Release Notes for Cisco 4000 Series ISRs, Cisco IOS XE Gibraltar 16.12.x

First Published: 2019-07-25

Last Modified: 2022-09-23

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 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.

Note For more information on the Cisco WAAS IOS-XE interoperability, refer to 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 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 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.

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.

CTI Configuration

CME does not support CTI configurations on Cisco 4000 Series ISRs.

TACACS Legacy Command

Do not configure the legacy **tacacs-server host** command; this command is deprecated. If the software version running on your device is Cisco IOS XE Gibraltar 16.12.2 or a later release, using the legacy command can cause authentication failures. Use the tacacs server command in global configuration mode.

New and Changed Information

New Software Features in Cisco 4000 Series ISRs Release Cisco IOS XE Gibraltar 16.12.2

The following features are supported by the Cisco 4000 Series Integrated Services Routers for Cisco IOS XE Gibraltar 16.12.2:

- Support for Media Flow-around using Multi-VRF: Multi-VRF is added following call flows in standalone and high availability scenarios:
  - Basic Audio Call
  - Call Hold and Resume
  - Re-INVITE based Call Transfer
  - 302 based Call Forward
  - Fax Pass Through Calls
  - T.38 Fax Calls

New Hardware Features in Cisco IOS XE Gibraltar 16.12.1a

The following features are supported by the Cisco 4000 Series Integrated Services Routers for Cisco IOS XE Gibraltar 16.12.1a:

- Installing the Cisco SM-X-16G4M2X EtherSwitch Service Module—Cisco SM-X-16G4M2X is a layer-2 switch module that bring high-density Small Form-Factor Pluggable (SFP) /Small Form-Factor Pluggable Plus (SFP+), 1 Gigabit, 2.5 mGiG, and 10G connectivity to the Cisco 4000 Series Integrated Services Routers (ISRs).

New Software Features in Cisco 4000 Series ISRs Release Cisco IOS XE Gibraltar 16.12.1a

The following features are supported by the Cisco 4000 Series Integrated Services Routers for Cisco IOS XE Gibraltar 16.12.1a:

- BGP Support for TCP-AOO—On a secure control plane, BGP uses Message Digest 5 (MD5) algorithm as the authentication mechanism. It uses the TCP API to configure the keychain on a TCP connection. When authentication is enabled, any Transmission Control Protocol (TCP) segments belonging to BGP are exchanged between peers, verified and then accepted only if authentication is successful.

- Configuring the SM-X-16G4M2X EtherSwitch Service Module—Cisco SM-X-16G4M2X service module provides a variety of 1 Gigabit, 2.5 mGiG, and 10G SFP/SFP+ ethernet connectivities. Also, provides 10G-capable internal uplink to central forwarding data plane on modular Cisco 4000 Series ISRs.

- Configuring FXS Ports for Supplementary Services—To handle supplementary services for FXS ports, FXS ports event handler handles the hookflash or onhook events.

- Support for DHCP on DMVPN Tunnels—In a Dynamic Multipoint VPN (DMVPN) network, each spoke has a unique IP address belonging to the same IP subnet. On a large DMVPN network, it is difficult to manually configure the spoke addresses. With this feature, you can dynamically configure the spoke addresses of the Generic Routing Encapsulation (GRE) tunnel interfaces using DHCP.

- IPv6 Support for Encrypted Traffic Analytics (ET-Analytics)—This feature extends support for ET-Analytics to IPv6 addresses. ET-Analytics is used to identify malware communications in encrypted traffic. ET-Analytics uses passive monitoring, extraction of relevant data elements, and supervised machine learning with cloud-based global visibility.

- Multi-SA Support for SVTI—You can define and associate an Access Control List (ACL) with an SVTI to select traffic between specific source and destination proxies. By associating the ACL, you are modifying

the default configuration that uses a single any-any traffic selector and for every non-any-any traffic selector, IPSec SAs are created.

- PFS for GETVPN—If a Group Member (GM) is compromised, an attacker may access saved long-term keys and messages. Use Perfect Forward Secrecy (PFS) for GETVPN so that the attacker cannot use the keys and messages to obtain the keys of past or future sessions to decrypt recorded or future communication.

