Release Notes for Cisco Catalyst 8500 Series Edge Platforms, Cisco IOS XE Cupertino 17.9.x

First Published: 2022-08-26

Last Modified: 2026-08-05

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 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)

About Cisco Catalyst 8500 Series Edge Platforms



Note Cisco IOS XE Cupertino 17.9.1a is the first release for Cisco Catalyst 8500 Series Edge Platforms in the Cisco IOS XE Cupertino 17.9.x release series.

The Cisco Catalyst 8500 Series Edge Platforms are high-performance cloud edge platforms designed for accelerated services, multi-layer security, cloud-native agility, and edge intelligence to accelerate your journey to cloud.

The Cisco Catalyst 8500 Series Edge Platforms includes the following models:

- C8500-12X4QC
- C8500-12X
- C8500L-8S4X

For more information on the features and specifications of Cisco 8500 Series Catalyst Edge Platform, refer the Cisco 8500 Series Catalyst Edge Platform datasheet.

Sections in this documentation apply to all models of unless a reference to a specific model is made explicitly.

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.

New and Changed Software Features

New and Changed Software Features in Cisco IOS XE 17.9.10

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.9.9

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.9.8

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.9.7a

There are no new features in this release.

New and Changed Software Features in Cisco IOS XE 17.9.6

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.9.5f

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.9.5e

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.9.5a

There are no new software 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

Table 1: Software Features in Cisco IOS XE 17.9.3a

Feature	Description
Support for broadband features and functionalities with DNA Network Advantage Tier 3 license	From Cisco IOS XE 17.9.3a release, the following functionalities and features are supported on C8500-12X and C8500-12X4QC platforms with DNA Network Advantage Tier 3 license: • Layer 2 Tunnel Protocol Network Server (LNS) • Broadband Network Gateway (BNG) • Layer 2 Access Concentrator (LAC) • Intelligent Services Gateway (ISG) • Intelligent Wireless Access Gateway (iWAG) • PPP and IP sessions

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 in Cisco IOS XE 17.9.1a

Table 2: Software Features

Feature	Description
Disabling USB Ports	You can now use the **platform usb disable** command to disable the USB ports on Cisco Catalyst 8500 Edge Series platforms.
Increase ACE Scale Limit Per OGACL	This feature provides an increase in the ACE (Access Control Engine) scale limit per ACL and OGACL(Object Group Access Control List) as the current implementation of CACE (Common Adaptive Classification Engine) has a total limit of only 64K entries. The scale for this feature is 1D and the scale information for OGACL is 3000 ACE entries per OGACL, 2400 OGs and 100 networks per OG.
Logging Destination IP Address and Port Details	The **ip nat settings log-destination** command is introduced in Carrier Grade Network Address Translation (CGN) mode to include the destination IP address and the destination port details in the add and delete HSL records.
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 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.
MACsec Extended Packet Numbering (XPN) Support	This enhancement introduces support for extending the packet number (PN) for MACsec frames from 32-bit to 64-bit. The 64-bit extended packet number (XPN) eliminates the need for frequent SAK(Security Association Key) rekey due to exhaustion of the 32-bit PN that may occur in high-capacity links.
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.
Smart Licensing Using Policy Features	

Feature	Description
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)
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).
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.

Feature	Description
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)

Feature Navigator

You can use Cisco Feature Navigator (CFN) to find information about the features, platform, and software image support on Cisco Catalyst 8500 Series Edge Platforms. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/ An account on cisco.com is not required.

Resolved and Open Bugs in Cisco IOS XE 17.9.10

Resolved Bugs in Cisco IOS XE 17.9.10

Identifier	Headline
CSCwt42293	IR8140: Cellular interface flap causing crypto enrollment failure.

Open Bugs in Cisco IOS XE 17.9.10

There are no customer impacting bugs that were identified in this release.

