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

First Published: 2022-08-26

Last Modified: 2024-02-28

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.

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	isr_4400v2_cpld_update_v2.0.SPA.bin isr4400v2-hw-programmable.04.01.00.SPA.pkg
Cisco 4451-X ISR	16.12(2r)	19042950	isr4400_cpld_update_v2.0.SPA.bin
Cisco 4431 ISR	16.12(2r)	19042950	isr4400_cpld_update_v2.0.SPA.bin
Cisco 4351 ISR	16.12(2r)	19040541	isr4300_cpld_update_v2.0.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_v2.0.SPA.bin
Cisco 4321 ISR	16.12(2r)	19040541	isr4300_cpld_update_v2.0.SPA.bin
Cisco 4221 ISR	16.12(2r)	19042420	isr4200_cpld_update_v2.0.SPA.bin

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://cfnng.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 17.9.4a

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
IPsec Dual Stack Support on Non-Cisco Devices	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.
Support for BGP additional paths with label-unicast unique mode	This enhancement introduces support for configuring BGP additional paths when label-unicast unique mode is configured.
Support for Unicast-to-Multicast Destination Reflection	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.
Cisco Unified Border Element (CUBE) Features	
End-to-end Secure Calling for Courtesy Call Back and Unified Contact Center Survivability	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.
Load Balancing for DNS SRV Host	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.

Feature	Description
Options Ping for DNS SRV Hosts	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.
Transfer of Call Detail Records Using SFTP	Cisco IOS gateways can use FTP and now SFTP servers to transfer call accounting files.
Webex Calling Branch Survivability	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. **Note** 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.
Programmability Features	
Pubd Restartability	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.
Smart Licensing Using Policy Features	

Feature	Description
Hostname support	Support for sending hostname information was introduced. If you configure a hostname on the product instance and disable the corresponding privacy setting (**no license smart privacy hostname** command in global configuration mode), hostname information is sent from the product instance, in a separate sync message or offline file. 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. For more information, see license smart (global config) 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).
Inconsistent system behavior for **license boot** global configuration command rectified	The system does not allow overlapping suite and technology package configuration to co-exist. For more information, see license boot.
New mechanism to send data privacy related information	A new mechanism to send data privacy related information was introduced. This information is no longer included in a RUM report. If data privacy is disabled (**no license smart privacy** {**all**|**hostname**|**version**} command in global configuration mode), data privacy related information is sent in a separate sync message or offline file. 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. For more information, see license smart (global config).

Feature	Description
RUM Report Throttling	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. The affected topologies are: *Connected Directly to CSSM*, *Connected to CSSM Through CSLU* (product instance-initiated communication), *CSLU Disconnected from CSSM* (product instance-initiated communication), and *SSM On-Prem Deployment* (product instance-initiated communication). 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. You can override the reporting frequency throttling, by entering the **license smart sync** 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. 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 *all* subsequent releases.
Virtual Routing and Forwarding (VRF) Support	On a product instance where VRF is supported, you can configure the **license smart vrf** *vrf_string* command and use a VRF to send licensing data to CSSM, or CSLU, or SSM On-Prem. **Note** When using a VRF, the supported transport types are **smart** and **cslu** only.) For more information, see license smart (global config).

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 17.9.5a

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

Bug ID	Description
CSCwh73350	Router keeps crashing when processing a firewall feature.
CSCwf67564	Device observes memory leak at process "SSS Manager".
CSCwf23291	"write" or "do write" saves configuration but RSA keys /SSH lost after reload.
CSCwc79115	Policy commit failure notification and alarm.
CSCwh06834	Using special characters in the password while generating TP generates an invalid TP.

