



# Release Notes for Cisco 4000 Series ISRs, Cisco IOS XE Cupertino 17.9.x

---

**First Published:** 2022-08-26

**Last Modified:** 2024-09-26

## Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

## Cisco 4000 Series Integrated Services Routers Overview



**Note** Cisco IOS XE Cupertino 17.9.1a is the first release for Cisco 4000 Series Integrated Services Routers in the Cisco IOS XE 17.9.x release series.

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	

## Product Field Notice

Cisco publishes Field Notices to notify customers and partners about significant issues in Cisco products that typically require an upgrade, workaround or other user action. For more information, see <https://www.cisco.com/c/en/us/support/web/field-notice-overview.html>.

We recommend that you review the field notices to determine whether your software or hardware platforms are affected. You can access the field notices from <https://www.cisco.com/c/en/us/support/web/tsd-products-field-notice-summary.html#%7Etab-product-categories>.

## 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 17.9.x 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 [Installing 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	<a href="#">isr_4400v2_cpld_update_v20SPA.bin</a> <a href="#">isr44002hwprogrammable04010SPA.pkg</a>
Cisco 4451-X ISR	16.12(2r)	19042950	<a href="#">isr4400_cpld_update_v20SPA.bin</a>
Cisco 4431 ISR	16.12(2r)	19042950	<a href="#">isr4400_cpld_update_v20SPA.bin</a>
Cisco 4351 ISR	16.12(2r)	19040541	<a href="#">isr4300_cpld_update_v20SPA.bin</a>

Cisco 4000 Series ISRs	Existing ROMMON	Cisco Field-Programmable Devices	CCO URL for the CPLD Image
Cisco 4331 ISR	16.12(2r)	19040541	<a href="#">isr4300_cpld_update_v20.SPA.bin</a>
Cisco 4321 ISR	16.12(2r)	19040541	<a href="#">isr4300_cpld_update_v20.SPA.bin</a>
Cisco 4221 ISR	16.12(2r)	19042420	<a href="#">isr4200_cpld_update_v20.SPA.bin</a>



**Note** Cisco 4461 ISR may require two upgrade packages to upgrade to 21102941. See [CPLD-4-1 Release Notes](#).

## 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://cfng.cisco.com/>. An account on cisco.com is not required.

## New and Changed Information

### New and Changed Hardware Features

There are no new hardware features for this release.

### New and Changed Software Features in Cisco IOS XE 17.9.6

There are no new features in this release.

### New and Changed Software Features in Cisco IOS XE 17.9.5a

There are no new features in this release.

### New and Changed Software Features in Cisco IOS XE 17.9.4a

There are no new features in this release. This release provides a fix for [CSCwh87343](#): Cisco IOS XE Software Web UI Privilege Escalation Vulnerability. For more information, see the Security Advisory: [cisco-sa-iosxe-webui-privesc-j22SaA4z](#).

## New and Changed Software Features in Cisco IOS XE 17.9.4

There are no new software features in this release.

## New and Changed Software Features in Cisco IOS XE 17.9.3a

There are no new software features in this release.

## New and Changed Software Features in Cisco IOS XE 17.9.2a

There are no new software features in this release.

## New and Changed Software Features

*Table 2: New Software Features in Cisco IOS XE 17.9.1a*

Feature	Description
<a href="#">IPsec Dual Stack Support on Non-Cisco Devices</a>	This feature provides the capabilities to carry both IPv4 and IPv6 traffic using a single IPsec Security Association (SA) that is tunnelled over IPv4. From IOS XE release 17.9.1a onwards, Cisco supports specific subnets in the access control list when the ingress end of the tunnel interface is configured with a third party IPsec client. With the introduction of the SVTI single security association dual stack feature, you can now manage the business-to-business services and other IOT business efficiently.
<a href="#">Support for BGP additional paths with label-unicast unique mode</a>	This enhancement introduces support for configuring BGP additional paths when label-unicast unique mode is configured.
<a href="#">Support for Unicast-to-Multicast Destination Reflection</a>	This feature introduces support for configuration of unicast-to-multicast destination reflection to facilitate unicast-to-multicast destination translation and unicast-to-multicast destination splitting. It also provides the capability for users to translate externally received unicast destination addresses to multicast addresses.
<b>Cisco Unified Border Element (CUBE) Features</b>	
<a href="#">End-to-end Secure Calling for Courtesy Call Back and Unified Contact Center Survivability</a>	With the Cisco Voice Portal (CVP) application, a caller may request an automated callback, rather than wait in a queue for an extended period. When an agent becomes available, CVP sends a request to place a call to the original caller. When the call is answered, the agent is connected. With this update, outbound calls over a secure SIP PSTN trunk are possible.

Feature	Description
<a href="#">Load Balancing for DNS SRV Host</a>	This enhancement to the DNS session target feature, provides effective call distribution and load balancing of calls based on the preference, priority and availability of hosts provided in DNS SRV Resource Records. This feature further simplifies configuration by allowing effective call distribution with a single dial-peer.
<a href="#">Options Ping for DNS SRV Hosts</a>	Previously, CUBE (Local Gateway) had to be configured with separate dial-peers to monitor the availability of individual proxies used in services such as Webex Calling. To simplify this configuration, all targets resolved from a DNS SRV record may now be monitored using a common Options Ping policy defined for a single dial-peer. If a remote server becomes unresponsive, CUBE will busy out that destination, allowing calls to be sent to alternative destinations.
<a href="#">Transfer of Call Detail Records Using SFTP</a>	Cisco IOS gateways can use FTP and now SFTP servers to transfer call accounting files.
<a href="#">Webex Calling Branch Survivability</a>	<p>From Unified SRST 14.3, new CLI commands are introduced to support the forthcoming Webex Calling Site Survivability mode. This feature will only be available for use when the Webex Calling Site Survivability solution is made available through Webex Control Hub.</p> <p><b>Note</b> Customers using the CUBE WebSocket forking feature with the Cisco Agent Answers solution should not use the Cisco IOS XE Cupertino 17.9.1a release. We recommend that you use the Cisco IOS XE Bengaluru 17.6.x release for this feature.</p>
<p><b>Programmability Features</b></p>	
<a href="#">Pubd Restartability</a>	The pubd process is restartable on all platforms in this release. Prior to this release, pubd was restartable only on certain platforms. On other platforms, to restart the pubd process, the whole device had to be restarted.
<p><b>Smart Licensing Using Policy Features</b></p>	

Feature	Description
Hostname support	<p>Support for sending hostname information was introduced.</p> <p>If you configure a hostname on the product instance and disable the corresponding privacy setting (<b>no license smart privacy hostname</b> command in global configuration mode), hostname information is sent from the product instance, in a separate sync message or offline file.</p> <p>Depending on the topology you have implemented, the hostname information is received by CSSM, CSLU, and SSM On-Prem. It is then displayed on the corresponding user interface.</p> <p>For more information, see <a href="#">license smart (global config)</a></p> <p>With the introduction of this enhancement, the hostname limitation which existed from Cisco IOS XE Amsterdam 17.3.2 to Cisco IOS XE Cupertino 17.8.x – is removed. In these earlier releases, hostname information is not sent or displayed on various licensing utilities (CSSM, CSLU, and SSM On-Prem).</p>
Inconsistent system behavior for <b>license boot</b> global configuration command rectified	<p>The system does not allow overlapping suite and technology package configuration to co-exist.</p> <p>For more information, see <a href="#">license boot</a>.</p>
New mechanism to send data privacy related information	<p>A new mechanism to send data privacy related information was introduced. This information is no longer included in a RUM report.</p> <p>If data privacy is disabled (<b>no license smart privacy {all hostname version}</b> command in global configuration mode), data privacy related information is sent in a separate sync message or offline file.</p> <p>Depending on the topology you have implemented, the product instance initiates the sending of this information in a separate message, or CSLU and SSM On-Prem initiates the retrieval of this information from the product instance, or this information is saved in an offline file.</p> <p>For more information, see <a href="#">license smart (global config)</a>.</p>

