due to parser return error.

Caveat ID Number	Description
CSCvn08136	Removing FNF config using the command "no vlan config 1-4094" causes watchdog forced crash.
CSCvn15600	RTP-NTE packets in sip-kpml <-> rtp-nte scenario have timestamp 0 on CUBE.
CSCvn17530	Router Crashes When PKI-CRL-IO_0 Runs out of Stack Space During Failed DNS Lookup for CA Server.
CSCvn23906	DHCP Server sends Renew ACKs to Clients with 00:00:00:00:00:00 MAC in L2 frame.
CSCvn33127	ISAKMP SA is not deleted even if crypto config is deleted (IPsec NAT-T).
CSCvn33844	RATE_11M supported cannot be preserved in config after reboot(no lower datarates set as mand.)
CSCvn45732	Device crashing if we unconfigure the NTP on the device.
CSCvn47985	ACL remarks not handled correctly by Cisco-IOS-XE-acl YANG model.
CSCvn51557	Negating dialer watch-list command without alterning the entered CLI command.
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.
CSCvn69629	ND packets received in remote vtep SISF table - EVPN part.
CSCvn71373	IOS-XE routers cannot boot due to a bootflash problem.
CSCvn76236	Add support for AAA CC <cleartext> secrets.
CSCvn77594	SRTP decryption failure leading to one-way audio issues for hairpin calls on CUBE.
CSCvn78203	Router crashed when printing logs while constructing rekey packets (GETVPN).
CSCvn85422	Int index is 0 for the Cellular inteface in the exported flow.
CSCvn86466	AAA-CC: password type-6/7 should follow the hash design and only work against expiry or be removed.
CSCvn92709	SNG_AO unavailable alarms are not clearing after removing the monitor-load feature under policy.
CSCvo00664	SUP reload after running the command " show plat hard qfp act infr bqs debug qmrt_dump "
CSCvo03167	CUBE failed to send BYE on peer leg with 'media stats-disconnect' enabled.
CSCvo03458	PKI **revocation check crl none** does not fallback if CRL not reachable.
CSCvo05000	SIP global binding disappears when the interface to which SIP is bound flaps.
CSCvo05751	Changes for sending vlan attrs in access request.

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.
CSCvo12745	Packet drop occurs after acl permit configurations.
CSCvo15215	SIP-Notify/KPML to DTMF RTP-NTE interworking fails, NTE packets dont have the marker bit set to TRUE.
CSCvo17528	Reload initiated via SNMP on IOS-XE causes a crash
CSCvo19395	Router crashes when removing a crypto map.
CSCvo20620	CUBE DNS SRV Query is not performed for PRACK
CSCvo21122	Memory leak at hman process.
CSCvo22943	Expected error message is not seen after Configuring MisMatching Bit Length - 16.9 throttle..
CSCvo27553	PKI incorrect fingerprint calulation during CA authentication
CSCvo36031	WSMA crash formatting show command output.
CSCvo36948	Router crash when running show aaa user all command.
CSCvo37464	CUBE picks incorrect interface for media after receiving c=IN IP4 0.0.0.0.
CSCvo38985	Crash at the VRF configuration.
CSCvo41815	When roaming to another AP, services received from RADIUS are not applied to the session.
CSCvo42105	IOS-XE DHCP server creates option 125 with invalid format.
CSCvo43953	Memory leak in CENT-BR-0 process.
CSCvo45257	mem leak in ios_portal_vty_run_cmd.
CSCvo46127	MaxSusRate is not working with service class.
CSCvo46138	Stuck CPP Thread while processing H323 packet.
CSCvo47436	IOSXE - firewall corrupts half open list.
CSCvo47824	Cisco 4461 ISR may fail to recognize SFP+ 10GBASE-LR on the latest polaris_dev images.
CSCvo47866	Crash at Process = SCCP Auto Config
CSCvo57387	Blind Transfer fails due to 491 Request Pending against UPDATE in early dialog