Bug ID	Description
CSCwh68508	Unexpected reboot after establishing control plane of EVPN MPLS and receiving packets.
CSCvo01546	NHRP reply processing may dequeue an unrelated request.
CSCwf82676	CPU usage mismatch in **sh sdwan system status** vs **sh proc cpu platform**.
CSCwf03193	Device crash with crashinfo files were generated with Segmentation fault, Process IPSEC key engine.
CSCwh08434	OMP route is being advertised although the route is not available.
CSCwh40504	SM-X interface stops passing traffic.
CSCwf24164	Netflow stops working when flow monitor reaches cache limit.
CSCwh63061	Device is showing 4 additional NR bands support - 1, 3, 7, and 28.
CSCwf65540	Running >4 tests on ThousandEyes Agent causes tracebacks on device running TE in docker container.
CSCwi28227	NAT HSL logging vrf-filter not working.
CSCwe14885	VPN is established although the peer is using a revoked certificate for authentication.
CSCwd17272	UTD packet drop due to fragmentation for ER-SPAN traffic.
CSCwf55243	Device is crashing while adding a trustpoint to the router.
CSCwh49644	CSDL Compliance failure: Use of 3DES by IPSec is denied.
CSCwh32386	Unexpected reload on device due to critical process fman_fp_image.
CSCwe30514	Device reboots with sslproxy and utd enabled.
CSCwh30377	Device data plane crash in Umbrella/OpenDNS processing due to incorrect UDP length.
CSCwf34171	**configure replace** command fails due to the "license udi PID XXX SN:XXXX" line on IOS-XE devices.
CSCwf96980	Unexpected reboot after configuring application redundancy.
CSCwe64779	IOS XE router software forced reset during high IPC congestion with IPsec.
CSCwh20577	Crashed by TRACK client thread at access invalid memory location.
CSCwh00963	Unable to migrate from ADSL to VDSL without reboot.
CSCwh45121	Support ECM disable for T38 for WxC integration.
CSCwh36801	Crash in IP input process during tunnel encapsulation.
CSCwh96415	Cannot disable DMVPN logging in IOS-XE 17.8 and higher.

Bug ID	Description
CSCwe85301	Crypto PKI-CRL-IO_0 process crash when PKI trustpoint is being deleted.
CSCwh20734	Crypto PKI-CRL-IO_0 process crash when PKI trustpoint is requested & deleted.
CSCwf71557	IPv4 connectivity over PPP not restored after reload.
CSCwc97579	Spoke-spoke cache refresh not working correctly in case of multiple cache entries for same next hop.
CSCwf11394	IOS XE - debug log should mention port-hop and reason prior to DISTLOC.
CSCwf04866	Keyman process crash seen while re-generating SSH key.
CSCwf55830	No dial tone on analog phones due to DSP going into Power Denial State.
CSCwh00332	B2B NAT: when configration ip nat inside/outside on VASI intereface, ack/seq number abnormal.

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
CSCwh18120	IKEv2 - diagnose feature is taking 11% CPU during session bring up.
CSCwi25737	Router should discard IKE Notification messages with incorrect DOI.
CSCwi01046	PoE module is not providing enough power to bring the ports after an unexpected reload.
CSCwc30418	Segmentation fault observed in ikev2_dupe_delete_reason.
CSCwi06843	Endpoint tracker triggers a CPU hog.
CSCwi33168	DSP reporting out of range utilization values in SNMP.
CSCwh80441	Cosmetic 3G issue causeing distress to customers - Modem is displayed as Unknown.
CSCwi53306	Unknown appID in ZBFW HSL log.
CSCwi06404	PKI crash after failing a CRL fetch.
CSCwi46997	NAT Command not readable after reloaded.
CSCwh40073	Interoperability issue between Cisco ISR and Juniper ACX/MX devices with a direct fiber connection.
CSCwi08171	Router may crash due to Crypto IKMP process.
CSCwi53951	Packets with Unicast MAC get dropped on a Port Channel L2 Sub-intf after a router reboot.
CSCwb25507	CWMP: Add vendor-pecific parameter for NBAR protocol pack version.