Resolved and Open Bugs in Cisco IOS XE 17.9.9

Resolved Bugs in Cisco IOS XE 17.9.9

Identifier	Headline
CSCwq01495	Cisco IOS, IOS XE, Secure Firewall Adaptive Security Appliance, and Secure Firewall Threat Defense Software IKEv2 denial of service vulnerability.
CSCwo40128	Device could experience an unexpected reload while connecting with MFA.

Open Bugs in Cisco IOS XE 17.9.9

This release contains only PSIRT fixes. No new bugs are identified.

Resolved and Open Bugs for Cisco IOS XE 17.9.8

Table 3: Resolved Bugs for Cisco IOS XE 17.9.8

Bug ID	Description
CSCwq31287	Cisco IOS and IOS XE Software SNMP Denial of Service and Remote Code Execution Vulnerability.

Open Bugs for Cisco IOS XE 17.9.8

This release contains only PSIRT updates. No new bugs were identified.

Resolved and Open Bugs for Cisco IOS XE 17.9.7b

There are no open and fixed issues identified in this release.

Resolved and Open Bugs for Cisco IOS XE 17.9.7a

Table 4: Resolved Bugs for Cisco IOS XE 17.9.7a

Identifier	Headline
CSCwk31560	NAT Command not readable after reload
CSCwm78086	BFD session is down after changing TLOC preference with pairwise-keying enabled
CSCwm07396	Few BFD sessions down after clear mka session on client
CSCwm07651	Device may experience an unexpected reset due to dbgd process
CSCwn56474	Pairwise-keying every single BFD session up/down which trigger tunnel delete/create events
CSCwm05395	Add event cause in IPsec vesen log
CSCwo14912	Replay window programming errors may cause transient protocol flaps (e.g. ISIS)
CSCwn19888	Device may experience a qfp-ucode crash due to stuck thread condition
CSCwn07671	Tracker group with IP and DNS name tracker elements goes down when DNS query is failing
CSCwj92560	STCAPP command removed from device after reload
CSCwm81900	CPP crashed during UTD security policy config
CSCwk03686	Crash due a segmentation fault due a negative value
CSCwd01261	MACsec with Non XPN cipher suite can't rekey as expected when PN reach 75%(2^32 - 1)
CSCwh50510	Device crash with segmentation fault when processing NHRP traffic
CSCwn20614	After change integrity-type twice, all BFD sessions will be down.
CSCwh45169	Unexpected reboot while dispalying information from cleared session
CSCwm38875	Device fatal crash
CSCwk97930	Crash occurs when IPv6 packets with link-local source are forwarded to tunnels
CSCwk45165	Memory leak on device

Identifier	Headline
CSCwm81246	MACsec interfaces lock up on TX direction after reload
CSCwi87546	CPP unexpectedly reboot due to QFP CPP stuck released
CSCwn24226	GETVPN Mismatch in GMs reported across COOP Due to KEK Sync Issue Between Prim & Sec KSs
CSCwk95044	Packet drops observed with packet duplication enabled when the Primary TLOC is shut
CSCwk75459	MGCP GW fails to respond with 250 OK when there's a delay from dataplane in gathering stats
CSCwc28751	ZBFW crash when enabled on L2 firewall
CSCwm48755	Static IP NAT outside entry is translating traffic only in one direction with MPLS VPN
CSCwm79570	Cisco IOS and IOS XE SNMP Denial of Service Vulnerabilities
CSCwm89600	Cisco IOS, IOS XE, and IOS XR SNMP Denial of Service Vulnerabilities
CSCwm79581	Cisco IOS and IOS XE SNMP Denial of Service Vulnerabilities
CSCwm79554	Cisco IOS and IOS XE SNMP Denial of Service Vulnerabilities
CSCwm79596	Cisco IOS and IOS XE SNMP Denial of Service Vulnerabilities
CSCwm79577	Cisco IOS and IOS XE SNMP Denial of Service Vulnerabilities
CSCwk08261	device unexpected reload with ipv4_sbc_input () at /dplane/feature/sbc/sbc_packet decode
CSCwn48914	Device crash during SGW sync in VOICE REG BG Process
CSCwn61584	**listen-port** command is not working properly under tenants for UDP
CSCwn13988	CDR file accounting credentials exposure
CSCwn60303	CUBE sip-ua commands lost after reload, CAT8
CSCwm91195	Memory leak on CUBE in subscribe pass-thru scenario
CSCwn19326	CDR file accounting creates dummy files
CSCwm91175	OOD Subscribe with event message-summary is causing memory leak on CUBE
CSCwn49403	CUBE incorrectly offers rtp instead of srtp in 200OK for srtp fallback scenario