Caveat ID Number	Description
CSCvo58098	CTS PACS not downloading to the devices.
CSCvo60302	Deleting one sip-copylist will remove all sip copy-lists from dialpeers.
CSCvo62584	DHCP discover packets were being dropped at firewall since UDP source port as 0.
CSCvo67856	In.telnetd process consumes 100% CPU in show process cpu platform sorted.
CSCvo70504	Missing Calling-Station-ID in Accounting Ticket for Web-Tal locations.
CSCvo70837	Cisco 4300 ISR: show version IDMGR-3-INVALID_ID: bad id in id_to_ptr traceback.
CSCvo71381	Dot1x dynamic voice assignment failure after data domain auth such.
CSCvo71721	When sending account-logon ISG do not reply with ACK nor NACK.
CSCvo73205	Identity policy won't update after config changes.
CSCvo75523	Cisco 4000 Series ISR: Router crash with ZTP using Python script running in guest shell.
CSCvo78685	Ambiguous/unidentical ConnectionID and Fcid during CDR accounting after IOS upgrade.
CSCvo80960	Streaming CRCs seen with GLC-GE-100FX VID: V02 on ISR4k.
CSCvo87827	Crash when polling IPForwarding MIB.
CSCvo90060	Wrong label programming leading to traffic drop.
CSCvo92514	SDP attribute list corruption causes voice gateway crash.
CSCvo99156	Unexpected reload in btrace routines due to division by NULL.
CSCvp00579	Bqs may select an inaccurate rate
CSCvp08738	Router loses **transport tcp tls v1.0** on reload.
CSCvp10711	Hierarchical QoS stops working on GRE tunnel if dest route flaps between 2nd tunnel and physical int.
CSCvp16730	Incoming ESP packets with SPI value starting with 0xFF are dropped due to Invalid SPI error.
CSCvp19568	L2VPN - Xconnect - filtering of LDP targeted hellos using ACL not working.
CSCvp20770	Nas Identifier not sent in Accounting Packet.
CSCvp26876	PNP profile using hostname is not working anymore.
CSCvp27139	Async lines configuration is not retrievable over netconf
CSCvp33578	Crash at the moment of deleting a DVTI.

Caveat ID Number	Description
CSCvp34230	CUBE HA - Global bind is removed during interface flap
CSCvp35643	CDP and ping to next hop fails on Ten Gig int after device comes up post "wr er" and reload.
CSCvp39597	Crashes with GRE tunnels configured with QOS over Multilink Frame-relay interfaces.
CSCvp42709	Cisco 4000 Series ISR NO_PUNT_KEEPALIVE kernel crash due to CP drivers stuck punt and IPC rings.
CSCvp46381	Static nat which has been deleted is shown when **show ip nat** translation.
CSCvp47792	VG3x0 - groundstart voice-port configuration removed after reload.
CSCvp49863	Incomplete arp in management interface.
CSCvp50733	UTD: Process SSL callback on client hello message as opposed to server response.
CSCvp60827	Delay of 30 sec while creating a new config file for phone using tftp.
CSCvp61738	Split DNS not working in case of TCP query coming on WAN interface and destined to LAN interface.
CSCvp63616	Crash due to too many DSPs.
CSCvp66281	Default ip forward-protocol udp xx changed to no ip forward-protocol udp xx after rollback
CSCvp66443	HTTP Client inside IOS-XE incorrectly reports "Invalid IP address in Hostname" for legal IP address.
CSCvp70443	ISDN cause-location command support for switch-type primary-ntt.
CSCvp72379	**ip dns primary** command does not get removed.
CSCvp73344	Standby crash during ISSU.
CSCvp75121	Ucode crash when PfRv3 and IPv6 monitor are configured on the same tunnel with IPv6 VRF configured.
CSCvp79333	SSH may crash due to a corrupt MAC.
CSCvp83882	NIM-VAB-A stops forwaring traffic after line resync.
CSCvp87195	200 OK and UPDATE in fast succession causes issue with refresher param in update response.
CSCvp90226	"advertise ospf external" throws application error.
CSCvp91966	When Dial-Peer is Marked Down Due to Option Pings the Call Fails with Cause Value 47.
CSCvp92334	Crash after Media monitor look up.

