Release Notes for Cisco 4000 Series ISRs, Cisco IOS XE Amsterdam 17.2.x

First Published: 2020-05-07

Last Modified: 2020-04-09

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 Amsterdam 17.2.1 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

The following table lists the recommended Rommon and CPLD versions for Cisco IOS XE 17.2.x onwards releases.

Table 1: Recommended Firmware Versions

Cisco 4000 Series ISRs	Existing RoMmon	Cisco Field-Programmable Devices	CCO URL for the CPLD Image
Cisco 4461 ISR	16.12(2r)	21102941	isr_4400v2_cpld_update_v20.SPA.bin isr4400v2hwprogrammdb040100SPA.pkg
Cisco 4451 ISR	16.12(2r)	19042950	isr4400_cpld_update_v20.SPA.bin
Cisco 4431 ISR	16.12(2r)	19042950	isr4400_cpld_update_v20.SPA.bin
Cisco 4351 ISR	16.12(2r)	19040541	isr4300_cpld_update_v20.SPA.bin

Cisco 4000 Series ISRs	Existing RoMmon	Cisco Field-Programmable Devices	CCO URL for the CPLD Image
Cisco 4331 ISR	16.12(2r)	19040541	isr4300_cpld_update_v20.SPA.bin
Cisco 4321 ISR	16.12(2r)	19040541	isr4300_cpld_update_v20.SPA.bin
Cisco 4221 ISR	16.12(2r)	19042420	isr4200_cpld_update_v20.SPA.bin

Note Cisco 4461 ISR may require two upgrade packages to upgrade to 21102941. See CPLD-4-1 Release Notes.

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.

New and Changed Information

New Hardware Features in Cisco IOS XE Amsterdam 17.2.1

There are no new hardware features for this release.

New Software Features in Cisco 4000 Series ISRs Release Cisco IOS XE Amsterdam 17.2.1

The following features are supported by the Cisco 4000 Series Integrated Services Routers for Cisco IOS XE Amsterdam 17.2.1:

Note Cisco IOS XE Amsterdam 17.2.1r is the first release for Cisco 4000 Series ISRs in the Cisco IOS XE Amsterdam 17.2.1 release series.

- Install and Deploy Cisco IOS XE and Cisco IOS XE SD-WAN Functionality on Edge Platforms—This feature supports the use of a single universalk9 image to deploy Cisco IOS XE SD-WAN and Cisco IOS XE functionality on all the supported devices. This universalk9 image supports two modes - Autonomous mode (for IOS XE features) and controlled mode (for SD-WAN features).
- 6VPE over DMVPN with IPv6 Transport—This feature supports multi-tenant IPv6 LAN prefixes over IPv4 overlay neighborship, which is created over an IPv6 DMVPN transport.
- Block BGP Dynamic Neighbor Sessions—With this feature, you can block a router from establishing BGP dynamic neighbor sessions with certain nodes in a BGP peer group, these nodes are identified with their IP addresses. The ability to shut down or prevent the creation of BGP dynamic neighbor sessions can be useful when a peer needs maintenance.
- CUBE: Fax detect for IP-IP flows with Cisco IOS XE—Support for fax detection for IP to IP flows with Cisco IOS XE.
- CUBE: Smart Licensing based on Dynamic Call Counting— Support for Smart Licensing based on dynamic call counting.