- Support for Federal Information Processing Standards (FIPS)—FIPS are publicly announced standards developed by the United States federal government for use in computer systems by non-military government agencies and government contractors. In FIPS mode, the device tries to prevent the use of non-FIPS compatible algorithms, but you must ensure that you configure the device to use only FIPS approved algorithms. Some functionality may silently fail in FIPS mode if it attempts to use non-FIPS compliant algorithms.

- Support for IEEE 802.1Q Tunneling and Layer 2 Protocol Tunneling—IEEE 802.1Q Tunneling is designed for service providers to carry traffic of multiple customers across their networks while maintaining the VLAN and Layer 2 protocol configurations of each customer without impacting the traffic of other customers. Layer 2 protocol tunneling can be used independently or can enhance IEEE 802.1Q tunneling.

- Show Command for IP Route Sum VRG All—Address and IA_PD (Identity Association-Prefix Delegation) components of the packet, and extracts each IPv6 address contained in the packet.

- Secure Control Plane: Infra Crypto Module Integration—The key chain related commands are updated.

- Show Commands Updates for SRTP Rollover Counter (ROC)—The output of the following commands is enhanced to display SRTP ROC information:: **show voip fpi calls**, **show voip fpi stats**, and **show voip rtp connections**.

- Online Diagnostics—Online diagnostics are used to check different hardware components, interfaces, and verify the status of software processes.

- Show Tech OSPF—You can specify a vrf-instance with the show tech-support ospf command so that the following commands are executed for the specified VRF: **show ip route summar** and **show ip route ospf**.

- TCP-AO Support for SXP—CTS SXP peers exchange IP-SGT bindings over a TCP connection. TCP Authentication Option (TCP-AO) guards against spoofed TCP segments in CTS SXP sessions between a set of peers.

- 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 Gibraltar 16.12.1a:

  - Configuring Cisco Unified Communications Manager Express
  - Configuring Trustsec
  - Viewing File Manager
  - Monitoring Trustsec Statistics

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

- YANG Data Models—For the list of Cisco IOS XE YANG models available with this release, navigate to https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/16121/BIC. 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.

Note In Cisco IOS XE Release 16.12.3, the semantic version number for the YANG models is not updated and is therefore not accurate. However, this limitation does not impact the functionality of the YANG models.

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.

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

Resolved Caveats - Cisco IOS XE Gibraltar 16.12.8

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

Caveat ID Number	Description
CSCvy91615	OpenSSH vulnerability for IOS-XE platforms.
CSCwb08932	Standby switch crashed due to SISF BT mac mov.
CSCvz80171	SIP call fails egress dial-peer uses "session server-group" and "sip options-keepalive".
CSCwa27659	Virtual VRRP IP address unreachable from the BACKUP VRRP.
CSCwb26335	RSP3: Err reading data from table dmi-general: Could not get boolean val for feature.side_effect_sync.
CSCvz77313	Device reload due to SFF8472.
CSCvw60355	DHCPv6: Memory allocation of DHCPv6 relay option results in crash.
CSCwb96964	Device crashes on creating telemetry subscription.
CSCwb24680	LLDP system description not correctly seen in ISE.
CSCwa82143	%SYS-2-INTSCHED: 'may_suspend' disabled -Process= "HSRP IPv4" log generate during boot up.

Resolved Caveats - Cisco IOS XE Gibraltar 16.12.7

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

Caveat ID Number	Description
CSCvy79950	Cannot force the switch to ask for option 12 to be assigened from the DHCP server.

Caveat ID Number	Description
CSCvz24267	Static NAT entry is injecting a route to Null0.
CSCvz69851	CSR: Missing iid_certs for AWS invite-only regions.
CSCvz57415	128.0.0.0/2 is installed into CEF as unusable on a PETR after EID-Prefix is removed.
CSCwa36699	Prefetch CRL download fails.