Caveat ID Number	Description
CSCvp96418	Cisco 4000 Series ISR: BRI ping failure with WIC-1B-S/T-V3 with ISDN 128 leased line.
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
CSCvq00619	BGP flap while doing shut/no-shut on a different FPGE interface.
CSCvq01055	Replaces string not passed on CUBE REFER consumption scenario when address-hiding is configured.
CSCvq04828	VRF aware reverse DNS lookup not working.
CSCvq04989	Ping between 2 Interfaces is not working , dialer interface is interferring in the ARP Processs.
CSCvq12723	DPDK: Performing Shut/No-Shut with traffic running can cause packets to silently drop on TX.
CSCvq18105	Cisco 4321 ISR ifOperStatus for Cellular reports Up when it should be dormant.
CSCvq18328	SSH: host_key->name is not null after reload which prevents SSH from starting up
CSCvq18793	NIM-2FXS/4FXOP crashing due to DSP failed to reply properly.
CSCvq19808	Egress shaping on port-channel sub-intf tail dropping traffic long before rate.
CSCvq25176	SIP GW/CUBE does not update the change in remote SRTP key on session refresh re-invite.
CSCvq27812	Sessmgr CPU is going high due to DB cursor is not disabled after switchover.
CSCvq29953	IP SLA react for packetloss and successivepacketloss do not set $_ipsla_react_type in EEM.
CSCvq36130	Router is on Bootloop after QoS configuration.
CSCvq47186	L2 EVPN: Remote MAC not unfrozen when duplicate cleared with no MAC-only route.
CSCvq49721	Telnet access fails when VRF-aware extended VTY ACL is configured.
CSCvq50164	Back out Monolith code of CSCvp10711.
CSCvq58378	Crash after exiting RADIUS server configuration mode.
CSCvq59908	Stack crashed after upgrade.
CSCvq60252	PBR works although an interface is down.
CSCvq76537	CUBE fails to respond to second Session Refresh after refresher is forcefully reversed.
CSCvo15003	CUBE - SDP version increment behaviour creates cypto interworking issues.

Caveat ID Number	Description
CSCvq11134	SDP version was incremented due to misplace of PT 100.

Open Caveats - Cisco IOS XE Fuji 16.9.3

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

Caveat ID Number	Description
CSCvj17588	Cisco 4000 Series ISRs may reload in ""BGP Router" process when interface flap occurs with IPv6 MPLS per vrf routes
CSCvn56017	Crash while processing ISIS updates when DiffServ-TE is enabled.
CSCvn78203	Router crashed when printing logs while constructing rekey packets (GETVPN).
CSCvo09246	Cisco 4351 ISR communication down few minute after shutdown/no shutdown interface.
CSCvo18177	IPV4 routes on the global routing table learnt via BGP refreshes upon adding or removing a VRF.
CSCvo22398	Cisco 4000 Series ISRs with NIM-ES2 do not forward STP Uplink Fast dummy packet
CSCvo24170	Crash due to chunk corruption in ISIS code.
CSCvo35606	Dialer interface shutdown caused crash of router.
CSCvo36188	Crash at NAT clear.
CSCvo43897	Cisco4331 ISR , wrongly adding to Port to subscriber field after translation.
CSCvo46405	qfp ucode crashed with sRTP traffic - chunk memory corruption.
CSCvo47436	IOS-XE - firewall corrupts half open list.
CSCvo62122	IOS-XE Router may crash when attempting to Fragment Corrupted IPv4 Packet
CSCvo62584	DHCP discover packets were being dropped at firewall since UDP source port as 0.

Resolved Caveats - Cisco IOS XE Fuji 16.9.3

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

Caveat ID Number	Description
CSCvg29037	Traceback is observed during mid-call media IP and port change.
CSCvh77984	Router shows "Flash disk quota exceeded" during the reload, but it still has 60% of free memory left.
CSCvj45781	QFP CGM Memory depletion during ISG session churn.
CSCvk20560	491 not sent in a multiple re-invites in DO2EO scenario.

Caveat ID Number	Description
CSCvk62792	IKE Fragmentation payload incorrectly marked as critical.
CSCvk73696	MGCP auto-config: Port command under pots dial-peer goes missing from the configuration.
CSCvm01420	CUBE crashes at sipSPI_ipip_vcc_CheckCodecSetType.
CSCvm19399	CRL file is getting overwritten when PKI server turns up after reload.
CSCvm39894	False authorizations and authentications even without radius server for dot1x/mab.
CSCvm42441	Router crash when clearing ip nat translations.
CSCvm45068	IOS CUBE Ent does not show 'media anti-trombone' in configuration.
CSCvm51112	"clear crypto sa vrf MyVrf" triggers crash after updating pre-shared-keys.
CSCvm58960	"VoIP dial-Peer <XX> is Busied out" printed in log every 2 minutes when destination is not reachable.
CSCvm59483	Host crashes the DSP if ipv6 commands are configured under Service-Engine [Purge ipv6 config option].
CSCvm61279	Crash under AFW_application_process with shared-line configuration.
CSCvm62419	Crash at CCB of RTPSPI at the moment of creating a disconnect timer.
CSCvm65384	SNMP PKI trap are generated with wrong OID of 6999 instead of 854 per OID assignment.
CSCvm74894	PKI authentication should proceed even if GetCACaps return any http failure.
CSCvm76295	[SAP] syncfd fails to start on reload after upgrade to new ES image.
CSCvm76452	IPSec background crash while sending SNMP trap.
CSCvm76590	CUBE doesn't forward 200 OK in SRTP-RTP scenario with TCL script on Dial-peer.
CSCvm83720	Cisoc 4431 ISR GW crashed due to flex_dsprm_vtsp_close.
CSCvm86397	CUBE: Crash observed at rbuf_ooh_handler.
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.
CSCvm94112	DSM-3-INTERNAL: Internal Error : No DSM handle provided traceback on TDM voice gateway.
CSCvm94788	Device reloads when applying #client <IP> vrf Mgmt-vrf server-key 062B0C09586D590B5656390E15.
CSCvm94891	Crash caused by a "TLB Modification exception" after processing a null chunk in "IP Input" process.