Table 5: Open Bugs for Cisco IOS XE 17.9.7a

Identifier	Headline
CSCwm33545	FlexVPN - IP address assigned to spoke changes to unassigned
CSCwh18120	IKEv2 diagnose feature is taking 11% CPU during session bring up

Identifier	Headline
CSCwn51758	Incoming packet are drop with bad checksum when l2tp through ipsec encrypted tunnel on device

Resolved and Open Bugs for Cisco IOS XE 17.9.6

Table 6: Resolved Bugs for Cisco IOS XE 17.9.6

Identifier	Headline
CSCwj70335	Crypto IKEv2 - Fragmented Authentication packets detected as malformed on third party vendor device
CSCwj04575	Device crashed during SNMPwalk when removing SFP
CSCwj08744	Unexpected reload when using **show running-config full | format**
CSCwi93422	Unexpected reload due IPV6 TCP packet in QFP
CSCwi56804	IPSEC FlowDB exhaustion
CSCwk26247	QFP stuck threads crash while handling netflow features under autonomous mode
CSCwi58732	IPSEC FlowDB duplicate flow
CSCwh96578	SKA_PUBKEY_DB leak in TDL
CSCwi08171	Device may crash due to Crypto IKMP process
CSCwi68865	Memory leak in crypto IKEv2
CSCwj88872	IPSec tunnel fails to establish due to error
CSCwj92234	Segmentation fault
CSCwj84949	Unencrypted traffic due to non-functional IPSec tunnel in FlexVPN hub and spoke setup
CSCwj40589	Endpoint tracker using DNS does not log down message when DNS server reachability is lost
CSCwk33173	EzPM application-performance profile cause memory leak and crash with long-lived idle TCP flows
CSCwj24511	Tunnel QoS - Incorrect IP precedence classification
CSCwj53986	Extremely poor DMVPN performance on device with TrustSec
CSCwj76501	Data Plane Crash in ERSPAN Processing
CSCwb47658	Repeated and endless messages
CSCwj45130	Segmentation fault IPSec dummy packet process

Identifier	Headline
CSCwi06404	PKI crash after failing a CRL fetch
CSCwk12524	Device reloaded due to ezManage mobile app service.
CSCwi89510	MPLS elephant flow causing overruns
CSCwj72888	Reload in tcp_sanity due to l4 pointer not set
CSCwi56114	Secure datawipe should reset the configuration register
CSCwi25737	Device should discard IKE notification messages with incorrect DOI
CSCwj36915	MACsec not working under LACP port-channel member port
CSCwh50628	Race condition crash on device
CSCwi78365	Trim installed certificate on upgrade
CSCwk53680	nbound calls through device results in phantom calls
CSCwi09301	Shutting a dialer interface with PPPoA unshuts it automatically
CSCwj48421	FlexVPN client : IPSec tunnels are down due to issue with SADB detach and delete
CSCwd17906	Input overrun errors on interfaces under bursty conditions
CSCwj86794	Device crashes while processing an NWPI trace
CSCwj73113	Device doesn't respond with 250 OK for a DLCX leading to DLCX loop from CUCM side
CSCwj30334	Router rebooted when attempting merge on used CVLA block
CSCwi62239	%IOSXE_MGMTVRF-3-INTF_ATTACH_FAIL error after configuring loopback managment vrf
CSCwj05013	CUBE Media Proxy(CMP) dual forking not working after upgrade
CSCwi27011	Inbound- outbound call drops with CC=47
CSCwi51157	Device crashing due to a segmentation Fault in CCSIP_SPI_CONTROL process
CSCwi62717	Ambiguous CLI **exit** under **voice class tenant**
CSCwj23804	Password created with "key config-key password-encrypt" ending with a "\" are lost after reload
CSCwj23735	CUBE - "rtp port range" configuration lost under "voice service voip" after reload
CSCwj26668	IOS XE wrong audio rtp packet marking for SCCP SRST
CSCwh81312	Internal Error : NO MEMORY seen in standby router while checkpointing legs.
CSCwj05139	CUBE incorrectly switch to flow-trough mode on one leg after reinvite
CSCwj03696	Cannot call device in survivability mode if its ID ends with "T", CUBE Enterprise