Open Caveats - Cisco IOS XE Gibraltar 16.12.6

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

Caveat ID Number	Description
CSCvp46414	TunnelUnsupportedConfig drops seen during volume based rekey
CSCvp93108	ISR4k crash seen in SCCP due to an invalid stream idx
CSCvq84411	ISR4461 Fails to Populate Configurable Interfaces When Creating Global SIP Bind
CSCvq93257	Update new OID numbers to ciscoC83001N1S6G and ciscoC83001N1S4G2X in CISCO-PRODUCTS-MIB.my
CSCvr74819	DHCP server on ISR4k - Android devices are not getting IP addresses
CSCvr93635	flows not moving to unutilized link even after the hardthreshold
CSCvt03033	ISR4351:%BGP-3-BGP_SRTE_FAILURE: BGP SRTE failed to register with TE -Restarting BGP may be required
CSCvt89441	IOS-XE device crashed with CGD shared memory corruption freed by FMAN-FP
CSCvt99760	Crash when btrace modules exceed the initially max number of registration
CSCvy34805	Consecutive Multicast Crashes in ISR4K
CSCvy57684	ISR4k rebooted unexpectedly with reason \"LocalSoft\"
CSCvy94954	LA LED turns green when just inserted SFP-10G-LR on ISR4k without cable connecting
CSCvz14745	Memory leak seen when using DNS with IP SLA

Resolved Caveats - Cisco IOS XE Gibraltar 16.12.6

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

Caveat ID Number	Description
CSCvt35331	Console port goes unresponsive, reboot required to restore it.
CSCvv50627	VLAN registration failed when ISRV boots using igbvf interface from ENCS

Caveat ID Number	Description
CSCvv59311	Repeated \"kernel: DMA: Out of SW-IOMMU space\" logs
CSCvw14836	ISR router running 16.9.6 crashes authenticating crypto certificate
CSCvw17687	Crash with RTP extended port range
CSCvw42048	c1111 vtcp may cause packet drop for sip packets causing phones to reset
CSCvw51738	ISR4K - NIM-ES2 module soft-reload leads to a memory leak in iomd
CSCvw51810	Disruption of IP communication due to AUTH_DRIVEN_DROP on uplinks when flapping downlink ports
CSCvw57860	Duplicate entries seen in MAC filter table.
CSCvw74609	ISR4k LACP Configuration lost: channel-group X \"mode active\" gets removed on reload
CSCvw90288	ISR 4331 Fork Correlator
CSCvx01171	Smart Licensing: ISR4K Consumes Multiple Boost Performance Licenses
CSCvx19135	ISR crashes when ZBFW ALG inspects tunneled packet
CSCvx19983	Sip-server command is added to ISR4431/K9 CUBE after upgrading from 16.03.06 to 16.09.06
CSCvx33043	ISR4400 routing multicast packets out of order VASI-left in VRF RIB VASI-right in Global RIB
CSCvx38454	ISR Crash for CENT-MC-0 process
CSCvx58532	ISR4K CUBEs - crash in AFW_application_process due to \"XCC_TCL_ActiveDest_Connected\"
CSCvx83671	Router restarts unexpectedly reporting segmentation fault by AFW_application_process
CSCvx84617	ISR - Appnav service controller ucode crash during packet intercept from network
CSCvx97647	IOS-XE CUBE Unexpected Reboot during SRTP fallback
CSCvx97718	vtcp frees rx buffer when packet with expected next sequence arrives with no payload; phones reset
CSCvy04933	Power supply failure alarm appears in ISR4331 when using DC Power module
CSCvy25961	WebUI CME not Loading properly on Phones Tab
CSCvy31298	ISR4461 NIM-2GE-CU-SFP - Sub-interfaces not transmitting traffic
CSCvy31577	PDP Type error on ISR4K using Cellular 4G

Open Bugs-Cisco IOS XE Gibraltar 16.12.5

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

Caveat ID Number	Description
CSCvp93108	Cisco 4000 Series ISR crash seen in SCCP due to an invalid stream idx.
CSCvq84411	Cisco 4461 ISR Fails to Populate Configurable Interfaces When creating global SIP bind.
CSCvr74819	DHCP server on Cisco 4000 Series ISRs - Android devices are not getting IP addresses
CSCvt03033	Cisco 4351 ISR :%BGP-3-BGP_SRTE_FAILURE: BGP SRTE failed to register with TE -Restarting BGP may be required
CSCvt35331	Console port goes unresponsive, reboot required to restore it.
CSCvt97975	TenGig SPA Module went down because of site power issue.
CSCvu32446	Cisco 4451 ISR rebooted with reason_code "CPU Usage due to Memory Pressure exceeds threshold"
CSCvw51738	Cisco 4000 Series ISR - NIM-ES2 module soft-reload leads to a memory leak in iomd
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.
CSCvw80529	Cisco 4331 ISR Router experiencing modem crash.
CSCvw84042	Cisco IOS-XEdoes not correlate indices properly with cellular radio band output.
CSCvw88866	Cisco 4331 ISR - ucode crash with FNF.
CSCvw90983	Cisco 4000 Series ISR crashes with scaled QOS after applying QOS configuration to sub-interfaces.
CSCvw96723	Cisco 4000 Series ISR crash occurred.
CSCvx01171	Smart Licensing: Cisco 4000 Series ISR consumes multiple boost performance licenses.