Caveat ID Number	Description
CSCvm99036	CUBE Crash in CCSIP_SPI_CONTROL process.
CSCvm99045	IOS-XE PKI: Certificate with 4 dashes imported in trustpool gets lost after reboot.
CSCvn00218	CUBE Crash in sipSPIAppAddCallInfoUI.
CSCvn01507	ISR not re-calculating the hash value correctly after payload change.
CSCvn01681	IPv6 To/From headers malformed with TCL IVR Script and header-passing.
CSCvn02419	Device running IOS-XE 16 Polaris Sees Crash When Performing NAT ALG on FTP Packet.
CSCvn07614	Out of Band DTMF Events Not Passing to CUCM via SCCP When Using IOS MTP.
CSCvn14737	Crash with SIP call.
CSCvn15588	Loss of two way audio with Skinny Phone, Line instance does not work until the next reboot.
CSCvn15647	ISR4k: "mach vlan" support on Ethernet-internal interface.
CSCvn17062	ISR4K: add SCCP MTP single-VRF support with a limitation no traffic from/to other VRF
CSCvn18500	Certificate map does not work always with UPN in SAN field.
CSCvn18790	Cube crash with %SDP-3-SDP_PTR_ERROR.
CSCvn27579	Cisco 4000 Series ISRs%FMFP-3-OBJ_DWNLD_TO_DP_FAILED:fman_fp_image.
CSCvn33961	SSRC-field in RTCP gets changes to 0 when going through TRP present in the media path.
CSCvn36359	CUBE does not forward INVITE with "midcal-signalling passthru media-change" during a video escalation.
CSCvn37915	Crash in cpp_bqs_rm_yoda_proc_pend_fc_cb.
CSCvn41467	Recommit of CSCvm99778 - eca/ewlc/qwlc/mewlc Sanity : AP join failed.
CSCvn47534	RTP/SRTP interworking fails when 18x w/o SDP is before 183 w/SDP.
CSCvn51553	QFP crashes with a HW interrupt.
CSCvn53969	Memory leak in SMD process due to AAA Idle-timer not being freed.
CSCvn55148	Router not closing TCP connections when "reload" is executed.
CSCvn64296	Crash when making an external call.
CSCvn64397	Incorrect syntax in CRL download URL cause crash.
CSCvn67837	TCP port takes 4 minutes to get released after it is closed.

Caveat ID Number	Description
CSCvn71041	TACACS group server is not seen, when "transport-map type console test" is configured.
CSCvn78349	FlexVPN with password encryption - keyring aaa LIST password 6 xxxxx encrypted again upon reload.
CSCvn78961	Subscribers cannot re-login due to CoA time-out (lite-sessions in routed mode).
CSCvo00968	Radius attr 32 NAS-IDENTIFIIER not sending the FQDN.
CSCvo08337	Crash when inserting second NIM-2MFT-T1/E1 in Cisco 4331 ISR.
CSCvo15141	CLI "nat force-on" in voice service voip not working as expected.