Identifier	Headline
CSCwj95128	CUBE incorrectly change dtmf payload in asymmetric case
CSCwi47242	destination calling e164-pattern-map doesn't work
CSCwj59262	Secure media forking -1 of 2 audio Streams is encrypted due to same key sent for both streams
CSCwj54666	SIP cause code incorrect for CCAPI cause code 31
CSCwi77331	IOS-XE unexpected reboot after CLI **show sip-ua connection**
CSCwk21056	Unexpected reboot due to HTTPc when executing XCC
CSCwi69071	Unexpected reload caused by crash
CSCwj93967	History-Info header compatibility between CUBE and MS Direct Routing
CSCwk81414	CUBE Sending + on DID Number When "+" is Showing in the Line Text Label portion of From Header
CSCwj98360	Media forking not working in CUBE
CSCwj82258	IOS-XE router may crash during transfer call flow in SRST
CSCwi59377	Calls are intermittently hitting the incorrect di
CSCwk08864	**authentication** command under dial-peer is missing "challenge
CSCwi39253	Out of Dialog SIP options ping not received but dial peer status still shows as active
CSCwj41553	SGW calling to TDM, AOR is not getting changed to number
CSCwj75508	SRST running on device fails to register SCCP phones after reload

Table 7: Open Bugs for Cisco IOS XE 17.9.6

Identifier	Headline
CSCwj79987	Device does not establish BFD sessions after upgrade
CSCwk89256	Speed mismatch in IOS-XE configuration
CSCwk31560	NAT command not readable after reload
CSCwm27647	BFD sessions are down and not recovering for one color after hub replacement
CSCwj44868	Wrong severity for rekey acknowledgement configuration mismatch log message
CSCwm07651	Device crash due to dbgd process
CSCwm11819	Device crash due to SIGSEGV
CSCwk95308	CRC errors increment on down interface of device
CSCwi16716	Device crashed upon increasing the gatekeeper cache size
CSCwi05232	Traceback seen when no dialer interface or peer down