Resolved Bugs-Cisco IOS XE Gibraltar 16.12.5

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

Caveat ID Number	Description
CSCvs81967	Cisco 4000 Series ISR: %BOOT-3-BOOT_SRC: R0/0: No space on boot /dev/bootflash5 for packages, using bootflash!.
CSCvt48480	Cisco 4000 Series ISR: Flow monitor is removed from interface configuration on reload
CSCvu04426	Cisco 4000 Series ISR reloads with erroneous reload cause code.

Caveat ID Number	Description
CSCvu59956	Cisco IOS cannot boot with 16.12(1r) or later rommon due to cookie PID field incorrectly programmed.
CSCvu66698	Cisco 4000 Series ISR suppress timer is started on the serial interfaces instead of the dialer interfaces
CSCvu82189	Enabling guestshell gives "float division by zero"
CSCvu99045	NIM-1GE-CU-SFP/NIM-2GE-CU-SFP: Show interface output reports incorrect bandwidth
CSCvv01250	IGMP reports are forwarded to mrouter port untagged regardless of which VLAN the group is in.
CSCvv17488	Cisco 4000 Series ISR with SM-X-ES3-module: Memory leak in iomd.
CSCvv17730	IP DHCP Snooping not working for the voice vlan.
CSCvv33576	IGMP snooping table not populated on Cisco 4000 Series ISR.
CSCvv37172	License lost after "no license boot level <>" CLI followed by reset button.
CSCvv43027	VDSL performance impacted if more than two vlan tags are used.
CSCvv58919	Police to PPS is not configurable on Cisco 4000 Series ISR.
CSCvw31389	pktlog functionality is broken.

Open Bugs-Cisco IOS XE Gibraltar 16.12.4

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

Caveat ID Number	Description
CSCvt35331	Console port goes unresponsive, reboot required to restore it.
CSCvt48480	Flow monitor is removed from interface configuration on reload
CSCvt89441	IOS-XE device crashed with CGD shared memory corruption freed by FMAN-FP
CSCvu65369	Link auto-negotiation fails between switch module and Meraki MX100
CSCvu62273	The tacacs-server commnad should be auto-upgraded to newer version while upgrading.

Resolved Bugs-Cisco IOS XE Gibraltar 16.12.4

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

Caveat ID Number	Description
CSCvr25074	Power event detected when connecting with theswitch module.

Caveat ID Number	Description
CSCvs35368	Cisco 4331 ISR rebooted with "CPU Usage due to Memory Pressure exceeds threshold" when running traffic.
CSCvs75958	ISR4331/K9 Dialer cannot make calls suddenly
CSCvs88686	Cisco 4300 ISR crashes in cpp_cp_svr due to watchdog timeout.
CSCvt03264	UltimaThule: ISR4451 router crashed when template is pushed from vManage
CSCvt05460	IOS-XE: NAT not work for Active FTP.
CSCvt21691	VLAN1 is allowed on the trunk port even though it is not allowed in configurations.
CSCvt52168	SSH Process Thrash During Normal Operations.
CSCvt54305	Device crashed after Boost license expire.
CSCvu43248	%IP-4-DUPADDR: Duplicate address issue at NAT-HSRP on Ci8sco 4000 Series ISRs.