Bug ID	Description
CSCwh12093	Enable SoS/ROC feature for DSL.
CSCwh50510	Router crash with segmentation fault(11), process = NHRP when processing NHRP traffic.
CSCwi10735	ZBF drops transit WAAS PSH/ACK packet due to 'Invalid ACK number'.
CSCwh91136	IOS XE: Traffic not encrypted and droped over IPSEC SVTI tunnel.
CSCwe24491	Static NAT with HSRP stops working after removing / adding standby.
CSCwh41497	DDNS update retransmission timer fails to work with a traceback error.
CSCwi51326	CPP CP SVR crash after decoding all packets to text (using l2 copy) on fia trace.
CSCwe70259	Nightwatch interface flapping when configure 100M full with crossover cable.
CSCwi04547	Custom application is marked as invalid.
CSCwi16111	IPv6 TCP adjust-mss not working after delete and reconfigure.
CSCwi63042	Packet drops observe between LISP EID over GRE tunnel.
CSCwi30529	AAA:Template push fail when aaa authorization is set to local.

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
CSCwh87343	Cisco IOS XE Software Web UI Privilege Escalation Vulnerability. For more information, see Security Advisory: cisco-sa-iosxe-webui-privesc-j22SaA4z

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
CSCwf53555	Incorrect **Unknown Power Supply** displayed in **show inventory**.
CSCwe95072	Unexpected reload due to memory corruption when modifying and access list.
CSCwf52751	CLI template fails to attach with error **access-denied**.
CSCwf24164	Netflow stops working when flow monitor reaches cache limit.
CSCwd61988	Output packet bytes calculation biase when we enable QoS on port channel.
CSCwf41492	NHRP BFD flaps randomly with dynamic tunnel (NHRP phase 3) in DMVPN.
CSCwe14885	VPN is established although the peer is using a revoked certificate for authentication.

Bug ID	Description
CSCwc86434	Static NAT DIA inside static routes being advertised over OMP to remote sites.
CSCwd17272	UTD packet drop due to fragmentation for ER-SPAN traffic.
CSCwf55243	Device is crashing while adding a trustpoint to the router.
CSCwe85301	Crypto PKI-CRL-IO_0 process crash when PKI trustpoint is being deleted.
CSCwf34171	**configure replace** command fails due to the **license udi PID XXX SN:XXXX** line on IOS-XE devices.
CSCwf41450	Device reloads changing the resource profile.
CSCvz82148	%CRYPTO_SL_TP_LEVELS-6-VAR_NEW_VALUE message is observed in each write config with same crypto value.
CSCwf25735	Device QoS more than four remark with set-cos not work.
CSCwf00276	Packets with L2TP headers cause device to crash.
CSCwd39257	IOS-XE CPP crash when entering **no ip nat create flow-entries**.
CSCwf03193	Device crash with crashinfo files were generated with segmentation fault, process IPSEC key engine.
CSCwf60120	Static NAT entry gets deleted from running configuration; but remains in startup configuration.
CSCwf51206	EVPN: BUM traffic is not flooded to bridge domain interface.
CSCwf11394	IOS XE - debug log should mention port-hop and reason prior to DISTLOC.
CSCwf55830	No dial tone on analog phones due to DSP going into Power Denial State.
CSCwe51910	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
CSCwf48808	FlexVPN: Stale client routes stuck in RIB on FlexServer.
CSCwe93905	NAT ALG is changing the Call-ID within SIP message header causing calls to fail.
CSCwf02225	Device freezes for **show sdwan** commands.
CSCwe24210	SNMP MIB does not show correct firmware version.
CSCwe09805	OID for SNMP monitoring of DSP resources are not working as expected.
CSCwe89404	No way audio when using secure hardware conference with secure endpoints.