Open Caveats - Cisco IOS XE Fuji 16.9.2

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

Caveat ID Number	Description
CSCvj12370	cpp_cp_svr crash in bqs while running QMRT test tool.
CSCvj17588	Cisco 4000 Series ISRs may reload in ""BGP Router" process when interface flap occurs with IPv6 MPLS per vrf routes.
CSCvj45781	QFP CGM memory depletion during ISG session churn.
CSCvk10212	Unable to migrate from ADSL to VDSL without a reboot.
CSCvk59169	Strict SID has NOT been enabled in ISIS segment-routing..
CSCvm59483	Host crashes the DSP if ipv6 commands are configured under Service-Engine [Purge ipv6 config option].
CSCvm61279	Crash under AFW_application_process with shared-line configuration.
CSCvm76590	CUBE does not forward 200 OK in SRTP-RTP scenario with TCL script on Dial-peer.
CSCvm78822	The config-sync failure is seen while using 'aaa authorization' commands.
CSCvm91323	Router crash with reload reason: LocalSoftADR and core file generated 'cpp-mcplo-ucode'.
CSCvm94788	Device reloads when applying #client <IP> vrf Mgmt-vrf server-key 062B0C09586D590B5656xxxx.
CSCvn01507	Cisco 4000 Series ISR is not recalcluating the hash value correctly after payload change.
CSCvn02047	More than 5k NAT entries is causing high CPU utilization even with no traffic.

Resolved Caveats - Cisco IOS XE Fuji 16.9.2

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

Caveat ID Number	Description
CSCuz14861	IOS-XE fails to correctly populate RTCP SSRC field.
CSCve31475	SNMP Error: OID not increasing: @ipAddressIfIndex.ipv6zr
CSCvi08303	Standby RP reloads due to config sync failure when Applied Service-insertion WAAS on physical Int.
CSCvi63425	Cisco 4400 ISR router cpp crashed when configured HSRP with PMIPv6.
CSCvi92528	ZBFW HA: Configuring redundancy RII on virtual template auto-tunnel does not take effect.
CSCvj16209	CME with external SIP trunk registration results into crash.
CSCvj24940	Voice VRF with No Bind OPTIONS ping response not sent.
CSCvj25678	The router crashes after failing to modify xcode.
CSCvj27172	The router crashes during Generic Call Filter Module clean-up.
CSCvj43156	Crash in XDR process: "fib_rp_table_broker_encode_buf.size <= FIB_RP_TABLE_BROKER_ENC_BUF_SZ".
CSCvj50005	Ciso 4000 Series ISR PPE ucode crashes when processing ipsec traffic on CWS tunnel.
CSCvj69654	OSPF originates default route without "default-information originate".
CSCvj73544	OSPF routing loop for external route with multiple VLINKs/ABRs.
CSCvj76285	Snmp v2 breaks due to Authentication failure, bad community string, 16.03.06.
CSCvj78647	MTU CLI is disappeared from show run when interface dialer sh/no shut.
CSCvj90426	Dash i2c kernel message outputted during boot up.
CSCvj90814	Crash 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 Trustpoin.
CSCvj92862	Netconf returns 255 length byte-stream chars instead of actual length for OSPFV2 Key-string.
CSCvj95351	OSPF SR uloop : After issuing "clear ip ospf process". ospf process crashed.
CSCvk00446	BGP high CPU when config 256k vxlan static route.
CSCvk02072	Hoot-n-holler multicast traffic marked with DSCP 0.
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.

Caveat ID Number	Description
CSCvk12152	Unable to remove command 'ip nat inside destination.'
CSCvk12448	ESP crashes due to fatal error.
CSCvk15062	Modification to ZBFW access-lists do not reflect in TCAM.
CSCvk27007	MGCP status remains Down after IOS upgrade caused by CSCvh70570.
CSCvk37875	High Availability system crashes with two Voice Gateways.
CSCvk44570	16.9 memory leak when create VLAN on ISRs.
CSCvk53405	Router crash - AFW_application_process.
CSCvk56331	Initial contact in IKEv1 phase 2 rekey (QM1) causes all crypto sessions to drop.
CSCvk56356	NETCONF the IP routes with DHCP are not presented in a consistent way for rpc-reply.
CSCvk60184	Random crash of data plane with SRTP-SRTP / SRTP-RTP load tests.
CSCvk65072	Crashes 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 and stale entries are present.
CSCvk69093	CUBE is not responding to SIP INFO.
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 4400 Series ISRs.
CSCvm06270	ICMP unrechables are not sent to the client on Cisco 1117 ISR platform.
CSCvm14346	Cisco ISR/CSR: Memory Corruption of mdl_tbl due to fia-history CLI.
CSCvm16619	CPP-mcplo-ucode crash while encrypting SIP packets with ALG NAT for SIP.
CSCvm17883	Standby switch crashes when adding a host name to an object-group.
CSCvm21219	Crash on Running "show vpdn tunnel summary" command.
CSCvm36190	Traceback seen when attempting to recover sw port from bpduguard err-disable state
CSCvm51739	SNMP v3 discloses password in the parser warning syslog trap.
CSCvm53491	SIP CME Crashes when Calling Shared Line.
CSCvm56592	CME/BE4K: Corrupted config file for Auto Registered IP Phones after reload.