Open Bugs-Cisco IOS XE Gibraltar 16.12.3

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

Caveat ID Number	Description
CSCvp46414	TunnelUnsupportedConfig drops seen during volume based rekey.
CSCvp93108	Cisco 4000 ISR crashes in skinny_unreserve_xcode_stream on XE 16.9.
CSCvr25074	Power event detected when connect with switch module.
CSCvr74819	DHCP server on Cisco 4000 Series ISRs - Android devices are not getting IP addresses
CSCvr76593	Memory leak in CC-API_VCM and CCSIP_SPI_CONTROL.
CSCvr93635	Flows not moving to unutilized link even after the hardthreshold.
CSCvs28073	IOS-XE memory leak seen in 16.3.7 in IOSd due to update_sn_ao_state not deleting TDL bucket.
CSCvs41030	Ciso 4331 ISR crashed upon reload *cpp_qos_qm_queue_update_cb*.
CSCvs46351	IPSLA UDP-jitter authentication failure with more than 16 characters key string.
CSCvs56586	While upgrading the Cisco IOS XE version from XE Release 16.9.2 to 16.9.4 , smart licensing registration was lost.
CSCvs75958	Cisco 4331 ISR/K9 Dialer cannot make calls suddenly.
CSCvs85642	Cisco 4331 ISR: IOS XE 16.9.4 QFP ucode crash due to null derefence.
CSCvs88686	Cisco 4300 ISR crash in cpp_cp_svr due to watchdog timeout.

Caveat ID Number	Description
CSCvs98578	Cisco 4221 ISR router with NIM switch module MAB/Dot1x does not start.

Resolved Bugs-Cisco IOS XE Gibraltar 16.12.3

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

Caveat ID Number	Description
CSCvq18105	Cisco 4321 ISR ifOperStatus for Cellular reports Up when it should be dormant.
CSCvq44603	Cisco 4000 Series ISR reloads Unexpectedly, Crashing in the "IP NAT Ager" Process
CSCvq93850	Passive FTP will fail when going over NAT and either client or server are off a SM-X-ES3.
CSCvq98999	Cisco 4451-X ISR / 16.09.01 - Crashes when IPSEC SA installation fails.
CSCvr13380	Cisco 4000 Series ISR: Guestshell must be supported for all license levels for ZTP.
CSCvr17670	Cisco 4000 Series ISR crashes after VoIP AAA test.
CSCvr41193	EVC cross vlan label stack communication.
CSCvr66754	CME and Cisco 4000 Series ISR: BLF working Inconsistently on 16.09.03 [Bad code fix was done in CSCvk49797]
CSCvr76534	Cisco 4000 Series ISR\ Crash seen at Process Exec
CSCvr87906	Cisco 4461 ISR: Large un-fragmented IPSEC packets cause router to crash
CSCvr89182	ISR4331 fails upgrade to 16.12.1d and rollsback with ASR1001-HX identity
CSCvr99034	ISR 4K router crash during updating the OpenDNS bypass whitelist
CSCvs02000	%IOSXE-3-PLATFORM: R0/0: kernel: DMA: Out of SW-IOMMU space.
CSCvs07447	Cisco 4000 Series ISR Mgmt Gi0 up with speed 100Mbps.

Resolved Bugs-Cisco IOS XE Gibraltar 16.12.2S

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

Caveat ID Number	Description
CSCvs35311	MAP-E: Remove embedded customer specific data from the image.

Open Bugs-Cisco IOS XE Gibraltar 16.12.2

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

Caveat ID Number	Description
CSCvp70459	IOS: Prevent crypto ACL change if already mapped with crypto map configuration.

Caveat ID Number	Description
CSCvq18105	Cisco 4321 ISR if OperStatus for Cellular reports Up when it should be dormant.
CSCvq44603	Cisco 4000 Series ISRs reloads unexpectedly, Crashing in the "IP NAT Ager" process.
CSCvq98999	Cisco 4451-X ISR/ 16.09.01 / crashes when IPSEC SA installation fails.
CSCvr15127	Cisco 4000 Series ISRs calls fade to no-way audio due to media inactivity detection after 20 minutes.
CSCvr33864	NIM-2GE-CU-SFP: Failed to boot up after upgrade.
CSCvr62697	Cedge Cisco 4000 Series ISRs not able to upgrade to 16.12.1d.
CSCvr74819	DHCP server on Cisco 4000 Series ISRs- Android devices are not getting IP addresses.