Feature	Description
RUM Report Throttling	<p>For all topologies where the product instance initiates communication, the minimum reporting frequency is throttled to one day. This means the product instance does not send more than one RUM report a day.</p> <p>The affected topologies are: <i>Connected Directly to CSSM</i>, <i>Connected to CSSM Through CSLU</i> (product instance-initiated communication), <i>CSLU Disconnected from CSSM</i> (product instance-initiated communication), and <i>SSM On-Prem Deployment</i> (product instance-initiated communication).</p> <p>This resolves the problem of too many RUM reports being generated and sent for certain licenses. It also resolves the memory-related issues and system slow-down that was caused by an excessive generation of RUM reports.</p> <p>You can override the reporting frequency throttling, by entering the <b>license smart sync</b> command in privileged EXEC mode. This triggers an on-demand synchronization with CSSM or CSLU, or SSM On-Prem, to send and receive any pending data.</p> <p>RUM report throttling also applies to the Cisco IOS XE Amsterdam 17.3.6 and later releases of the 17.3.x train, and Cisco IOS XE Bengaluru 17.6.4 and later releases of the 17.6.x train. From Cisco IOS XE Cupertino 17.9.1, RUM report throttling is applicable to <i>all</i> subsequent releases.</p>
Virtual Routing and Forwarding (VRF) Support	<p>On a product instance where VRF is supported, you can configure the <b>license smart vrf vrf_string</b> command and use a VRF to send licensing data to CSSM, or CSLU, or SSM On-Prem.</p> <p><b>Note</b> When using a VRF, the supported transport types are <b>smart</b> and <b>cslu</b> only.)</p> <p>For more information, see <a href="#">license smart (global config)</a>.</p>

## 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](#).

## 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.

---

## Resolved and Open Bugs in Cisco 4000 Series Integrated Services Routers

### Resolved Bugs - Cisco IOS XE 17.9.6

All resolved bugs for this release are available in the [Cisco Bug Search Tool](#).

Bug ID	Description
<a href="#">CSCwj70335</a>	Crypto IKEv2 - Fragmented Authentication packets detected as malformed on 3rd party vendor device
<a href="#">CSCwj08744</a>	Unexpected reload when using "show running-config full   format"
<a href="#">CSCwi93422</a>	Unexpected reload due IPV6 TCP packet in QFP
<a href="#">CSCwh96578</a>	SKA_PUBKEY_DB leak in TDL

Bug ID	Description
<a href="#">CSCwi88969</a>	FMFP-3-OBJ_DWNLD_TO_DP_FAILED observed when delete and configure zone-pair back
<a href="#">CSCwi06843</a>	Endpoint tracker triggers a CPU Hog
<a href="#">CSCwi68865</a>	Memory leak in Crypto IKEv2 due to C_NewObject
<a href="#">CSCwj88872</a>	IPsec tunnel fails to establish due to error IPsec policy invalidated proposal
<a href="#">CSCwj92234</a>	IR1833: UNIX-EXT-SIGNAL: Segmentation fault(11), Process = Cellular CNM
<a href="#">CSCwi70559</a>	SFP-10G-LRM starting with SN OPMxxxxxxxx not detecting in ISR4000 with SM-X-4X1G-1X10G module
<a href="#">CSCwj84949</a>	Unencrypted Traffic Due to Non-Functional IPsec Tunnel in FLEXVPN Hub & Spoke Setup
<a href="#">CSCwj40589</a>	Endpoint tracker using DNS does not log "DOWN" message when DNS server reachability is lost
<a href="#">CSCwk33173</a>	EzPM application-performance profile cause memory leak and crash with long-lived idle TCP flows
<a href="#">CSCwh40073</a>	Interoperability issue between Cisco ISR and Juniper ACX/MX devices with a direct fiber connection
<a href="#">CSCwi82405</a>	mGRE Tunnels with shared ipsec profile cause ucode crash
<a href="#">CSCwb47658</a>	Repeated and endless messages "Network change event - activated 4G Carrier Aggregation."
<a href="#">CSCwi08171</a>	Router may crash due to Crypto IKMP Process
<a href="#">CSCwj45130</a>	Segmentation Fault - Process = IPsec dummy packet process
<a href="#">CSCwj86794</a>	ASR1K crashes while processing an NWPI trace
<a href="#">CSCwi06404</a>	PKI crash after failing a CRL Fetch
<a href="#">CSCwk12524</a>	Device reloaded due to ezManage mobile app Service.
<a href="#">CSCwh73202</a>	IOS-XE unexpected reboot due to Critical process qfp_ucode_utah fault on fp_0_0 (rc=139)
<a href="#">CSCwj72888</a>	Reload in tcp_sanity due to l4 pointer not set
<a href="#">CSCwj48421</a>	FlexVPN Client : IPsec tunnels are down due to issue with SADB detach and delete
<a href="#">CSCwi78060</a>	Woodlawn SM-X - Marvell Phy Errata + MAC reset adjustment
<a href="#">CSCwi25737</a>	Router should discard IKE Notification messages with incorrect DOI
<a href="#">CSCwj36915</a>	C-NIM-2T: macsec not working under LACP port-channel member port

Bug ID	Description
<a href="#">CSCwh50628</a>	Race condition crash on IOS-XE device
<a href="#">CSCwi78365</a>	Trim installed certificate on upgrade
<a href="#">CSCwk53680</a>	[vg400] Inbound calls through VG400 results in phantom calls (64.3.0, 60.1.4, 62.3.3)
<a href="#">CSCwi09301</a>	Shutting a Dialer interface with PPPoA unshuts it automatically
<a href="#">CSCwj49297</a>	ISR 4351 send out BYE message with high RTT to CUCM (64.2.0/62.3.2/60.1.3)
<a href="#">CSCwe70259</a>	Nightwatch interface flapping when configure 100M Full with crossover cable
<a href="#">CSCwk15127</a>	Failure to communicate a period of time after the stp status changes
<a href="#">CSCwi66850</a>	C-SM-16P4M2X stuck in Bootloop when "platform urpf" command issued.
<a href="#">CSCwj73113</a>	MGCP GW doesn't respond with 250 OK for a DLCX leading to DLCX loop from CUCM side
<a href="#">CSCwi18456</a>	no voice in 3way conference on 4461 DSPfarm
<a href="#">CSCwj30334</a>	Router rebooted when attempting merge on used CVLA block

### Open Bugs - Cisco IOS XE 17.9.6

All open bugs for this release are available in the [Cisco Bug Search Tool](#).