  For a more detailed overview on Cisco Licensing, go to https://cisco.com/go/licensingguide.
- CUBE: Cisco 4461 ISR Platform Support — Support for Cisco Unified Border Element on Cisco 4461 ISR.
- DHCP Client Operation—This feature introduces support for unicast mode on DHCP. This helps with splitting the horizon therefore improving security of the network.
- Fail Close Revert Mode—When there is no rekey or the group member is not able to re-register to the key server, group members in GETVPN can remove the downloaded key server policy, and thereby return to the fail close mode.
- LISP Support for TCP Authentication Option— You can use TCP Authentication Option (TCP AO) to be secured against spoofed TCP segments in the sessions between an ETR and an MS.
- MACSec on Port Channel—With MACsec support on port channels, you can now configure encryption for port-channels, and therefore increasing the security of the traffic. This is only applicable for port-channels which have member-links with the MACSec (PHY) encryption capablilities.
- Debug Commands for PIM and VRF—This feature introduces debug commands for VRF (**debug condition vrf**) and PIM (**debug ip pim**) details. The **debug condition vrf** command lets you limit the debug output to a specific virtual routing and forwarding (VRF) instance. The **debug ip pim** command displays PIM packets received and transmitted, as well as PIM related events.
- Support for YANG Models for SIP-FXS/FXO trunk and Unified SIP SRST—Support for YANG Models for SIP-FXS/FXO trunk and Unified SIP SRST.
- Tunneling and Forwarding Protocols—The Layer 2 Tunneling Protocol on Cisco 4000 Series ISRs with switchport does not make any change to L2 PDU, and forwards it to service provider devices.
- VPN-ID in NetFlow Exported Packet—With the VPN-ID in Netflow exported packet, you can now identify a VPN using the MPSL VPN-ID.

- IP Multiplexing: Restriction and Limitation—This features introduces IP multiplexing support on Cisco 4000 Series ISRs to optimize IPv4 and IPv6 traffic in environments such as a satellite network, where packet-per-second transmission limitations causes inefficient bandwidth utilization.
- Performing Factory Reset—You can use the **factory-reset all secure** command to reset the router and securely clear the files stored in the bootflash memory.
- SRST: Voice VRF support with Cisco IOS XE—this feature provides support for Voice VRF for Unified SRST.
- Support for Spoke Nodes as P Nodes in MPLS over DMVPN Phase 3—With this feature, you can configure a spoke node as either a P node or PE node in an MPLS over DMVPN deployment. To configure the spoke node, MP-BGP is required to redistribute the route or label information between the spoke node and a PE node behind it.

Configure the Cellular Back-off Operation

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

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

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

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

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

Configure the Router for Web User Interface

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

- An HTTP or HTTPs server must be enabled with local authentication.
- A local user account with privilege level 15 and accompanying password must be configured.
- Vty line with protocol ssh/telnet must be enabled with local authentication. This is needed for interactive commands.
- 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

Open Bugs - Cisco IOS XE Amsterdam 17.2.2

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

Caveat ID Number	Description
CSCvt85954	IWAN routers: Cisco 4000 Series ISRs reloads multiple times.
CSCvu04160	Unexpected reload in device classifier code due to segmentation fault.
CSCvu27910	Controller crashes when FNF is configured under physical interface.
CSCvu41583	Controller crashes when FNF is configured under physical/port-channel interface.
CSCvv03229	Crash in sre_dp_traverse_dfa_legacy as SIP invite messages crosses a GRE Tunnel.
CSCvv21125	Interface qlimit size decreases causing output / tail drops.
CSCvv65068	Crash after flexible netflow cache cleanup.
CSCvv71238	Sup crashed with cpp-bqs fatal.

Resolved Bugs - Cisco IOS XE Amsterdam 17.2.2

Caveat ID Number	Description
CSCvh24730	PfRv3: Crash while printing the same TCA message.
CSCvp24405	Router crashes after adding macsec reply-protection command on an interface.
CSCvp88044	Performance monitor crash.
CSCvq42698	Update "bandwidth remaining percent" doesn't take effective reliably on datapath.
CSCvr42504	Ping is not working on port-channel after router reload.