Resolved Bugs-Cisco IOS XE Gibraltar 16.12.2

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

Caveat ID Number	Description
CSCvs35311	MAP-E: Remove embedded customer specific data from the image.
CSCvp47723	Cisco 4000 Series ISRs: CME no way audio on calls across E1/PRI, reboot resolves for sometime.
CSCvp72039	Ucode crash in infra with injected jumbo packet after upgrading to Cisco IOS XE 16.9.2 release.
CSCvq19808	Egress shaping on port-channel sub-intf tail dropping traffic long before rate.
CSCvq29575	Voice gateway crash due to segmentation fault in process CCSIP_DNS.
CSCvq39121	Cisco 4000 Series ISRs crash during packet inspection due to stuck thread.
CSCvq61590	ESP reload due to cpp_cp_svr exception at cpp_bqs_exponent_cnt_validate
CSCvq71864	Crash after executing "show archive config differences".
CSCvq74831	Enable modem CO4 setting for VDSL CPE.
CSCvq75610	IWAN router crash after upgrading to Cisco IOS XE 16.3.8 release.
CSCvr00983	Unrecoverable Error with PVDM in 0/4 and Thule+dreamliner in 1/0 on Cisco 4300 ISRs.
CSCvr06666	Cisco 4000 Series ISRs CPP ucode Crash due IPv4 Fragmented packets.

Open Bugs - Cisco IOS XE Gibraltar 16.12.1a

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

Caveat ID Number	Description
CSCvg68226	Excluding cisco802TapMIB or ciscoTap2MIB should not require Lawful Intercept licence
CSCvq36179	Interfaces with 'shutdown' configuration in UP state.
CSCvo46253	BGP Oper model rpc reply error with aggregate bgp ipv6 route.
CSCvp08353	Add ERROR message over IOS console when HSPRDA TCAM region gets full
CSCvp16862	EVPN Prefix import Count/Limit show incorrectly
CSCvp30081	BGP looped update among 3 peers.
CSCvp34344	Cisco legacy PD not supported by Cisco 22-Port and 50-Port Etherswitch Service Module.
CSCvp38407	"Radius-server attribute 31" command broken on LNS when LAC sends Remote-Id string
CSCvp89419	When try to configure"logging persistent protected" the system throws the following error messages: Router(config)#logging persistent protected and %No space left on the device, free up storage and retry.
CSCvp69393	Router crashes after snmpget to OID related to NHRP.
CSCvp79485	DMVPN - Packet is encapsulated but not encrypted going out DMVPN tunnel.
CSCvp96086	Cellular Backoff counters is not correct after modem reset.
CSCvp97235	Crash while BGP was updating rib table.
CSCvq00263	Device crashed @ radius_io_stats_timer_handler due to dynamic-author.
CSCvq03972	AS-path prepend happens on iBGP neighbor with route-map continue.
CSCvq14883	Default-information originate configuration does not advertise default route.
CSCvq16878	Stale Nat Entries On Secondary Router.
CSCvq18004	BGP evpn table and vrf table out of sync.
CSCvq25297	BRI leased line cannott come up automatically after remove/insert one sides cable.
CSCvq26821	Shaper of the internal crypto interface is incorrectly programmed
CSCvq29838	Cisco 4451 SIR with E1/T1 NIM shows SPA-1-DB_AUTHENTICATION_FAIL:iomd: Module daughter board auth.
CSCvq31129	AppNav: Optimization failed with Asymmetrical traffic, VRF, FNF and NBAR.
CSCvq31871	Router crashes with ZBF HA sync.

Caveat ID Number	Description
CSCvq33073	OBS : PE ignores IGP metric while advertising the MED value to CE
CSCvq33994	BGP YANG oper address-family fails with vpnv4-unicast
CSCvq36130	Router is on Bootloop after QoS configuration.
CSCvq39121	Cisco 4000 Series ISR crashes during packet inspection due to stuck thread.
CSCvq39840	CiscoFlashFile - Get-Next request takes longer time for last file on directory.
CSCvq40443	"Clock: inserting leap second" message does not output on NTP client when leap second inserted.
CSCvq44860	Static routing redistribution under RIP with route-map is not working after reload.
CSCvq45984	ISDN 4K: isdn bchan-number-order descending has no effect.
CSCvq46526	DMVPN: Spoke to Spoke traffic fails when Tunnel initiated by Tunnel IP to tunnel IP pings.
CSCvq46617	RLFA config causing OSPF to ignore backup path addition for NSSA prefix after primary link flap.
CSCvq49172	Cisco IOS XE multicast-intact issue with SR uloop EP.
CSCvq49721	Telnet access fails when VRF-aware extended VTY ACL is configured.
CSCvq50129	Route-map not exporting prefix with 6PE BGP Neighbour.
CSCvq50202	Class-attributes duplicated after EAP reauthen. in ISG radius proxy scenario.
CSCvq53063	Tacacs direct-request does not authenticate using the correct source interface.