Bug ID	Description
<a href="#">CSCwk53231</a>	ISR 4k - ISR4451-X-4x1GE - Front Panel (FPGE) Interface stops passing traffic
<a href="#">CSCwj79987</a>	C1121X SD-WAN Router does not establish BFD sessions after upgrade to 17.9.3a or 17.9.4a
<a href="#">CSCwk89256</a>	vManage/IOS-XE 17.9.3 speed mismatch in IOS-XE configuration after device template push for ISR
<a href="#">CSCwk31560</a>	NAT Command not readable after reloaded
<a href="#">CSCwj44868</a>	GETVPN COOP KS   Wrong Severity for Rekey Acknowledgement configuration mismatch log message
<a href="#">CSCwm07651</a>	ISR4K crash due to dbgd process
<a href="#">CSCwj77594</a>	IOS XE Controller Mode - WAN IP is allowed to be configured as SYSTEM IP
<a href="#">CSCwk49806</a>	ASR1002-HX router running IOS 17.06.05 rebooted unexpectedly due to process NHRP crash
<a href="#">CSCwi31110</a>	Traceback seen @_nhrp_cache_delete due to negative global cache count
<a href="#">CSCwb55514</a>	Unexpected reboot of the ESP seen after enabling "platform qos port-channel-aggregate"
<a href="#">CSCwe22066</a>	Unexpected reload on IOS XE device due to cmand process with PIM

Bug ID	Description
<a href="#">CSCwk63722</a>	Startup Configuration Failure Post PKI Server Enablement
<a href="#">CSCwi33168</a>	DSP reporting out of range utilization values in SNMP
<a href="#">CSCwh44418</a>	ARP incomplete in VRF Mgmt-intf - G0/0/0 - Switch -G0
<a href="#">CSCwk75459</a>	MGCP GW fails to respond with 250 OK when there's a delay from dataplane in gathering stats
<a href="#">CSCwf73123</a>	BFD timers reverting back to default value after negotiating correctly
<a href="#">CSCwk61133</a>	process IOMd memory leak due to POE TDL message
<a href="#">CSCwk03686</a>	Crash due a segmentation fault due a negative value
<a href="#">CSCwb25507</a>	CWMP : Add vendor specific parameter for NBAR protocol pack version
<a href="#">CSCwh50510</a>	Router Crash with Segmentation fault(11), Process = NHRP when processing NHRP traffic
<a href="#">CSCwk31715</a>	After deleting a NAT configuration, the IP address still shows up in routing table.
<a href="#">CSCwm27005</a>	"CCA Detected Logic Error, code = 14" Traceback seen constantly
<a href="#">CSCwf25735</a>	ASR1009x QoS more than four remark with set-cos not work
<a href="#">CSCwk30527</a>	IKEv2 session is down after reload if identity local address is assigned to interface on Switch
<a href="#">CSCwh45169</a>	Unexpected Reboot while Displaying Information from Cleared SSS Session
<a href="#">CSCwk44078</a>	GETVPN / Migrating to new KEK RSA key doesn't trigger GM re-registration
<a href="#">CSCwm27647</a>	BFD sessions are down and not recovering for one color after Hub replacement
<a href="#">CSCwm32269</a>	Cisco DNA Center - SBEN Onboarding fails - EAP-TLS Failed to fetch IP address
<a href="#">CSCwm13223</a>	IOS-XE 17 Crashes in IOSd Due to Malformed DMVPN-5-NHRP_RES_REPLY_IGNORE Syslog
<a href="#">CSCwk22942</a>	Unable to build two IPSec SAs w/same source/destination where one peer is PAT'd through the other
<a href="#">CSCwk79454</a>	Endpoint Tracker does not fail if default route is removed
<a href="#">CSCwh12093</a>	Enable SoS/ROC feature for DSL
<a href="#">CSCwm14665</a>	Enable BFD L2 messages in the Punt path for CAT8300/CAT8200/ISR4K/1K platform.
<a href="#">CSCwk37351</a>	IOS XE Router: Unexpected Reboot during PVDm OIR
<a href="#">CSCwh41497</a>	DDNS update retransmission timer fails to work with a traceback error
<a href="#">CSCwk27099</a>	Cellular connection is picking the wrong profile

Bug ID	Description
<a href="#">CSCwi87546</a>	ISR4k Unexpectedly reboot due to QFP CPP stuck at waiting for rw_lock - Lock id of 0 released
<a href="#">CSCwc86434</a>	Static NAT DIA inside static routes being advertised over OMP to remote sites
<a href="#">CSCwi72295</a>	Inconsistencies with openconfig-interfaces:config yang model in IOS-XE after defaulting interface
<a href="#">CSCwi16111</a>	ipv6 tcp adjust-mss not working after delete and reconfigure
<a href="#">CSCwi63042</a>	Packet drops observe between LISP EID over GRE Tunnel
<a href="#">CSCwi62098</a>	show crypto ipsec sa output displays incorrect replay status

### Resolved Bugs - Cisco IOS XE 17.9.5a

All resolved bugs for this release are available in the [Cisco Bug Search Tool](#).

Bug ID	Description
<a href="#">CSCwh73350</a>	Router keeps crashing when processing a firewall feature.
<a href="#">CSCwf67564</a>	Device observes memory leak at process "SSS Manager".
<a href="#">CSCwf23291</a>	"write" or "do write" saves configuration but RSA keys /SSH lost after reload.
<a href="#">CSCwc79115</a>	Policy commit failure notification and alarm.
<a href="#">CSCwh06834</a>	Using special characters in the password while generating TP generates an invalid TP.
<a href="#">CSCwh68508</a>	Unexpected reboot after establishing control plane of EVPN MPLS and receiving packets.
<a href="#">CSCvo01546</a>	NHRP reply processing may dequeue an unrelated request.
<a href="#">CSCwf82676</a>	CPU usage mismatch in <b>sh sdwan system status</b> vs <b>sh proc cpu platform</b> .
<a href="#">CSCwf03193</a>	Device crash with crashinfo files were generated with Segmentation fault, Process IPSEC key engine.
<a href="#">CSCwh08434</a>	OMP route is being advertised although the route is not available.
<a href="#">CSCwh40504</a>	SM-X interface stops passing traffic.
<a href="#">CSCwf24164</a>	Netflow stops working when flow monitor reaches cache limit.
<a href="#">CSCwh63061</a>	Device is showing 4 additional NR bands support - 1, 3, 7, and 28.
<a href="#">CSCwf65540</a>	Running >4 tests on ThousandEyes Agent causes tracebacks on device running TE in docker container.
<a href="#">CSCwi28227</a>	NAT HSL logging vrf-filter not working.
<a href="#">CSCwe14885</a>	VPN is established although the peer is using a revoked certificate for authentication.