Caveat ID Number	Description
CSCvm56670	ACL dropping packets after updating it - %CPPEXMEM-3-NOMEM.
CSCvm66103	Crash due to communication failure - IPC (Inter-Procedure Call) messages between DSP and RP.
CSCvm67419	Cisco 4400 Series ISRs MACsec drops small frames.

Open Caveats - Cisco IOS XE Fuji 16.9.1

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

Caveat ID Number	Severity	Description
CSCuz14861	2	IOS-XE Fails to correctly populate RTCP SSRC Field
CSCve31475	2	SNMP Error: OID not increasing: @ipAddressIfIndex.ipv6z
CSCvi08303	1	Standby RP Reloads due to Config Sync Failure When Applied Service-insertion WAAS on Physical Int
CSCvi63425	2	ISR4400 router cpp crashed when configured HSRP with PMIPv6
CSCvi92528	2	ZBFW HA: Configuring redundancy RII on virtual template auto-tunnel does not take effect
CSCvj16209	2	CME with external SIP trunk registration results into crash.
CSCvj24940	2	Voice VRF with No Bind OPTIONS Ping response not sent
CSCvj25678	2	Crash after failing to modify xcode
CSCvj27172	2	Crash during Generic Call Filter Module cleanup
CSCvj43156	1	Crash in XDR process: "fib_rp_table_broker_encode_buf.size <= FIB_RP_TABLE_BROKER_ENC_BUF_SZ"
CSCvj50005	2	ISR4K PPE ucode crash when processing ipsec traffic on CWS tunnel
CSCvj69654	2	OSPF originates default route without "default-information originate"
CSCvj73544	2	ospf routing loop for external route with multiple VLINKs/ABRs
CSCvj76285	2	Snmp v2 breaks due to Authentication failure, bad community string, 16.03.06
CSCvj78647	2	mtu cli is disappeared from show run when interface dialer sh/no shu
CSCvj90426	3	Dash i2c Kernel message outputted during boot up
CSCvj90814	2	Crash due to Memory corruption in ISR4k

Caveat ID Number	Severity	Description
CSCvj91448	2	PKI:-IP address parsing issue while printing the subject name if classless IP is used in Trustpoint
CSCvj92862	2	Viptela-netconf returns 255 length byte-stream chars instead of actual length for OSPFV2 Key-string
CSCvj95351	2	OSPF SR uloop : After issuing "clear ip ospf process". ospf process crashed.
CSCvk00446	2	BGP high CPU when config 256k vxlan static route
CSCvk02072	2	Hoot-n-holler multicast traffic marked with DSCP 0
CSCvk07838	2	CUBE is using wrong source IP address to send SIP error
CSCvk10633	2	bgp crash while running show command and same time bgp peer reset
CSCvk10909	1	ISRv: ONEP process crash during day0 bringup
CSCvk12152	2	Unable to remove command 'ip nat inside destination'
CSCvk12448	2	ESP crash due to fatal error
CSCvk15062	2	Modification to ZBFW access-lists do not reflect in TCAM
CSCvk27007	2	MGCP status remains Down after IOS upgrade caused by CSCvh70570
CSCvk37875	2	High Availability system with two Voice Gateways - Crash
CSCvk44570	2	16.9 Memory leak when create VLAN on ISRs
CSCvk53405	1	Router crash - AFW_application_process
CSCvk56331	2	Initial contact in IKEv1 phase 2 rekey (QM1) causes all crypto sessions to drop
CSCvk56356	2	NETCONF the IP routes with DHCP are not presented in a consistent way for rpc-reply
CSCvk60184	2	Random crash of data plane with SRTP-SRTP / SRTP-RTP load tests
CSCvk65072	2	Crash due ZBF + NAT
CSCvk65354	2	Extension Mobility Not working when used with Greek locale on SIP CME
CSCvk66880	2	CUBE incorrectly fomats SIP SDP
CSCvk69075	2	No calls shown in output "show call active voice brief" on CUBE & stale entries are present
CSCvk69093	2	CUBE is not responding to SIP INFO