Identifier	Headline
CSCwk49806	Device rebooted unexpectedly due to process NHRP crash
CSCwi31110	Traceback seen due to negative global cache count
CSCwb55514	Unexpected reboot of the ESP seen after enabling **platform qos port-channel-aggregate**
CSCwj13395	Device data plane crashed when starting a new NWPI trace from this device with NAT DIA/ZBFW
CSCwk63722	Startup configuration failure post PKI server enablement
CSCwj77594	WAN IP is allowed to be configured as system IP
CSCwh44418	ARP incomplete in VRF management interface
CSCwk75459	Device fails to respond with 250 OK when there's a delay from dataplane in gathering statistics
CSCwk89523	Device crash during function to add/delete a MAC address from the MAC accounting table.
CSCwf73123	BFD timers reverting back to default value after negotiating correctly
CSCwk20583	40G interfaces with breakout configurations flap after reload
CSCwk03686	Crash due a segmentation fault due a negative value
CSCwb25507	Add vendor specific parameter for NBAR protocol pack version
CSCwh50510	Device crash with segmentation fault when processing NHRP traffic
CSCwk31715	After deleting a NAT configuration, the IP address still shows up in routing table.
CSCwm27005	Traceback seen constantly
CSCwf25735	QoS more than four remark with set-cos not work
CSCwc42837	Device crash when creating VRF when subscriber event tracing is enabled
CSCwk30527	IKEv2 session is down after reload if identity local address is assigned to interface
CSCwh45169	Unexpected reboot while displaying information from cleared SSS session
CSCwk44078	GETVPN migrating to new KEK RSA key doesn't trigger GM re-registration
CSCwk61133	IOMd memory leak due to POE TDL message
CSCwm32269	Onboarding fails - EAP-TLS failed to fetch IP address
CSCwm13223	Device crashes due to malformed syslog
CSCwk22942	Unable to build two IPSec SAs

Identifier	Headline
CSCwk57979	Fault due to ensor has exceeded it's maximum number of read errors
CSCwk79454	Endpoint tracker does not fail if default route is removed
CSCwh12093	Enable SoS or ROC feature for DSL
CSCwm14665	Enable BFD L2 messages in the punt path for device.
CSCwk37351	Unexpected reboot during PVDM OIR
CSCwh41497	DDNS update retransmission timer fails to work with a traceback error
CSCwk27099	Cellular connection is picking the wrong profile
CSCwk72795	No statistics for the SBFD protocol
CSCwc86434	Static NAT DIA inside static routes being advertised over OMP to remote sites
CSCwi72295	Inconsistencies with openconfig-interfaces:config yang model after defaulting interface
CSCwi16111	ipv6 tcp adjust-mss not working after delete and reconfigure
CSCwi63042	Packet drops observed between LISP EID over GRE Tunnel
CSCwi62098	**show crypto ipsec sa output** displays incorrect replay status

Resolved and Open Bugs for Cisco IOS XE 17.9.5f

There are no customer impacting bugs that were fixed or identified in this release.

Resolved and Open Bugs for Cisco IOS XE 17.9.5e

Resolved Bugs for Cisco IOS XE 17.9.5e

Identifier	Headline
CSCwi88969	FMFP-3-OBJ_DWNLD_TO_DP_FAILED observed when delete and configure zone-pair back
CSCwi06404	PKI crash after failing a CRL Fetch
CSCwi04547	Custom Application is marked as invalid
CSCwk84047	Memory Leak due to security violation by new MAC address and Del Pend object increases - ACE_IPV4
CSCwh96578	SKA_PUBKEY_DB leak in TDL
CSCwk50488	Memory leak in fman_rp under acl_db
CSCwj03200	Reboot on IOS-XE during internal SSH certificate check when SSH session is started from device

Identifier	Headline
CSCwk45165	fman_fp Memory Leak
CSCwj40589	Endpoint tracker using DNS does not log DOWN message when DNS server reachability is lost
CSCwi87546	CPP unexpectedly reboot due to QFP CPP stuck at waiting for rw_lock - Lock id of 0 released