Bug ID	Description
<a href="#">CSCwd17272</a>	UTD packet drop due to fragmentation for ER-SPAN traffic.
<a href="#">CSCwf55243</a>	Device is crashing while adding a trustpoint to the router.
<a href="#">CSCwh49644</a>	CSDL Compliance failure: Use of 3DES by IPSec is denied.
<a href="#">CSCwh32386</a>	Unexpected reload on device due to critical process fman_fp_image.
<a href="#">CSCwe30514</a>	Device reboots with sslproxy and utd enabled.
<a href="#">CSCwh30377</a>	Device data plane crash in Umbrella/OpenDNS processing due to incorrect UDP length.
<a href="#">CSCwf34171</a>	<b>configure replace</b> command fails due to the "license udi PID XXX SN:XXXX" line on IOS-XE devices.
<a href="#">CSCwf96980</a>	Unexpected reboot after configuring application redundancy.
<a href="#">CSCwe64779</a>	IOS XE router software forced reset during high IPC congestion with IPsec.
<a href="#">CSCwh20577</a>	Crashed by TRACK client thread at access invalid memory location.
<a href="#">CSCwh00963</a>	Unable to migrate from ADSL to VDSL without reboot.
<a href="#">CSCwh45121</a>	Support ECM disable for T38 for WxC integration.
<a href="#">CSCwh36801</a>	Crash in IP input process during tunnel encapsulation.
<a href="#">CSCwh96415</a>	Cannot disable DMVPN logging in IOS-XE 17.8 and higher.
<a href="#">CSCwe85301</a>	Crypto PKI-CRL-IO_0 process crash when PKI trustpoint is being deleted.
<a href="#">CSCwh20734</a>	Crypto PKI-CRL-IO_0 process crash when PKI trustpoint is requested & deleted.
<a href="#">CSCwf71557</a>	IPv4 connectivity over PPP not restored after reload.
<a href="#">CSCwc97579</a>	Spoke-spoke cache refresh not working correctly in case of multiple cache entries for same next hop.
<a href="#">CSCwfl1394</a>	IOS XE - debug log should mention port-hop and reason prior to DISTLOC.
<a href="#">CSCwf04866</a>	Keyman process crash seen while re-generating SSH key.
<a href="#">CSCwf55830</a>	No dial tone on analog phones due to DSP going into Power Denial State.
<a href="#">CSCwh00332</a>	B2B NAT: when configuration ip nat inside/outside on VASI interface, ack/seq number abnormal.
<a href="#">CSCwh60848</a>	CUBE - SIP TCP Message Queuing Fails to Resume Transmission.

### Open Bugs - Cisco IOS XE 17.9.5a

All open bugs for this release are available in the [Cisco Bug Search Tool](#).

Bug ID	Description
<a href="#">CSCwh18120</a>	IKEv2 - diagnose feature is taking 11% CPU during session bring up.
<a href="#">CSCwi25737</a>	Router should discard IKE Notification messages with incorrect DOI.
<a href="#">CSCwi01046</a>	PoE module is not providing enough power to bring the ports after an unexpected reload.
<a href="#">CSCwc30418</a>	Segmentation fault observed in ikev2_dupe_delete_reason.
<a href="#">CSCwi06843</a>	Endpoint tracker triggers a CPU hog.
<a href="#">CSCwi33168</a>	DSP reporting out of range utilization values in SNMP.
<a href="#">CSCwh80441</a>	Cosmetic 3G issue causing distress to customers - Modem is displayed as Unknown.
<a href="#">CSCwi53306</a>	Unknown appID in ZBFW HSL log.
<a href="#">CSCwi06404</a>	PKI crash after failing a CRL fetch.
<a href="#">CSCwi46997</a>	NAT Command not readable after reloaded.
<a href="#">CSCwh40073</a>	Interoperability issue between Cisco ISR and Juniper ACX/MX devices with a direct fiber connection.
<a href="#">CSCwi08171</a>	Router may crash due to Crypto IKMP process.
<a href="#">CSCwi53951</a>	Packets with Unicast MAC get dropped on a Port Channel L2 Sub-intf after a router reboot.
<a href="#">CSCwb25507</a>	CWMP: Add vendor-specific parameter for NBAR protocol pack version.
<a href="#">CSCwh12093</a>	Enable SoS/ROC feature for DSL.
<a href="#">CSCwh50510</a>	Router crash with segmentation fault(11), process = NHRP when processing NHRP traffic.
<a href="#">CSCwi10735</a>	ZBF drops transit WAAS PSH/ACK packet due to 'Invalid ACK number'.
<a href="#">CSCwh91136</a>	IOS XE: Traffic not encrypted and dropped over IPSEC SVTI tunnel.
<a href="#">CSCwe24491</a>	Static NAT with HSRP stops working after removing / adding standby.
<a href="#">CSCwh41497</a>	DDNS update retransmission timer fails to work with a traceback error.
<a href="#">CSCwi51326</a>	CPP CP SVR crash after decoding all packets to text (using l2 copy) on fia trace.
<a href="#">CSCwe70259</a>	Nightwatch interface flapping when configure 100M full with crossover cable.
<a href="#">CSCwi04547</a>	Custom application is marked as invalid.
<a href="#">CSCwi16111</a>	IPv6 TCP adjust-mss not working after delete and reconfigure.
<a href="#">CSCwi63042</a>	Packet drops observe between LISP EID over GRE tunnel.

**Resolved Bugs - Cisco IOS XE 17.9.4a**

All resolved bugs for this release are available in the [Cisco Bug Search Tool](#).

Bug ID	Description
<a href="#">CSCwh87343</a>	Cisco IOS XE Software Web UI Privilege Escalation Vulnerability. For more information, see Security Advisory: <a href="#">cisco-sa-iosxe-webui-privesc-j22SaA4z</a>

**Open Bugs - Cisco IOS XE 17.9.4a**

All open bugs for this release are available in the [Cisco Bug Search Tool](#).

Bug ID	Description
<a href="#">CSCwf53555</a>	Incorrect <b>Unknown Power Supply</b> displayed in <b>show inventory</b> .
<a href="#">CSCwe95072</a>	Unexpected reload due to memory corruption when modifying and access list.
<a href="#">CSCwf52751</a>	CLI template fails to attach with error <b>access-denied</b> .
<a href="#">CSCwf24164</a>	Netflow stops working when flow monitor reaches cache limit.
<a href="#">CSCwd61988</a>	Output packet bytes calculation biase when we enable QoS on port channel.
<a href="#">CSCwf41492</a>	NHRP BFD flaps randomly with dynamic tunnel (NHRP phase 3) in DMVPN.
<a href="#">CSCwe14885</a>	VPN is established although the peer is using a revoked certificate for authentication.
<a href="#">CSCwc86434</a>	Static NAT DIA inside static routes being advertised over OMP to remote sites.
<a href="#">CSCwd17272</a>	UTD packet drop due to fragmentation for ER-SPAN traffic.
<a href="#">CSCwf55243</a>	Device is crashing while adding a trustpoint to the router.
<a href="#">CSCwe85301</a>	Crypto PKI-CRL-IO_0 process crash when PKI trustpoint is being deleted.
<a href="#">CSCwf34171</a>	<b>configure replace</b> command fails due to the <b>license udi PID XXX SN:XXXX</b> line on IOS-XE devices.
<a href="#">CSCwf41450</a>	Device reloads changing the resource profile.
<a href="#">CSCvz82148</a>	%CRYPTO_SL_TP_LEVELS-6-VAR_NEW_VALUE message is observed in each write config with same crypto value.
<a href="#">CSCwf25735</a>	Device QoS more than four remark with set-cos not work.
<a href="#">CSCwf00276</a>	Packets with L2TP headers cause device to crash.
<a href="#">CSCwd39257</a>	IOS-XE CPP crash when entering <b>no ip nat create flow-entries</b> .
<a href="#">CSCwf03193</a>	Device crash with crashinfo files were generated with segmentation fault, process IPSEC key engine.
<a href="#">CSCwf60120</a>	Static NAT entry gets deleted from running configuration; but remains in startup configuration.



Bug ID	Description
<a href="#">CSCwf51206</a>	EVPN: BUM traffic is not flooded to bridge domain interface.
<a href="#">CSCwf11394</a>	IOS XE - debug log should mention port-hop and reason prior to DISTLOC.
<a href="#">CSCwf55830</a>	No dial tone on analog phones due to DSP going into Power Denial State.
<a href="#">CSCwe51910</a>	SNMP ifindex persist does not work.