Bug ID	Description
CSCwe07055	Device frequent reloads.
CSCwe25076	ALG breaks NBAR recognition impacting application firewall performance.
CSCwd87195	NAT configuration with redundancy, mapping ID and match-in-vrf options with no-alias support.
CSCwf08698	Device crashes unexpectedly due to a fault in the 'TLSCLIENT_PROCESS'.
CSCwd34941	NAT configuration with no-alias option is not preserved after reload.
CSCwf47796	NHRP cache entries flood matching a /32 default route.
CSCwf09758	Watchdog crash while importing a large CRL file into switch.
CSCwe41946	DTMF is failing through IOS MTP during call on-hold.
CSCwe37123	Device uses excessive memory when configuring ACLs with Large Object Groups.
CSCwe12194	Auto-update cycle incorrectly deletes certificates.
CSCwd49309	uCODE crash seen with traffic pointing to segfault in COFF handler.
CSCwe33793	Memory allocation failure with extended antireplay enabled.
CSCwe66318	NAT entries expire on standby router.
CSCwe31471	Segmentation fault when per-tunnel QoS config withdraw.
CSCwd59722	Unexpected reboot due to IOSXE-WATCHDOG: Process = Crypto IKMP.
CSCwe70374	Platform punt-policer is not configurable.
CSCwf37888	Packet Duplication: Duplicate packets are counted on Primary Tunnel Interface Statistics.
CSCwe20008	SNMP MIB OID changing its last index.
CSCwe60059	Device crash when using dial-peer groups with STCAPP.
CSCwe18124	MACsec remains marked as SECURED, but randomly the traffic stops working.
CSCwe18058	Unexpected reload with IPS configured.
CSCwd73783	Observed qfp-ucode-wlc crash.
CSCwe39011	GARP on port up/up status from router is not received by remote peer device.
CSCwf39490	MCID (Malicious Call Identification) gets broken due to custom prefix setting under STCAPP FAC.
CSCwe19084	NAT: Traffic is not translated to the same global address though PAP is configured.

Bug ID	Description
CSCwe69783	Deice can lose its config during a triggered resync process if lines are in an off-hook state.
CSCwe37184	Device seeing out of service on modules when using new DC power supply.
CSCwe41234	Race condition causes no ringing for analog phones.
CSCwa96399	Configuring **entity-information** xpath filter causes syslogs to print, does not return data.
CSCwc89823	Router crashes due to CPUHOG when walking ciscoFlashMIB @snmp_platform_get_flash_file_info.
CSCwe32862	Router IOS-XE crash while executing AES crypto functions.
CSCwf47563	Device is crashing after importing the trustpoint with RSA key pair.
CSCwf32156	ATTN-3-SYNC_TIMEOUT after upgrading.
CSCwd68994	ISAKMP profile does not match as per configured certificate maps.
CSCwd35047	Failed to ping gateway while configuring SharedLOM with console, TE1 interface, until router reload.
CSCwd49177	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
CSCwf53555	Incorrect **Unknown Power Supply** displayed in **show inventory**.
CSCwe95072	Unexpected reload due to memory corruption when modifying and access list.
CSCwf52751	CLI template fails to attach with error **access-denied**.
CSCwf24164	Netflow stops working when flow monitor reaches cache limit.
CSCwd61988	Output packet bytes calculation biase when we enable QoS on port channel.
CSCwf41492	NHRP BFD flaps randomly with dynamic tunnel (NHRP phase 3) in DMVPN.
CSCwe14885	VPN is established although the peer is using a revoked certificate for authentication.
CSCwc86434	Static NAT DIA inside static routes being advertised over OMP to remote sites.
CSCwd17272	UTD packet drop due to fragmentation for ER-SPAN traffic.
CSCwf55243	Device is crashing while adding a trustpoint to the router.
CSCwe85301	Crypto PKI-CRL-IO_0 process crash when PKI trustpoint is being deleted.