Caveat ID Number	Description
CSCvr76593	Memory leak in CC-API_VCM and CCSIP_SPI_CONTROL.
CSCvr85094	Enabling Telemetry can cause router to crash.
CSCvs42075	Crash with shared-line command
CSCvs63606	Ping fails on hundred gig primary interface with FRR configured though MPLS traffic is not impacted.
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.
CSCvs90555	Template push fails when enabling ipv4 addr family on BGP ipv4 neighbor.
CSCvt02534	Cisco 4000 Series ISR: Unexpectedly Reboots with CENT-BR-0.
CSCvt02567	BGP crash @ bgp_db_ipstr2address when get bgp neighbor via bgp-oper yang
CSCvt05460	IOS-XE: NAT not work for Active FTP.
CSCvt12245	16.12.3 ZBFW-Mismatch in firewall stats between the device and vmanage.
CSCvt15007	Unable to detach device from Integration Management
CSCvt18190	Router crash when doing 'show bgp ipv6 unicast summary'
CSCvt19772	Stackwise Virtual FMAN-RP IPC channel stuck (paused).
CSCvt21373	unexpected reload in CPP ucode forced by nat 514.
CSCvt33018	MACsec 128/256 XPN on 40g/100g, stop passing traffic for one of AN and interface link flap seen.
CSCvt38466	SNMP TIMETICKS difference between sysUpTime vs ipslaEtherJAggStatsStartTimeId.
CSCvt40021	Omp-tag is not being set via route-map configuration under BGP.
CSCvt42659	Possible Regression Cisco 4000 Series ISR Mgmt Port ACL Breakage or simply day one implementation as designed.
CSCvt48480	Flow monitor is removed from interface configuration on reload
CSCvt54359	BGP config does not rollback if template push errors out.
CSCvt57181	Leaf sends packets to a wrong BVI MAC of ASR GOLF routers.
CSCvt58616	L2VPN Crash @ Process = XC Mgr.
CSCvt58858	Incorrect CEF programming for local SVI.
CSCvt60040	VPLS:MAC learning not happening on SSO.
CSCvt60979	ODN Policy for Global prefix still UP even after withdrawing global routes.

Caveat ID Number	Description
CSCvt65588	FlexVPN IKEv2 Tunnel route removed after establishing new IKEv2 SA to another peer.
CSCvt67752	Object (IPv6 ACL) stuck in forwarding data plane. No ipv6 traffic goes towards the upstream router.
CSCvt73592	Missing/corrupt IOS-XE PKSC10 format.
CSCvt74694	Cert validation failures seen for traffic after template push with SSL.
CSCvt76409	Crash due to "Crimson flush transactions Process".
CSCvt78405	Code review: Just fire assert when we reach limit of counter.
CSCvt89337	Incorrect Source IP when resolving DNS.
CSCvt89441	IOS-XE device crashed with CGD shared memory corruption freed by FMAN-FP.
CSCvt94577	Incorrect CEF entry for LISP action signal-fwd.
CSCvt98034	BGP communities: changes to route-map which sets BGP communities discards existing communities.
CSCvu00956	Cisco 9600 HA / quad-SUP SVL, on enable and disable of IOX, supervsior reloads silently.
CSCvu21761	RAR: PADG and PADC are not being consumed properly. PPPoE session statistics are not matching.
CSCvu22576	Keepalive CLI needs to be unhidden for GRE tunnel.
CSCvu23567	RSP3: BGP crash seen on Stand by router when 100 BGP sessions are established.
CSCvu26678	Some qos config lost during upgrade to 17.02.
CSCvu26741	Punt-Keepalive crash with lsmpi_lo_drv and container app traffic.
CSCvu27813	Complete Traffic drop seen on Head Node Post configuring Binding SID on PFP Policy.
CSCvu34381	Packets are not dropped as expected in selfzone to zone vpn 0 firewall configuration.
CSCvu52218	Router crashes frequently on NBAR.
CSCvu54786	Crash on configuring a highest key identifier for OSPF authentication under an interface.
CSCvu65669	Traffic drop from branch overlay ping to service side without zp vpn1 to vpn1 when FW and IPS enabled.
CSCvu66723	Evaluation of CVE-2020-10188 - Cisco IOS XE Persistent Telnet.
CSCvu80644	LSP Checksum error when default-info originate is configured.
CSCvu87786	CUBE Segmentation Fault @ sipSPIFreeOneSCB due to corrupt ccb.