### Resolved Bugs - Cisco IOS XE 17.9.4

All resolved bugs for this release are available in the [Cisco Bug Search Tool](#).

Bug ID	Description
<a href="#">CSCwf48808</a>	FlexVPN: Stale client routes stuck in RIB on FlexServer.
<a href="#">CSCwe93905</a>	NAT ALG is changing the Call-ID within SIP message header causing calls to fail.
<a href="#">CSCwf02225</a>	Device freezes for <b>show sdwan</b> commands.
<a href="#">CSCwe24210</a>	SNMP MIB does not show correct firmware version.
<a href="#">CSCwe09805</a>	OID for SNMP monitoring of DSP resources are not working as expected.
<a href="#">CSCwe89404</a>	No way audio when using secure hardware conference with secure endpoints.
<a href="#">CSCwe07055</a>	Device frequent reloads.
<a href="#">CSCwe25076</a>	ALG breaks NBAR recognition impacting application firewall performance.
<a href="#">CSCwd87195</a>	NAT configuration with redundancy, mapping ID and match-in-vrf options with no-alias support.
<a href="#">CSCwf08698</a>	Device crashes unexpectedly due to a fault in the 'TLSCLIENT_PROCESS'.
<a href="#">CSCwd34941</a>	NAT configuration with no-alias option is not preserved after reload.
<a href="#">CSCwf47796</a>	NHRP cache entries flood matching a /32 default route.
<a href="#">CSCwf09758</a>	Watchdog crash while importing a large CRL file into switch.
<a href="#">CSCwe41946</a>	DTMF is failing through IOS MTP during call on-hold.
<a href="#">CSCwe37123</a>	Device uses excessive memory when configuring ACLs with Large Object Groups.
<a href="#">CSCwe12194</a>	Auto-update cycle incorrectly deletes certificates.
<a href="#">CSCwd49309</a>	uCODE crash seen with traffic pointing to segfault in COFF handler.
<a href="#">CSCwe33793</a>	Memory allocation failure with extended antireplay enabled.
<a href="#">CSCwe66318</a>	NAT entries expire on standby router.
<a href="#">CSCwe31471</a>	Segmentation fault when per-tunnel QoS config withdraw.

Bug ID	Description
<a href="#">CSCwd59722</a>	Unexpected reboot due to IOSXE-WATCHDOG: Process = Crypto IKMP.
<a href="#">CSCwe70374</a>	Platform punt-policer is not configurable.
<a href="#">CSCwf37888</a>	Packet Duplication: Duplicate packets are counted on Primary Tunnel Interface Statistics.
<a href="#">CSCwe20008</a>	SNMP MIB OID changing its last index.
<a href="#">CSCwe60059</a>	Device crash when using dial-peer groups with STCAPP.
<a href="#">CSCwe18124</a>	MACsec remains marked as SECURED, but randomly the traffic stops working.
<a href="#">CSCwe18058</a>	Unexpected reload with IPS configured.
<a href="#">CSCwd73783</a>	Observed qfp-ucode-wlc crash.
<a href="#">CSCwe39011</a>	GARP on port up/up status from router is not received by remote peer device.
<a href="#">CSCwf39490</a>	MCID (Malicious Call Identification) gets broken due to custom prefix setting under STCAPP FAC.
<a href="#">CSCwe19084</a>	NAT: Traffic is not translated to the same global address though PAP is configured.
<a href="#">CSCwe69783</a>	Deice can lose its config during a triggered resync process if lines are in an off-hook state.
<a href="#">CSCwe37184</a>	Device seeing out of service on modules when using new DC power supply.
<a href="#">CSCwe41234</a>	Race condition causes no ringing for analog phones.
<a href="#">CSCwa96399</a>	Configuring <b>entity-information</b> xpath filter causes syslogs to print, does not return data.
<a href="#">CSCwc89823</a>	Router crashes due to CPUHOG when walking ciscoFlashMIB @snmp_platform_get_flash_file_info.
<a href="#">CSCwe32862</a>	Router IOS-XE crash while executing AES crypto functions.
<a href="#">CSCwf47563</a>	Device is crashing after importing the trustpoint with RSA key pair.
<a href="#">CSCwf32156</a>	ATTN-3-SYNC_TIMEOUT after upgrading.
<a href="#">CSCwd68994</a>	ISAKMP profile does not match as per configured certificate maps.
<a href="#">CSCwd35047</a>	Failed to ping gateway while configuring SharedLOM with console, TE1 interface, until router reload.
<a href="#">CSCwd49177</a>	ISG: L2-connected subscriber: IPv6 prefix delegation is not reachable when packet are switched.s

## Open Bugs - Cisco IOS XE 17.9.4

All open bugs for this release are available in the [Cisco Bug Search Tool](#).

Bug ID	Description
<a href="#">CSCwf53555</a>	Incorrect <b>Unknown Power Supply</b> displayed in <b>show inventory</b> .
<a href="#">CSCwe95072</a>	Unexpected reload due to memory corruption when modifying and access list.
<a href="#">CSCwf52751</a>	CLI template fails to attach with error <b>access-denied</b> .
<a href="#">CSCwf24164</a>	Netflow stops working when flow monitor reaches cache limit.
<a href="#">CSCwd61988</a>	Output packet bytes calculation bias when we enable QoS on port channel.
<a href="#">CSCwf41492</a>	NHRP BFD flaps randomly with dynamic tunnel (NHRP phase 3) in DMVPN.
<a href="#">CSCwe14885</a>	VPN is established although the peer is using a revoked certificate for authentication.
<a href="#">CSCwe86434</a>	Static NAT DIA inside static routes being advertised over OMP to remote sites.
<a href="#">CSCwd17272</a>	UTD packet drop due to fragmentation for ER-SPAN traffic.
<a href="#">CSCwf55243</a>	Device is crashing while adding a trustpoint to the router.
<a href="#">CSCwe85301</a>	Crypto PKI-CRL-IO_0 process crash when PKI trustpoint is being deleted.
<a href="#">CSCwf34171</a>	<b>configure replace</b> command fails due to the <b>license udi PID XXX SN:XXXX</b> line on IOS-XE devices.
<a href="#">CSCwf41450</a>	Device reloads changing the resource profile.
<a href="#">CSCvz82148</a>	%CRYPTO_SL_TP_LEVELS-6-VAR_NEW_VALUE message is observed in each write config with same crypto value.
<a href="#">CSCwf25735</a>	Device QoS more than four remark with set-cos not work.
<a href="#">CSCwf00276</a>	Packets with L2TP headers cause device to crash.
<a href="#">CSCwd39257</a>	IOS-XE CPP crash when entering <b>no ip nat create flow-entries</b> .
<a href="#">CSCwf03193</a>	Device crash with crashinfo files were generated with segmentation fault, process IPSEC key engine.
<a href="#">CSCwf60120</a>	Static NAT entry gets deleted from running configuration; but remains in startup configuration.
<a href="#">CSCwf51206</a>	EVPN: BUM traffic is not flooded to bridge domain interface.
<a href="#">CSCwf11394</a>	IOS XE - debug log should mention port-hop and reason prior to DISTLOC.
<a href="#">CSCwf55830</a>	No dial tone on analog phones due to DSP going into Power Denial State.
<a href="#">CSCwe51910</a>	SNMP ifindex persist does not work.
<a href="#">CSCwh60848</a>	CUBE - SIP Message Queuing Fails to Resume Transmission

## Resolved Bugs - Cisco IOS XE 17.9.3a

All resolved bugs for this release are available in the [Cisco Bug Search Tool](#).