Open Bugs for Cisco IOS XE 17.9.5e

Bug ID	Headline
CSCwm83692	removes NAT egress-interface option from config

Resolved and Open Bugs for Cisco IOS XE 17.9.5a

Resolved Bugs for Cisco IOS XE 17.9.5a

Identifier	Headline
CSCwh73350	Device keeps crashing when processing a firewall feature.
CSCwf67564	Device observes memory leak at process SSS manager.
CSCwf23291	**write** or **do write** saves the configuration but the RSA keys /SSH is lost after reload.
CSCwc79115	Device policy commit failure displays notification and alarm from Cisco Catalyst SD-WAN Controller.
CSCwh28680	Device packet duplication performance improvement.
CSCwf55933	Device crashed after Cisco Catalyst SD-WAN Manager running Network-Wide Path Insight.
CSCwh68508	Unexpected reboot after establishing control plane of EVPN MPLS and receiving packets.
CSCvo01546	NHRP reply processing dequeues an unrelated request.
CSCwf82676	CPU usage mismatch between **show sdwan system status** and **show proc cpu platform**.
CSCwf03193	Device crash with crashinfo files are generated with segmentation fault, and process IPSEC key engine.
CSCwh08434	OMP route is advertised although the route is not available.
CSCwf26875	Port-channel displayed suspended status applying **platform qos port-channel-aggregate**.
CSCwf24164	Netflow stops working when flow monitor reaches cache limit in the device.

Identifier	Headline
CSCwh63061	Device displays four additional NR bands support - 1, 3, 7, and 28.
CSCwf65540	Running tests on ThousandEyes Agent causes tracebacks on device running TE in docker container.
CSCwi28227	NAT HSL logging vrf-filter is not working.
CSCwh06834	Using special characters in the password while generating TP displays an invalid TP.
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.
CSCwe91898	Environmental syslog does not appear when power cord is disconnected from the redundant PS.
CSCwf55243	Device crashes while adding a trustpoint to the router .
CSCwf84522	Unexpected device reboot while classifying packet with CTF (Common Flow Table).
CSCwf62757	Device interface data report interval issue for physical interface.
CSCwh49644	CSDL compliance failure : Use of 3DES by IPSec is denied.
CSCwh32386	Unexpected reload on device due to the critical process fman_fp_image in 17.9.3a.
CSCwe30514	Device reboots with sslproxy and utd enabled.
CSCwh30377	Device data plane crashes in Umbrella/OpenDNS processing due to an incorrect UDP length.
CSCwf34171	**Configure replace** command fails due to the license UDI PID XXX SN:XXXX line on devices.
CSCwh62116	Device packet dup performance improvement.
CSCwf96980	Unexpected reboot after configuring application redundancy.
CSCwe64779	Device software forced reset during high IPC congestion with IPsec.
CSCwh01425	ITU channel configuration is not working on device.
CSCwh20577	Crashed by Track Client thread at access invalid memory location.
CSCwh00963	Unable to migrate from ADSL to VDSL without reboot on device.
CSCwh36801	Crash in IP input process during tunnel encapsulation.
CSCwh96415	Cannot disable DMVPN logging.
CSCwe85301	Crypto PKI-CRL-IO_0 process crash when PKI trustpoint is deleted.
CSCwh20734	Crypto PKI-CRL-IO_0 process crash when PKI trustpoint is requested and deleted.

Identifier	Headline
CSCwf71557	IPv4 connectivity over PPP not restored after reload.
CSCwc97579	Spoke-spoke cache refresh is not working correctly in case of multiple cache entries for same next hop.
CSCwf11394	Vdaemon debug log must mention port-hop and reason prior to DISTLOC.
CSCwf04866	Keyman process crashes while re-generating SSH key in the device.
CSCwh00332	B2B NAT: When configration IP NAT inside/outside on VASI intereface, the ack/seq number is abnormal.

Open Bugs for Cisco IOS XE 17.9.5a

Identifier	Headline
CSCwf84960	C-NIM-2T: LED L remains green after port shutdown.
CSCwh18120	IKEv2 - The diagnose feature is taking 11% CPU when brining up the session.
CSCwh22414	Warning and critical CPU utilization thresholds not recomputed when using data-plane-heavy mode.
CSCwi01046	PoE module is does not provide enough power to bring up the ports after an unexpected reload.
CSCwc30418	Segmentation fault observed in ikev2_dupe_delete_reason.
CSCwh84068	Device crash after changing NAT HSL configuration.
CSCwi16716	Device crashed upon increasing the gatekeeper cache size.
CSCwh12093	Enable SoS/ROC feature for DSL.
CSCwi06843	Endpoint tracker triggers a CPU Hog.
CSCwi05232	Traceback on device is seen when no dialer interface or peer down.
CSCwi53306	Unknown appID in ZBFW HSL log.
CSCwi10735	ZBF drops transit WAAS PSH/ACK packet due to invalid ACK number.
CSCwi06404	PKI crash after failing a CRL fetch.
CSCwi46997	NAT command not readable after a reload.
CSCwi33168	DSP reports out of range utilization values in SNMP.
CSCwi08171	Device crashes due to Crypto IKMP process.
CSCwi53951	Packets with unicast MAC get dropped on a Port Channel L2 Sub-intf after a router reboot.