Bug ID	Description
CSCwf34171	**configure replace** command fails due to the **license udi PID XXX SN:XXXX** line on IOS-XE devices.
CSCwf41450	Device reloads changing the resource profile.
CSCvz82148	%CRYPTO_SL_TP_LEVELS-6-VAR_NEW_VALUE message is observed in each write config with same crypto value.
CSCwf25735	Device QoS more than four remark with set-cos not work.
CSCwf00276	Packets with L2TP headers cause device to crash.
CSCwd39257	IOS-XE CPP crash when entering **no ip nat create flow-entries**.
CSCwf03193	Device crash with crashinfo files were generated with segmentation fault, process IPSEC key engine.
CSCwf60120	Static NAT entry gets deleted from running configuration; but remains in startup configuration.
CSCwf51206	EVPN: BUM traffic is not flooded to bridge domain interface.
CSCwf11394	IOS XE - debug log should mention port-hop and reason prior to DISTLOC.
CSCwf55830	No dial tone on analog phones due to DSP going into Power Denial State.
CSCwe51910	SNMP ifindex persist does not work.
CSCwh60848	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
CSCwd45402	MSR Unicast-To-Multicast not working if DST and SRC are the same in Service Reflect configuration.
CSCwd90168	Unexpected reload after running **show voice dsp** command while an ISDN call disconnects.
CSCwd16559	ISG FFR: ARP request to reroute nexthop IP is not triggered if ARP entry not in ARP table.
CSCwd79089	Controller crash when sending full line rate of traffic with >5 Intel AX210 stations.
CSCwc27307	Service Engine YANG support for ZBFW.
CSCwd16664	GetVPN long SA - GM re-registration after encrypting 2^32-1 of packets in one IPsec SA.
CSCwd81357	QoS classification not working for DSCP or ACL + MPLS EXP.

Bug ID	Description
CSCwd89338	Clear ISG existing lite-session upon reception of DHCP packet for same client.
CSCwc99823	FMAN crash seen in SGACL@ fman_sgacl_calloc.
CSCwc78021	Standby WLC crash @ fman_acl_remove_default_ace.
CSCwd25107	Interface VLAN1 placed in shutdown state when configured with **ip address pool**.
CSCwd61255	Data Plane crash on device when making Per-Tunnel QoS configuration changes with scale.
CSCwe01015	IKEv2/IPSec - phase 2 rekey failing when peer is behind NAT.
CSCwd03869	CEF DPI load-balancing causes out of order packets.
CSCwc65697	Device crashing and restarting during call flow with new image.
CSCwd84599	Dataplane memory utilization issue - 97% QFP DRAM memory utilization.
CSCwc88791	DSL: erroneous atm interface counter at DSL retraining.
CSCwe03614	CWMP : MAC address of ATM interface is not included in Inform message.
CSCwd38943	GetVPN: KS reject registration from a public IP.
CSCwd06372	Unconditional excessive logging in eogre tunnel error handling case.
CSCvy14316	MPLS VPN traffic dropped due FDB OOM with cause FIAError under scale flow number (<1M).
CSCwd85580	Device unexpected reload after **set ospfv3 authentication null** command.
CSCwd33202	DHCP behavior issue when BDI interface is enabled on WAN and SVI interface.
CSCwd06923	Stale IP alias left after NAT statement got removed
CSCwd47123	ISG uses identifier mac-address 0000.0000.0000 when DHCP LQ does not reply.
CSCwd72312	GetVPN : Traffic drops seen on GM after rekey installing policies on image.
CSCwc14688	Single WAN Interface subslot 0/0 timing.
CSCwd07516	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
CSCwd39257	IOS-XE CPP crash when entering **no ip nat create flow-entries**.
CSCwd63783	Memory leak caused router reload.

Bug ID	Description
CSCwd97077	Device leaking memory in MallocLite because of telemetry subscription to collect FNF cache.
CSCwe09805	OID for SNMP monitoring of DSP resources are not working as expected.
CSCwe25076	ALG breaks NBAR recognition impacting application firewall performance.
CSCwe14885	VPN is established although the peer is using a revoked certificate for authentication.
CSCwe24491	Static NAT with HSRP stops working after removing / adding standby.
CSCwd17272	UTD Packet drop due to fragmentation for ER-SPAN traffic.
CSCwe32862	Router IOS-XE crash while executing AES crypto functions.
CSCwe19084	NAT: Traffic is not translated to the same global address though PAP is configured.
CSCwe07055	Device frequent reloads.
CSCwc28468	Device always fails to push any template to device if device is running in FIPS mode.
CSCwe12652	Incorrect return MIB for ciscoWanCellExtMIB and ciscoWan3gMIB.
CSCwd68994	Unable to match on customer profile based on certificate-map.
CSCwc06327	PFP policy in SRTE, RIB resolution in FC bring down IPSec tunnel interface- stuck at linestate down.
CSCwe38732	IP CEF load sharing command is being changed by the device.
CSCwd34941	NAT configuration with no-alias option is not preserved after reload.
CSCwe37184	Device seeing out of service on Switch modules with new DC power supply.
CSCwh60848	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
CSCwc21739	NAT not requesting further for low ports after initial allocation when CLI knob **reserved-ports** set.
CSCwc39012	Crash saving tracelogs after "Too many open files" error.
CSCwc77663	Device frequent reloads due to stuck thread in CPP.
CSCwc03478	VTCP does not support L2 correctly.
CSCwc72923	ERROR info: Router configuration failed:interface Serial0/1/0:23 isdn switch-type primary-ntt.