Bug ID	Description
<a href="#">CSCwd45402</a>	MSR Unicast-To-Multicast not working if DST and SRC are the same in Service Reflect configuration.
<a href="#">CSCwd90168</a>	Unexpected reload after running <b>show voice dsp</b> command while an ISDN call disconnects.
<a href="#">CSCwd16559</a>	ISG FFR: ARP request to reroute nexthop IP is not triggered if ARP entry not in ARP table.
<a href="#">CSCwd79089</a>	Controller crash when sending full line rate of traffic with >5 Intel AX210 stations.
<a href="#">CSCwc27307</a>	Service Engine YANG support for ZBFW.
<a href="#">CSCwd16664</a>	GetVPN long SA - GM re-registration after encrypting 2^32-1 of packets in one IPsec SA.
<a href="#">CSCwd81357</a>	QoS classification not working for DSCP or ACL + MPLS EXP.
<a href="#">CSCwd89338</a>	Clear ISG existing lite-session upon reception of DHCP packet for same client.
<a href="#">CSCwc99823</a>	FMAN crash seen in SGACL@ fman_sgACL_alloc.
<a href="#">CSCwc78021</a>	Standby WLC crash @ fman_acl_remove_default_ace.
<a href="#">CSCwd25107</a>	Interface VLAN1 placed in shutdown state when configured with <b>ip address pool</b> .
<a href="#">CSCwd61255</a>	Data Plane crash on device when making Per-Tunnel QoS configuration changes with scale.
<a href="#">CSCwe01015</a>	IKEv2/IPSec - phase 2 rekey failing when peer is behind NAT.
<a href="#">CSCwd03869</a>	CEF DPI load-balancing causes out of order packets.
<a href="#">CSCwc65697</a>	Device crashing and restarting during call flow with new image.
<a href="#">CSCwd84599</a>	Dataplane memory utilization issue - 97% QFP DRAM memory utilization.
<a href="#">CSCwc88791</a>	DSL: erroneous atm interface counter at DSL retraining.
<a href="#">CSCwe03614</a>	CWMP : MAC address of ATM interface is not included in Inform message.
<a href="#">CSCwd38943</a>	GetVPN: KS reject registration from a public IP.
<a href="#">CSCwd06372</a>	Unconditional excessive logging in eogre tunnel error handling case.
<a href="#">CSCvy14316</a>	MPLS VPN traffic dropped due FDB OOM with cause FIAError under scale flow number (<1M).
<a href="#">CSCwd85580</a>	Device unexpected reload after <b>set ospfv3 authentication null</b> command.
<a href="#">CSCwd33202</a>	DHCP behavior issue when BDI interface is enabled on WAN and SVI interface.

Bug ID	Description
<a href="#">CSCwd06923</a>	Stale IP alias left after NAT statement got removed
<a href="#">CSCwd47123</a>	ISG uses identifier mac-address 0000.0000.0000 when DHCP LQ does not reply.
<a href="#">CSCwd72312</a>	GetVPN : Traffic drops seen on GM after rekey installing policies on image.
<a href="#">CSCwc14688</a>	Single WAN Interface subslot 0/0 timing.
<a href="#">CSCwd07516</a>	Memory leak under linux_iosd-imag related to SNMP.

### Open Bugs - Cisco IOS XE 17.9.3a

All open bugs for this release are available in the [Cisco Bug Search Tool](#).

Bug ID	Description
<a href="#">CSCwd39257</a>	IOS-XE CPP crash when entering <b>no ip nat create flow-entries</b> .
<a href="#">CSCwd63783</a>	Memory leak caused router reload.
<a href="#">CSCwd97077</a>	Device leaking memory in MallocLite because of telemetry subscription to collect FNF cache.
<a href="#">CSCwe09805</a>	OID for SNMP monitoring of DSP resources are not working as expected.
<a href="#">CSCwe25076</a>	ALG breaks NBAR recognition impacting application firewall performance.
<a href="#">CSCwe14885</a>	VPN is established although the peer is using a revoked certificate for authentication.
<a href="#">CSCwe24491</a>	Static NAT with HSRP stops working after removing / adding standby.
<a href="#">CSCwd17272</a>	UTD Packet drop due to fragmentation for ER-SPAN traffic.
<a href="#">CSCwe32862</a>	Router IOS-XE crash while executing AES crypto functions.
<a href="#">CSCwe19084</a>	NAT: Traffic is not translated to the same global address though PAP is configured.
<a href="#">CSCwe07055</a>	Device frequent reloads.
<a href="#">CSCwe28468</a>	Device always fails to push any template to device if device is running in FIPS mode.
<a href="#">CSCwe12652</a>	Incorrect return MIB for ciscoWanCellExtMIB and ciscoWan3gMIB.
<a href="#">CSCwd68994</a>	Unable to match on customer profile based on certificate-map.
<a href="#">CSCwe06327</a>	PFP policy in SRTE, RIB resolution in FC bring down IPSec tunnel interface- stuck at linestate down.
<a href="#">CSCwe38732</a>	IP CEF load sharing command is being changed by the device.
<a href="#">CSCwd34941</a>	NAT configuration with no-alias option is not preserved after reload.
<a href="#">CSCwe37184</a>	Device seeing out of service on Switch modules with new DC power supply.

Bug ID	Description
<a href="#">CSCwh60848</a>	CUBE - SIP Message Queuing Fails to Resume Transmission

### Resolved Bugs - Cisco IOS XE 17.9.2a

All resolved bugs for this release are available in the [Cisco Bug Search Tool](#).

Bug ID	Description
<a href="#">CSCwc21739</a>	NAT not requesting further for low ports after initial allocation when CLI knob <b>reserved-ports</b> set.
<a href="#">CSCwc39012</a>	Crash saving tracelogs after "Too many open files" error.
<a href="#">CSCwc77663</a>	Device frequent reloads due to stuck thread in CPP.
<a href="#">CSCwc03478</a>	VTCP does not support L2 correctly.
<a href="#">CSCwc72923</a>	ERROR info: Router configuration failed:interface Serial0/1/0:23 isdn switch-type primary-ntt.
<a href="#">CSCwd12591</a>	ucode crash during FW Classification, Session Frees.
<a href="#">CSCwc99668</a>	Routes added by IKEv2 getting deleted at responder.
<a href="#">CSCwc23077</a>	Firewall drop seen stating "FirewallL4" seen on device.
<a href="#">CSCwc78528</a>	DSPware 60.1.1 release targeting v179_throttle.
<a href="#">CSCwc44851</a>	Bootstrap failing on device.
<a href="#">CSCwc96444</a>	Router is not programming correct next-hop for unicast prefix with multicast config present.
<a href="#">CSCwc49715</a>	Crash @ UNIX-EXT-SIGNAL: Aborted(6), Process = Check heaps, having PPPoe with CWMP configs.
<a href="#">CSCwd06118</a>	IKEv2 Cert-based IPsec not working between IOS-XE and AWS.
<a href="#">CSCwb52324</a>	Device unexpected reload due to QFP ucode crash.
<a href="#">CSCwc77183</a>	Packet duplication is causing drops in payment transactions with SdwanGenericDrop code.
<a href="#">CSCwc20170</a>	Device reloads unexpectedly due to critical FTMD fault when VRF configuration is pushed.
<a href="#">CSCwb89958</a>	Unified Policy HSL not sending properly NBAR application information.
<a href="#">CSCwc89328</a>	Device might reboot when supporting explicit IV joins network.
<a href="#">CSCwc52538</a>	Flows are not distributed and load-balanced evenly and consistently.
<a href="#">CSCwc45950</a>	ZBFW self zone policy drops SSH session on Mgmt-intf 512 ports.