Caveat ID Number	Severity	Description
CSCvm02627	2	Incorrect Contact port 5060 used instead of 5061 by CUBE in "302 Moved Temporarily" message
CSCvm03744	2	"%FMFP-3-OBJ_DWNLD_TO_DP_FAILED:fman_fp_image:xxx" appears when configured "ip port-map" on ISR44xx.
CSCvm06270	2	ICMP unrechables are not sent to the client on C1117 platform
CSCvm14346	3	ISR/CSR - Memory Corruption of mdl_tbl due to fia-history CLI
CSCvm16619	1	CPP-mcplo-ucode crash while encrypting SIP packets with ALG NAT for SIP
CSCvm17883	2	Standby switch crashes when adding a host name to an object-group
CSCvm21219	1	Crash on Running "show vpdn tunnel summary" command.
CSCvm36190	3	Traceback seen when attempting to recover sw port from bpduguard err-disable state
CSCvm51739	1	SNMP v3 discloses password in the parser warning syslog trap
CSCvm53491	2	SIP CME Crashes when Calling Shared Line
CSCvm56592	2	CME/BE4K: Corrupted config file for Auto Registered IP Phones after reload
CSCvm56670	2	ACL dropping packets after updating it - %CPPEXMEM-3-NOMEM
CSCvm66103	2	Crash due to communication failure - IPC (Inter-Procedure Call) messages between DSP and RP.
CSCvm67419	1	ISR4400 MACsec drops small frames

Resolved Caveats - Cisco IOS XE Fuji 16.9.1

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

Caveat ID Number	Description
CSCve78802	Cisco 4451 ISR: GLC-TE SFP module cannot up after OIR during traffic
CSCvf68261	Crash when printing IPSEC anti-replay error.
CSCvf73320	Cisco 4431 ISR crashes while finding NDR with max oif number per multicast grp at scale.
CSCvf76101	First drop error cause Tracebacks observed with IWAN stress.
CSCvf76535	B2B NAT HA: Stale NAT translations stuck on primary router after communication loss with standby.

Caveat ID Number	Description
CSCvf84340	IOS crash when logging rx dsp ctrl message out_of_sequence count syslog.
CSCvf85386	Incorrect counters in output of "show macsec statistics".
CSCvf86185	NIM-SSD: Inventory of disk0 and disk1 are interchanged onIOS XE 16.x.
CSCvf87437	High memory utilization in the QFP of QM RM process.
CSCvf95141	Zone-based Firewall crashes on standby.
CSCvf98231	Broadcast counters issue on Cisco 4000 Series ISRs.
CSCvg00696	Throughput configuration CLI should log the message "write mem and reload" instead of just relaod.
CSCvg01760	Traceback-CPUHog seen on the device.
CSCvg03498	The "copy run start all" makes the router stuck.
CSCvg03981	IOS-XE NAT: IP header of tunneled traffic is translated twice (in inner and outer header).
CSCvg05599	Router does not recalculate UDP checksum after NAT.
CSCvg19203	SBC re-latch does not work as expected in case of ipv4 mask/0.
CSCvg21196	Cisco 4000 Series ISRs: SW MTP configured as TRP does not relay PLI/RTCP messages.
CSCvg26073	QFP Memory leak in cpp_cp_svr with CPP List Hdr chunk.
CSCvg31373	Cisco 4000 Series ISRs : Error Msg (SYS-2-CHUNKEXPANDFAIL: Could not expand chunk pool for ASR1000 SPA TDL).
CSCvg31929	Extended the retries on UCSE before NGIO control packet loss is detected.
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.
CSCvg39934	SL mode, unthrottled configuration and relaod without saving puts the system in inconsistent state.
CSCvg40430	Cisco 4431 ISR: QFP crashes by a LLC packet received in a serial interface.
CSCvg52180	Cisco 4000 Series ISRs: ROMMON upgrade fails on certain IOS-XE 16.x releases.
CSCvg63492	Cisco 4000 Series ISRs :IOS-XE 16.x: CWS CLI present but the feature is not supported.
CSCvg65632	CPP 0 failure Stuck Thread resulting in Unexpected Reboot
CSCvg89742	Incorrect pass-through statistics seen during soak run.