Bug ID	Description
CSCwd12591	ucode crash during FW Classification, Session Frees.
CSCwc99668	Routes added by IKEv2 getting deleted at responder.
CSCwc23077	Firewall drop seen stating “FirewallL4” seen on device.
CSCwc78528	DSPware 60.1.1 release targeting v179_throttle.
CSCwc44851	Bootstrap failing on device.
CSCwc96444	Router is not programming correct next-hop for unicast prefix with multicast config present.
CSCwc49715	Crash @ UNIX-EXT-SIGNAL: Aborted(6), Process = Check heaps, having PPPoe with CWMP configs.
CSCwd06118	IKEv2 Cert-based IPSec not working between IOS-XE and AWS.
CSCwb52324	Device unexpected reload due to QFP ucode crash.
CSCwc77183	Packet duplication is causing drops in payment transactions with SdwanGenericDrop code.
CSCwc20170	Device reloads unexpectedly due to critical FTMd fault when VRF configuration is pushed.
CSCwb89958	Unified Policy HSL not sending properly NBAR application information.
CSCwc89328	Device might reboot when supporting explicit IV joins network.
CSCwc52538	Flows are not distributed and load-balanced evenly and consistently.
CSCwc45950	ZBFW self zone policy drops SSH session on Mgmt-intf 512 ports.
CSCwc43794	VRF+NAT Outside Source Static - Drop packets during FTP (Active-mode) execution.
CSCwc79145	Throughput degrades when Local TLOC specified in Data Policy goes down.
CSCwc32595	BFD sessions remains down if interface flap form up/down/up.
CSCwb65396	CLI template push fails with error: 'Error: on line 48: line-mode single-wire line 0'.
CSCwb90252	Automatically freeing up filesystems stale image or recovered folder (lost+found).
CSCwc82140	QFP crash when ZBFW configuration features "log dropped-packets" configuration.
CSCvz89354	Router crashes due to CPUHOG when walking ciscoFlashMIB.
CSCwc39865	Subscriber Session getting stuck and needs clearing it manually.
CSCwb48953	Speed test failing with "Device Error: Speed test in progress".
CSCwd11365	Needs cert update - Azure CGW creation fails due to NVA provisioning failure.

Bug ID	Description
CSCwc56033	Not triggering any alarms when RPM of a fan is 0.
CSCwc84967	Intermittent double DTMF due to changing timestamp on a DTMF event.
CSCwb08057	ISG: Number of lite sessions conversion in progress counter not decrementing on failed account-logon.
CSCwc29629	Crashes when Virtual-Access tries to bring-up/bring-down OSPFv3 ipsec crypto session authentication.
CSCwd13352	SSH getting closed after update.
CSCwc77177	BFD and control packets are dropped when ACL is applied on gigi to which loopback is bind.
CSCwc68132	SIG tunnel tracker packets are dropped by firewall with self zone policy.
CSCwd56336	BFD sessions are not coming up after flapping the interface due to low FTM rate.
CSCwd56015	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
CSCwd45508	Device does not form BFD across Serial link when upgrading.
CSCwd23810	IOS-XE: High CPU utilization caused by NHRP.
CSCwd13050	After upgrade, device moved into Out of Sync status.
CSCwd12955	NAT translation is not correctly sent to hub router from branch when SSNAT and UTD are configured.
CSCwc28468	Device always fails to push any template if it is running in FIPS mode.
CSCwb74821	yang-management process confd is not running, controller mode.
CSCwd36621	CERM may kick in due to IPSec sessions initiated for on-demand tunnels.
CSCwd17579	Router crashing with reason CPU Usage due to Memory Pressure exceeds threshold (Reboot).
CSCwd34941	NAT configuration with no-alias option is not preserved after reload.
CSCwd33966	Unable to configure the local BGP as-path-list.
CSCwd37410	0365 and MS Teams applications access issues when using DIA with app-list match in data-policy.
CSCwd38626	Repeating SYS-2-PAK_SUBBLOCK_BADSIZE: 4 -Process= "&lt;interrupt level&gt;".