Resolved Bugs - Cisco IOS XE Gibraltar 16.12.1a

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

Caveat ID Number	Description
CSCvh92659	BFD flaps everytime with dynamic tunnel creation in DMVPN.
CSCvi26188	Watchdog crash within mgcpapp_free_sys_event_Q event dequeue loop after running 'ccm-manager configuration.
CSCvk71047	Router fails to reserve necessary ports for VPN traffic (UDP 500 & 4500) for ISAKMP
CSCvm25921	Signaling interface inactive on "show snmp mib ifmib ifindex de" on IOS 16.6.3
CSCvm75066	MPLSoVPN: Change behavior of default route in NHRP. Must insert 0.0.0.0/0 instead of /32
CSCvm94112	DSM-3-INTERNAL: Internal Error : No DSM handle provided traceback on TDM voice gateway

Caveat ID Number	Description
CSCvn03502	SR: CFLOW input intf index is 0xffffffff for Service-engine DSP module interface.
CSCvn12420	VXLAN static routes use wrong source for LFIB entries they create.
CSCvn46969	Cisco 4000 Series ISR: hang up when executing "sh ip nat tran" with static NAT entries.
CSCvn49351	Async line not visible in show run and show int brief output but visible in show line output.
CSCvn52019	Crashed while checking condition debug
CSCvn57165	Static Nat fails to translate SIP Trying L7 header.
CSCvn61039	Cisco 4000 Series ISR control-plane host feature was moved to APPX feature set.
CSCvn67870	Reorder ip nat configuration - to be placed after ip http configuration.
CSCvn69629	ND packets received in remote vtep SISF table - EVPN part.
CSCvn76837	DMVPN Phase 2 shortcut triggered from a spoke behind PAT may end up in stuck DNX state.
CSCvn78203	Router crashed when printing logs while constructing rekey packets (GETVPN)
CSCvn78349	FlexVPN with password encryption - keyring aaa LIST password 6 xxxxx encrypted again upon reload.
CSCvn82063	Input CRC counter increasing on Tengi interface.
CSCvn82245	EIGRP session is not coming up if the dynamic PBR is applied on interface.
CSCvn85422	Int index is 0 for the Cellular inteface in the exported flow.
CSCvo00664	SUP reload after running the command " show plat hard qfp act infr bqs debug qmrt_dump ".
CSCvo01206	Curie:Device is crashing while swapping between PoE and Non-PoE NIM-ES2-8 Module in slot 0/1.
CSCvo01298	Correction to Quick RP3 recovery after the Punt Path XAUI link goes down
CSCvo03458	PKI "revocation check crl none" does not fallback if CRL not reachable.
CSCvo08132	BUILT-IN-2T+20X1GE - VLAN bytes and packets counters are frozen.
CSCvo08337	Crash when inserting second NIM-2MFT-T1/E1 in Cisco 4331 ISR
CSCvo09059	No autostate" will auto add after re-configure svi interface.
CSCvo09246	Cisco 4351 ISR communication down few minute after shutdown/no shutdown interface.
CSCvo11361	Priority queueing on port-channel interfaces causes frame re-ordering.

Caveat ID Number	Description
CSCvo11786	SCCP Application does not clear failed sockets leading to leak and socket pool exhaustion.
CSCvo12745	Packet drop occurs after acl permit configurations.
CSCvo17738	Cellular interface lte Network Selection Mode switches to manual.
CSCvo19395	Router crashes when removing a crypto map.
CSCvo21122	Memory leak at hman process.
CSCvo22398	Cisco 4000 Series ISR with NIM-ES2 do not forward STP Uplink Fast dummy packet..
CSCvo27553	PKI incorrect fingerprint calulation during CA authentication
CSCvo30329	Router crashing after upgrade due to Crypto commands "Block overrun at 284B2160 (red zone 000110DF)".
CSCvo30641	Traceback: Error seen after tunnel flap: DATACORRUPTION-1-DATAINCONSISTENCY.
CSCvo36188	Crash at NAT clear.
CSCvo38985	Crash at the VRF configuration.
CSCvo43897	Cisco 4331 ISR, wrongly adding to Port to subscriber field after translation.
CSCvo45257	Memory leak in ios_portal_vty_run_cmd.
CSCvo46127	MaxSusRate is not working with service class.
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
CSCvo57746	CPUHOG while unconfiguring vrf with 1M vxlan static routes
CSCvo61610	FXS - no busy tone is generated on remote-onhook condition with call pickup scenario.
CSCvo61772	"ip nat translation port-timeout" limited to overflows after reaching 16bit.
CSCvo61914	GC NAT unable to detect dns packet.
CSCvo62584	DHCP discover packets were being dropped at firewall since UDP source port as 0.
CSCvo66216	IPSec-Session count in "show crypto eli" reaches max causing VPN failure.
CSCvo69320	ISR ipv6/dhcp tloc got DCONFAIL failure when connecting to vbond.
CSCvo71445	MACSEC license is not being consumed for sub-interfaces.