Bug ID	Description
<a href="#">CSCwc43794</a>	VRF+NAT Outside Source Static - Drop packets during FTP (Active-mode) execution.
<a href="#">CSCwc79145</a>	Throughput degrades when Local TLOC specified in Data Policy goes down.
<a href="#">CSCwc32595</a>	BFD sessions remains down if interface flap form up/down/up.
<a href="#">CSCwb65396</a>	CLI template push fails with error: 'Error: on line 48: line-mode single-wire line 0'.
<a href="#">CSCwb90252</a>	Automatically freeing up filesystems stale image or recovered folder (lost+found).
<a href="#">CSCwc82140</a>	QFP crash when ZBFW configuration features "log dropped-packets" configuration.
<a href="#">CSCvz89354</a>	Router crashes due to CPUHOG when walking ciscoFlashMIB.
<a href="#">CSCwc39865</a>	Subscriber Session getting stuck and needs clearing it manually.
<a href="#">CSCwb48953</a>	Speed test failing with "Device Error: Speed test in progress".
<a href="#">CSCwd11365</a>	Needs cert update - Azure CGW creation fails due to NVA provisioning failure.
<a href="#">CSCwc56033</a>	Not triggering any alarms when RPM of a fan is 0.
<a href="#">CSCwc84967</a>	Intermittent double DTMF due to changing timestamp on a DTMF event.
<a href="#">CSCwb08057</a>	ISG: Number of lite sessions conversion in progress counter not decrementing on failed account-logon.
<a href="#">CSCwc29629</a>	Crashes when Virtual-Access tries to bring-up/bring-down OSPFv3 ipsec crypto session authentication.
<a href="#">CSCwd13352</a>	SSH getting closed after update.
<a href="#">CSCwc77177</a>	BFD and control packets are dropped when ACL is applied on gigi to which loopback is bind.
<a href="#">CSCwc68132</a>	SIG tunnel tracker packets are dropped by firewall with self zone policy.
<a href="#">CSCwd56336</a>	BFD sessions are not coming up after flapping the interface due to low FTM rate.
<a href="#">CSCwd56015</a>	UTD skipped when interface UTD config is used to enable/disable UTD.

### Open Bugs - Cisco IOS XE 17.9.2a

All open bugs for this release are available in the [Cisco Bug Search Tool](#).

Bug ID	Description
<a href="#">CSCwd45508</a>	Device does not form BFD across Serial link when upgrading.
<a href="#">CSCwd23810</a>	IOS-XE: High CPU utilization caused by NHRP.
<a href="#">CSCwd13050</a>	After upgrade, device moved into Out of Sync status.

Bug ID	Description
<a href="#">CSCwd12955</a>	NAT translation is not correctly sent to hub router from branch when SSNAT and UTD are configured.
<a href="#">CSCwc28468</a>	Device always fails to push any template if it is running in FIPS mode.
<a href="#">CSCwb74821</a>	yang-management process confd is not running, controller mode.
<a href="#">CSCwd36621</a>	CERM may kick in due to IPsec sessions initiated for on-demand tunnels.
<a href="#">CSCwd17579</a>	Router crashing with reason CPU Usage due to Memory Pressure exceeds threshold (Reboot).
<a href="#">CSCwd34941</a>	NAT configuration with no-alias option is not preserved after reload.
<a href="#">CSCwd33966</a>	Unable to configure the local BGP as-path-list.
<a href="#">CSCwd37410</a>	0365 and MS Teams applications access issues when using DIA with app-list match in data-policy.
<a href="#">CSCwd38626</a>	Repeating SYS-2-PAK_SUBBLOCK_BADSIZE: 4 -Process= "&lt;interrupt level&gt;".
<a href="#">CSCwc37465</a>	Unable to push no-alias option on static NAT mapping from management system.
<a href="#">CSCwd44006</a>	Control connection on device doesn't come-up with reverse proxy using Enterprise Certificate.
<a href="#">CSCwd29334</a>	Upgrade failures due to inability to establish netconf connection.
<a href="#">CSCwc88791</a>	DSL: erroneous atm interface counter at DSL retraining.
<a href="#">CSCwa96399</a>	Configuring entity-information xpath filter causes syslogs to print, does not return data.
<a href="#">CSCwd44586</a>	Login banner config is changed after upgrade.
<a href="#">CSCwd12330</a>	Invalid TCP checksum in SYN flag packets passing through Router.
<a href="#">CSCwc76082</a>	check_sig_ipsec_ike_sessions fails with could not find entry for Tunnel100001.
<a href="#">CSCwa14636</a>	Device stopped forwarding traffic. Suspect OMPd is busy.
<a href="#">CSCwd15560</a>	With 2 sequences, should not skip if the match is different and action is same.
<a href="#">CSCwd33202</a>	DHCP behavior issue when BDI interface is enabled on WAN and SVI interface.
<a href="#">CSCwd17381</a>	NAT/DIA traffic is skipping UTD in forward direction after SSNAT path from service-side.
<a href="#">CSCwd18028</a>	After delete CSP, New CCM bringup on existing CSP is stuck in Initializing CCM on MT cluster.
<a href="#">CSCwc70511</a>	Router reloads unexpectedly during NHRP processing.



**Resolved Bugs - Cisco IOS XE 17.9.1a**

All resolved bugs for this release are available in the [Cisco Bug Search Tool](#).

Bug ID	Description
<a href="#">CSCvz65764</a>	Peer MSS value showing incorrect.
<a href="#">CSCwa95092</a>	When Object-group used in a ACL is updated, it takes no effect.
<a href="#">CSCwb33968</a>	Failed to display active flows when flow count is high on the device.
<a href="#">CSCwb02142</a>	Traceback: fman_fp_image core after clearing packet-trace conditions.
<a href="#">CSCwb49857</a>	Memory leaks on keyman process when key is not found.
<a href="#">CSCwa65728</a>	Large number of DH failures.
<a href="#">CSCwb11389</a>	NAT translation stops suddenly(ip nat inside doesn't work).
<a href="#">CSCwa84919</a>	Revocation-check crl none does not failover to NONE DNAC-CA.
<a href="#">CSCwb39098</a>	Router crashed after new IPv6 address assigned when router use specific configuration.
<a href="#">CSCwa69101</a>	Initiator unclassified ip-address LQipv4 command has no effect.
<a href="#">CSCwa67886</a>	UDP based DNS resolution doesn't work with IS-IS EMCP on IOS-XE.
<a href="#">CSCvz84588</a>	Destination prefix packets getting dropped because forwarding plane is not programming the next hop.
<a href="#">CSCwb27486</a>	New Key for NBAR app and NBAR category without OGREF optimized.
<a href="#">CSCwa72273</a>	ZBFW dropping return packets from tunnel post upgrade.
<a href="#">CSCwa49101</a>	OMP origin protocol comparison cleanup.
<a href="#">CSCwb17282</a>	Router crashing when clearing a VPDN session.
<a href="#">CSCwa49721</a>	Hub with firewall configured incorrectly dropping return packets when routing between VRFs.
<a href="#">CSCwb38501</a>	Support IGMP on voice vlan.
<a href="#">CSCwb21645</a>	NAT traffic gets dropped when default route changes from OMP to NAT DIA route.
<a href="#">CSCwb12647</a>	Device crash for stuck threads in cpp on packet processing.
<a href="#">CSCwb18223</a>	SNMP v2 community name encryption problem.
<a href="#">CSCwb16723</a>	Traceroute not working with NAT.
<a href="#">CSCwb31587</a>	Subject-alt-name attribute in certificate trustpoint causes Windows NDES/CA to reject SCEP requests.
<a href="#">CSCwb51238</a>	Router reload unexpectedly two times when enter netflow show command.