Bug ID	Description
CSCwc37465	Unable to push no-alias option on static NAT mapping from management system.
CSCwd44006	Control connection on device doesn't come-up with reverse proxy using Enterprise Certificate.
CSCwd29334	Upgrade failures due to inability to establish netconf connection.
CSCwc88791	DSL: erroneous atm interface counter at DSL retraining.
CSCwa96399	Configuring entity-information xpath filter causes syslogs to print, does not return data.
CSCwd44586	Login banner config is changed after upgrade.
CSCwd12330	Invalid TCP checksum in SYN flag packets passing through Router.
CSCwc76082	check_sig_ipsec_ike_sessions fails with could not find entry for Tunnel100001.
CSCwa14636	Device stopped forwarding traffic. Suspect OMPd is busy.
CSCwd15560	With 2 sequences, should not skip if the match is different and action is same.
CSCwd33202	DHCP behavior issue when BDI interface is enabled on WAN and SVI interface.
CSCwd17381	NAT/DIA traffic is skipping UTD in forward direction after SSNAT path from service-side.
CSCwd18028	After delete CSP, New CCM bringup on existing CSP is stuck in Initializing CCM on MT cluster.
CSCwc70511	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
CSCvz65764	Peer MSS value showing incorrect.
CSCwa95092	When Object-group used in a ACL is updated, it takes no effect.
CSCwb33968	Failed to display active flows when flow count is high on the device.
CSCwb02142	Traceback: fman_fp_image core after clearing packet-trace conditions.
CSCwb49857	Memory leaks on keyman process when key is not found.
CSCwa65728	Large number of DH failures.
CSCwb11389	NAT translation stops suddenly(ip nat inside doesn't work).
CSCwa84919	Revocation-check crl none does not failover to NONE DNAC-CA.

Bug ID	Description
CSCwb39098	Router crashed after new IPv6 address assigned when router use specific configuration.
CSCwa69101	Initiator unclassified ip-address LQipv4 command has no effect.
CSCwa67886	UDP based DNS resolution doesn't work with IS-IS EMCP on IOS-XE.
CSCvz84588	Destination prefix packets getting dropped because forwarding plane is not programming the next hop.
CSCwb27486	New Key for NBAR app and NBAR category without OGREF optimized.
CSCwa72273	ZBFW dropping return packets from tunnel post upgrade.
CSCwa49101	OMP origin protocol comparison cleanup.
CSCwb17282	Router crashing when clearing a VPDN session.
CSCwa49721	Hub with firewall configured incorrectly dropping return packets when routing between VRFs.
CSCwb38501	Support IGMP on voice vlan.
CSCwb21645	NAT traffic gets dropped when default route changes from OMP to NAT DIA route.
CSCwb12647	Device crash for stuck threads in cpp on packet processing.
CSCwb18223	SNMP v2 community name encryption problem.
CSCwb16723	Traceroute not working with NAT.
CSCwb31587	Subject-alt-name attribute in certificate trustpoint causes Windows NDES/CA to reject SCEP requests.
CSCwb51238	Router reload unexpectedly two times when enter netflow show command.
CSCwa98617	Memory Leak in AEM chunks related to Firewall.
CSCwa48512	CoR intercepted DNS reply packets dropped with drop code 52 (FirewallL4Insp) if UTD enabled also.
CSCwa93664	ThousandEyes container may fail to get installed on device.
CSCvz28950	DMVPN phase 2 connectivity issue between two spokes.
CSCwa78348	Traceback: IOS-XE reload after Segmentation fault on Process = SSS Manager.
CSCvz81664	Enabling or disabling OMP overlay AS prevents connected routes from being advertised in OMP.
CSCwa67029	ROMMON version not displaying correctly
CSCwb43423	IOS-XE image installation fails.
CSCwa08847	ZBFW policy stops working after modifying the zone pair.