Caveat ID Number	Description
CSCvo74486	IOS-XE ACL port information preserved after encapsulation.
CSCvo75992	tdl_fw_stats in FMAN logs errors.
CSCvo76641	L2 EVPN: When global and per-evi replication type different, wrong IP address is selected for IMET.
CSCvo78046	AWS: UDI serial changes when CSR 1000v instance type is changed from c4 to c5 or vice versa
CSCvo80960	Streaming CRCs seen with GLC-GE-100FX VID: V02 on Cisco 4000 Series ISR.
CSCvo83945	Ping failure on Port-channel sub interface when is using EVC in main port channel..
CSCvo84147	Cisco 4000 Series ISR TCP SEQ/ACK number wrongly inserted after OUT to IN NAT translation.
CSCvo87488	GetCACaps is using wrong CA-IDENT when using enrollment profiles.
CSCvo90060	Wrong label programming leading to traffic drop.
CSCvo94211	Traffic stops flowing on Xconnect tunnel when upgraded to 16.9.2.
CSCvo99156	Unexpected reload in btrace routines due to division by NULL.
CSCvp00271	Read and Write lock fix for ACL cache.
CSCvp05070	Overlay BGP down when configured "ip nhrp server-only".
CSCvp16730	Incoming ESP packets with SPI value starting with 0xFF are dropped due to Invalid SPI error.
CSCvp25052	Cisco 4000 Series ISR: Router crash due to twice memory release.
CSCvp38317	MGCP GW does not reset SSRC/ROC on receiving MDCX with new IP/port/SDP parameter for SRTP call.
CSCvp38424	On-Prem DMVPN fails to establish a dynamic tunnel between Spoke nodes.
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
CSCvp56737	Counters of interfaces are reporting inexistent peaks.
CSCvp62811	Engine keyword missing after "show utd engine standard statistics url-filtering".
CSCvp63616	Crash due to too many DSPs.
CSCvp70211	Crash when running show crypto map.

Caveat ID Number	Description
CSCvp75121	Ucode crash when PfRv3 and IPv6 monitor are configured on the same tunnel with IPv6 VRF configured.
CSCvp81102	IPsec SA installation fails with simultaneous negotiations despite fix for CSCve08418.
CSCvp92334	Crash after Media monitor look up.
CSCvq00263	Device crashed @ radius_io_stats_timer_handler due to dynamic-author.
CSCvq11196	SR Policy: crash in HA module.
CSCvq18793	NIM-2FXS/4FXOP crashing due to DSP failed to reply properly.
CSCvq20321	Console connection sometimes hangs after unplug cable used for ssh
CSCvq39840	CiscoFlashFile - Get-Next request takes longer time for last file on directory.
CSCvq40443	"Clock: inserting leap second" message does not output on NTP client when leap second inserted.
CSCvo75172	TE configuration is not nvgened which are configured under IS-IS.
CSCvq06645	Parser warning appears on the console %PARSER-5-HIDDEN: Warning!!!.
CSCvp79162	CoA with DHCPv6 PD prefix fails on the ISG session.
CSCvn56059	Cisco 4300 ISR ROMMON: Enable FastBoot.
CSCvn67410	Cisco 4462 ISR UEFI: The BIOS always takes the MRC ColdBoot path.
CSCvn67286	Cisco 4462 ISR UEFI: Specifically enable FastBoot(Cold) and disable RMT and memory testing.
CSCvn57779	ISR4K UEFI: Reduce network driver initialization time.
CSCvn75660	Cisco 4462 ISR ROMMON: Missing Microloader Certificate Serial Number
CSCvm74048	Cisco 4200 ISR ROMMON: Enable AER support for PCIe errors.

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.