Bug ID	Description
<a href="#">CSCwa98617</a>	Memory Leak in AEM chunks related to Firewall.
<a href="#">CSCwa48512</a>	CoR intercepted DNS reply packets dropped with drop code 52 (FirewallL4Insp) if UTD enabled also.
<a href="#">CSCwa93664</a>	ThousandEyes container may fail to get installed on device.
<a href="#">CSCvz28950</a>	DMVPN phase 2 connectivity issue between two spokes.
<a href="#">CSCwa78348</a>	Traceback: IOS-XE reload after Segmentation fault on Process = SSS Manager.
<a href="#">CSCvz81664</a>	Enabling or disabling OMP overlay AS prevents connected routes from being advertised in OMP.
<a href="#">CSCwa67029</a>	ROMMON version not displaying correctly
<a href="#">CSCwb43423</a>	IOS-XE image installation fails.
<a href="#">CSCwa08847</a>	ZBFW policy stops working after modifying the zone pair.
<a href="#">CSCwb15331</a>	Keyman memory leak using public keys.
<a href="#">CSCvw50622</a>	NHRP network resolution not working with link-local ipv6 address.
<a href="#">CSCwb59736</a>	CSR BFD tunnel are zero.
<a href="#">CSCwa57873</a>	Incorrect reload reason - Last reload reason: LocalSoft for Netconf Initiated request.
<a href="#">CSCwb51595</a>	Missing IOS config (voice translation rule) on upgrade.
<a href="#">CSCwb18315</a>	Umbrella DNS security policy doesn't work with Cloud onRamp with SIG tunnels.

### Open Bugs - Cisco IOS XE 17.9.1a

All open bugs for this release are available in the [Cisco Bug Search Tool](#).

Bug ID	Description
<a href="#">CSCwc39012</a>	Crash saving tracelogs after Too many open files error.
<a href="#">CSCwc56896</a>	Crash in ipv6_tunnel_macaddr while adding/removing gre multi-point tunnel mode.
<a href="#">CSCwb89958</a>	Unified Policy HSL not sending properly NBAR application information.
<a href="#">CSCwc23077</a>	Firewall drop seen stating FirewallL4.
<a href="#">CSCwb74821</a>	yang-management process confd is not running, controller mode.
<a href="#">CSCwc37465</a>	Static NAT configuration in CLI with the no-alias keyword cannot be retrieved via NETCONF/YANG.
<a href="#">CSCwc44851</a>	Bootstrap failing on device.
<a href="#">CSCwc55684</a>	Layer 7 health check doesn't work on loopback interfaces.

Bug ID	Description
<a href="#">CSCwc49715</a>	Crash @ UNIX-EXT-SIGNAL: Aborted(6), Process = Check heaps, having PPPoe with cwmp configs.
<a href="#">CSCwc52538</a>	Traffic flows are not distributed and load-balanced evenly and consistently.
<a href="#">CSCwc55260</a>	Memory leak due to FTMD process.
<a href="#">CSCwc69881</a>	Device lost configuration due to multiple power cycles on site.
<a href="#">CSCwc20170</a>	Device reloads unexpectedly due to critical FTMD fault when VRF configuration is pushed.
<a href="#">CSCwb88621</a>	Device unable to establish control connection with vBond due to out of order DTLS packets.
<a href="#">CSCwc59598</a>	Statistics collection causing service-side BFD to flap on every collection interval.
<a href="#">CSCwc50477</a>	Device crashed in ipv4_nat_create_out2in_session_entry.
<a href="#">CSCwc67465</a>	Router cannot be upgraded.
<a href="#">CSCwc32595</a>	BFD sessions remains down if interface flap form up/down/up.
<a href="#">CSCwc38529</a>	Traffic seems not inspected by UTD when umbrella is set.
<a href="#">CSCwc63563</a>	Unable to set specific speed and duplex values on SFP ports on IOS-XE routing platforms.
<a href="#">CSCwc39865</a>	Subscriber Session getting stuck and needs clearing manually.
<a href="#">CSCwc43973</a>	DLC is not completing after upgrading to Smart licensing from CSL.
<a href="#">CSCwc53885</a>	IOS-XE no ip nat config is allowed to be committed and removes nat routes among other nat config.
<a href="#">CSCwc55467</a>	BFD Tunnel on router is not staying up, 1 out of 40 tunnels.
<a href="#">CSCwc56033</a>	Not triggering any alarms when RPM of a fan is 0.
<a href="#">CSCwc42978</a>	Device loses all BFD sessions with Invalid SPI.
<a href="#">CSCwc67171</a>	Tracebacks at cgm_avlmgm_class_init and cpuhog_key_init.
<a href="#">CSCwb08057</a>	Number of lite sessions conversion in progress counter not decrementing on failed account-logon.
<a href="#">CSCwc63337</a>	Destination not reachable if configured as a next for a static route resolvable via non /32 OMP.
<a href="#">CSCwc19533</a>	CRC errors seen after upgrade on device.
<a href="#">CSCwc29629</a>	Crashes when Virtual-Access tries to bring-up/bring-down OSPFv3 ipsec crypto session authentication.

Bug ID	Description
<a href="#">CSCwc27208</a>	BFD sessions not coming UP because of ANTI-REPLAY-FAILURES.
<a href="#">CSCwc68132</a>	SIG tunnel tracker packets are dropped by firewall with self zone policy.
<a href="#">CSCwc70468</a>	CPA fail to send SIP Update for AsmT before maxTermToneAnalysis expiration.
<a href="#">CSCwc70511</a>	Router reloaded unexpectedly.
<a href="#">CSCwc65697</a>	Router crashes with CUBE WebSocket forking flows.

## Related Documentation

- [Release Notes for Previous Versions of Cisco 4000 Series ISRs](#)
- [Hardware Installation Guide for Cisco 4000 Series Integrated Services Routers](#)
- [Configuration Guides for Cisco 4000 Series ISRs](#)
- [Command Reference Guides for Cisco 4000 Series ISRs](#)
- [Product Landing Page for Cisco 4000 Series ISRs](#)
- [Datasheet for Cisco 4000 Series ISRs](#)
- [End-of-Sale and End-of-Life Announcement](#)
- [Upgrading Field-Programmable Hardware Devices for Cisco 4000 Series ISRs](#)
- [Field Notices](#)
- [Cisco Bulletins](#)

## 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 DevNet](#).
- 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.

## Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

## Troubleshooting

For the most up-to-date, detailed troubleshooting information, see the Cisco TAC website at <https://www.cisco.com/en/US/support/index.html>.

Go to **Products by Category** and choose your product from the list, or enter the name of your product. Look under **Troubleshoot and Alerts** to find information for the issue that you are experiencing.