Bug ID	Description
CSCwb15331	Keyman memory leak using public keys.
CSCvw50622	NHRP network resolution not working with link-local ipv6 address.
CSCwb59736	CSR BFD tunnel are zero.
CSCwa57873	Incorrect reload reason - Last reload reason: LocalSoft for Netconf Initiated request.
CSCwb51595	Missing IOS config (voice translation rule) on upgrade.
CSCwb18315	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
CSCwc39012	Crash saving tracelogs after Too many open files error.
CSCwc56896	Crash in ipv6_tunnel_macaddr while adding/removing gre multi-point tunnel mode.
CSCwb89958	Unified Policy HSL not sending properly NBAR application information.
CSCwc23077	Firewall drop seen stating FirewallL4.
CSCwb74821	yang-management process confd is not running, controller mode.
CSCwc37465	Static NAT configuration in CLI with the no-alias keyword cannot be retrieved via NETCONF/YANG.
CSCwc44851	Bootstrap failing on device.
CSCwc55684	Layer 7 health check doesn't work on loopback interfaces.
CSCwc49715	Crash @ UNIX-EXT-SIGNAL: Aborted(6), Process = Check heaps, having PPPoe with cwmp configs.
CSCwc52538	Traffic flows are not distributed and load-balanced evenly and consistently.
CSCwc55260	Memory leak due to FTMd process.
CSCwc69881	Device lost configuration due to multiple power cycles on site.
CSCwc20170	Device reloads unexpectedly due to critical FTMd fault when VRF configuration is pushed.
CSCwb88621	Device unable to establish control connection with vBond due to out of order DTLS packets.
CSCwc59598	Statistics collection causing service-side BFD to flap on every collection interval.
CSCwc50477	Device crashed in ipv4_nat_create_out2in_session_entry.

Bug ID	Description
CSCwc67465	Router cannot be upgraded.
CSCwc32595	BFD sessions remains down if interface flap form up/down/up.
CSCwc38529	Traffic seems not inspected by UTD when umbrella is set.
CSCwc63563	Unable to set specific speed and duplex values on SFP ports on IOS-XE routing platforms.
CSCwc39865	Subscriber Session getting stuck and needs clearing manually.
CSCwc43973	DLC is not completing after upgrading to Smart licensing from CSL.
CSCwc53885	IOS-XE no ip nat config is allowed to be committed and removes nat routes among other nat config.
CSCwc55467	BFD Tunnel on router is not staying up, 1 out of 40 tunnels.
CSCwc56033	Not triggering any alarms when RPM of a fan is 0.
CSCwc42978	Device loses all BFD sessions with Invalid SPI.
CSCwc67171	Tracebacks at cgm_avlmgr_class_init and cpuhog_key_init.
CSCwb08057	Number of lite sessions conversion in progress counter not decrementing on failed account-logon.
CSCwc63337	Destination not reachable if configured as a next for a static route resolvable via non /32 OMP.
CSCwc19533	CRC errors seen after upgrade on device.
CSCwc29629	Crashes when Virtual-Access tries to bring-up/bring-down OSPFv3 ipsec crypto session authentication.
CSCwc27208	BFD sessions not coming UP because of ANTI-REPLAY-FAILURES.
CSCwc68132	SIG tunnel tracker packets are dropped by firewall with self zone policy.
CSCwc70468	CPA fail to send SIP Update for AsmT before maxTermToneAnalysis expiration.
CSCwc70511	Router reloaded unexpectedly.
CSCwc65697	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 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.

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.