Caveat ID Number	Description
CSCvg94908	Mgig stack keeps crashing while configuring with Radius commands.
CSCvi63840	VIG interface counters do not increment with multicast service reflection on IOS-XE.
CSCvj51510	Crash after service-policy APPNAV change on WAAS instance. .
CSCuy30367	ENH: IOS-XE should allow "ip address dhcp" on Tunnel interface.s
CSCvb69966	Memory leak under LLDP Protocol process.
CSCvd62086	ISR4xxx needs to generate puntinject_stats.log.xxxx and save in bootflash.
CSCvf19460	CTS Pac download fails with ISE reachability through loopback interface over vrf .
CSCvf37923	Crash due to stack overflow.
CSCvf80363	Rrotate nginx access/error log files
CSCvg16234	ISR receives a control packet (CDP) with a CMD tag it should process it, not drop it.
CSCvg51358	DHCPNAK is not sent in roaming scenario.
CSCvh02516	Cannot add static route through dynamic NEMO tunnel interface.
CSCvh16650	Netconf Get routing-state received an errored RPC response.
CSCvh20041	UDP SLA Probes not working through PMIPv6 tunnel with GETVPN.
CSCvh26828	Crash in SNMP ENGINE when polling lldpRemChassisId object.
CSCvh32416	Evaluation of all for CPU Side-Channel Information Disclosure Vulnerability.
CSCvh57050	IGMP multicast SSM-map with DNS does not work with IGMPv3.
CSCvh60525	CLI aaa common-criteria not available on IPBASEK9 license.
CSCvh60871	Unexpected Reboot following show platform software adjacency oce [ID].
CSCvh61453	NULL remote_hostname from LAC.
CSCvh62532	System reload when clearing cts pac.
CSCvh63932	Noisy debugs in "periodic" tracelog.
CSCvh68810	16.8.1:dot1x Clients stops responding (ping to clinet IP fails) after 2nd SSO.
CSCvh69518	%SYS-3-TIMERNEG:Cannot start timer with negative offset Process= "ARP Background"
CSCvh70297	Redundancy Mode None does not Sync.
CSCvh73134	ISDN memory leak.

Caveat ID Number	Description
CSCvh77637	ISDN pri-group cause router get into a loop.
CSCvh80485	CTS pacs and cts credentials are lost after SSO.
CSCvh92275	QoS Overrides loadbalancing to per prefix even with only session level policing applied
CSCvh97226	Ordering isssue for crypto keyring and crypto isakmp profile.
CSCvh99651	AAA-Proxy errors in dmiauthd tracelogs.
CSCvi07387	IP dhcp excluded-address deletion issues via netconf.
CSCvi07402	No increment for input errors in show i/f counters for pkts larger than configured MTU+30 byte.
CSCvi11665	Virtual-service guest IP accepts broadcast address.
CSCvi12341	Unable to see device-sensor in accounting message on ISE (MUD URI).
CSCvi20882	Netconf IP-SLA udp-jitter case missing leaf codec.
CSCvi22603	Flex-LSP tunnel flap on failing active protecting link without WRAP enabled.
CSCvi22835	Vz: Non-XE to XE ISSU compatibility issue.
CSCvi24614	XE 16.8.1: MKA session not coming up consistently after SSO and keepalive timeout.
CSCvi25507	Session Mgrd crah obsered with XE 16.8.1 image.
CSCvi31493	Configuration of BGP auto-summary using NETCONF fails.
CSCvi35143	Repeatedly Tracebacks seen : %INFRA-3-INVALID_GPM_ACCESS: Invalid GPM Load.
CSCvi36290	Incorrect BDI configuration state shown by NETCONF on interface creation.
CSCvi36351	Standby rp crash on removing member link from port-channel.
CSCvi36875	Restored DB is session-lock locked out with insane timeout after boot
CSCvi60900	DHCP Leasequery Padding contains previously used data.
CSCvi72769	UDP SLA echo packets not getting encrypted.
CSCvi89742	Excessive memory (20MB)) allocated for event tracing by lslib subsys.
CSCvj29095	High CPU due to Alignment Corrections - DNS and NBAR.
CSCvj55797	NETCONF does not list all the ip nat configuration.
CSCvj56303	NETCONF issue when updating NAT config with VRF keyword.
CSCvj69569	The "show authentication session sw st" broken and session monitoring sessions coming in show auth sess in legacy mode.

Caveat ID Number	Description
CSCvj79542	Missing interface source template model.
CSCvj87392	DHCP server with option 249 pushes only the routes confiugred in the first instance.
CSCvj89345	AVC license should be activated only in case of smart licensing model.

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.