Caveat ID Number	Description
CSCvu99616	Snort initiate reset and Failed to load - Real websites in Browser.
CSCvv05893	CUBE router crashed due to memory corruption in subscription control block.
CSCvv16164	RSVP TE is not working for broadcast interfaces .
CSCvv20380	Removing and Adding Bulk ACL leads to Tracebacks and Error-Objects.

-

Open Bugs - Cisco IOS XE Amsterdam 17.2.1

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

Caveat ID Number	Description
CSCvh24730	PfRv3: Crashes while printing the same TCA message.
CSCvt28663	Traffic do not get dropped when UTD and Appfw is enabled together.
CSCvt25235	Performance degradation in Collab, Conatact centre and Mifid recorder flows.

Resolved Bugs - Cisco IOS XE Amsterdam 17.2.1

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

Caveat ID Number	Description
CSCvg79330	Enabling platform IPsec control plane conditional debug might cause FP/QFP IPsec outbound SA leak.
CSCvp72039	Ucode crashes in infra with injected jumbo packet.
CSCvq47444	The "config-exchange request" command for any ikev2 profile has inconsistent behavior between IOS and confd.
CSCvq71864	Crashes after executing the **show archive config differences** command.
CSCvq75610	The freed rpi_parent is hit when deleting parent route by route update event.
CSCvq87063	The getvpn suiteb:KS sends delete payload to gm's while scheduled rekey after primary KS dead/readded.
CSCvq90361	The NHRP process crashes on using same tunnel address on multiple spokes.
CSCvq93850	The passive FTP will fail when going over NAT and either client or server are off a SM-X-ES3.
CSCvq98999	The Cisco 4451-X ISR crashes when IPsec SA installation fails.
CSCvq99498	Crash is seen when trying to bring-up / bring-down IPsec crypto session for OSPFv3.
CSCvr05193	Cisco IOS PKI | intermittently SubCA fails to rollover.

Caveat ID Number	Description
CSCvr05214	NAT translation table is removed before IKE SA deleted when idle timeout occur.
CSCvr15127	Cisco 4000 Series ISR calls fade to no-way audio due to media inactivity detection after 20 minutes.
CSCvr17169	The qfp ucode crashes with media monitor.
CSCvr18570	When user cancel Call Forward All from the analog phone, user cannot hear the confirmation tone.
CSCvr24498	keyman_rp Memory Leak.
CSCvr26524	Crash is seen due to NBAR classification.
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.
CSCvr42776	FMAN crashed after firewall reconfiguration.
CSCvr42823	Umbrella local domain bypass list is not programmed to DP, FMFP-3-OBJ_DWNLD_TO_DP_FAILED.
CSCvr48349	ESP ucode crashed when running NAT with bpa (CGN).
CSCvr57565	MGCP Calls with SRTP fail to connect with Cause Value=47 due to T.38 calls.
CSCvr61217	GetVPN-Cisco 4461 ISR Getvpn traffic is failing with Transport mode with all the versions.
CSCvr76534	Cisco 4000 Series ISR crashes at Process Exec.
CSCvr87906	Cisco 4461 ISR: Large un-fragmented IPSEC packets cause router to crash
CSCvr89957	CFT crashed frequently.
CSCvr89973	NIM interfaces go into shutdown after router bootup.
CSCvr96597	Cisco IOS XE crashes after doing a SCEP enrollment.
CSCvr99034	Cisco 4000 Series ISR crashes during updating the OpenDNS bypass allowedlist.
CSCvs00410	MKA session up but unable to pass data across link using AES-256-XPN cipher
CSCvs13960	IWAN's CPU and memory usage is high.
CSCvs29535	IWAN crash is related to DCA channel.
CSCvs70052	ALG with NAT triggers a crash when a DNS writeback occurs.
CSCvs86573	Connect message is never forwarded to the calling side.

Related Documentation

Cisco IOS Software Documentation

The Cisco IOS XE Amsterdam17.x software documentation set consists of Cisco IOS XE Amsterdam17.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 Amsterdam 17.x release train. These Cisco IOS command references support all Cisco platforms that are running any Cisco IOS XE Amsterdam 17.x software image.

See https://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-xe-17/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.