Identifier	Headline
CSCwb25507	CWMP : Add vendor specific parameter for NBAR protocol pack version.
CSCwi25737	The device must discard IKE notification messages with incorrect DOI.
CSCwh50510	Device crashes with Segmentation fault(11), Process = NHRP when processing NHRP traffic.
CSCwh80441	Cosmetic 3G issue - device is displayed as unknown.
CSCwh91136	Traffic is not encrypted and droped over IPsec SVTI tunnel.
CSCwe24491	Device: 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 crashes after decoding all packets to text (using l2 copy) on fia trace.
CSCwi04547	Cisco SD-WAN custom application is marked as invalid.
CSCwi16111	IPv6 TCP adjust-mss not working after delete and reconfigure.
CSCwi63042	Packet drops observed between LISP EID over GRE tunnel.
CSCwi59202	C-NIM-2T cannot boot up in IOS.

Resolved and Open Bugs for Cisco IOS XE 17.9.4a

Resolved Bugs for 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 for Cisco IOS XE 17.9.4a

Bug ID	Headline
CSCwf26875	Ten0/0/2 from port-channel going to suspended status applying **platform qos port-channel-aggregate**.
CSCwe95072	Unexpected reload due to memory corruption when modifying and access list.
CSCwf52751	CLI template fails to attach to device with error access-denied.
CSCwf55145	SFP transceiver DOM not working after some time, however interface forwards the traffic as expected.
CSCwf24164	Netflow stops working when flow monitor reaches cache limit in C8500L.

Bug ID	Headline
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.
CSCwe25815	Crash due to dtl push/pop on wait loop.
CSCwf55243	Device is crashing while adding a trustpoint to the router.
CSCwf62757	C8500L interface data report interval issue for physical interface.
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	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 config; but remains in startup config.
CSCwf51206	EVPN: BUM traffic is not flooded to bridge domain interface.
CSCwf31934	C8500L - executing **show platform hardware qfp active fbd-flowdb dump** leads to a crash.
CSCwf11394	IOS XE debug log should mention port-hop and reason prior to DISTLOC.
CSCwe51910	SNMP ifindex persist does not work.

Resolved and Open Bugs for Cisco IOS XE 17.9.4

Resolved Bugs for Cisco IOS XE 17.9.4

Bug ID	Headline
CSCwf48808	FlexVPN: Stale client routes stuck in RIB on FlexServer.

Bug ID	Headline
CSCwe93905	NAT ALG is changing the Call-ID within SIP message header causing calls to fail.
CSCwf02225	Device freezes for show commands.
CSCwe28204	C8500L: control connection over L3 Tloc extension failing as no NAT table entry created.
CSCwe24210	SNMP MIB does not show correct firmware version for LTE module.
CSCwe18124	MACsec remains marked as secured, but randomly the traffic stops working.
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.
CSCwe41946	DTMF is failing through IOS MTP during call on-hold.
CSCwe37123	C8500 platform uses excessive memory when configuring ACLs with Large Object Groups.
CSCwe12194	Auto-Update cycle incorrectly deletes certificates.
CSCwd49309	uCode crash seen on device with traffic pointing to segfault in coff handler.
CSCwe33793	Memory allocation failure with extended antireplay enabled.
CSCwe66318	NAT entries expire on standby device.
CSCwe31471	Segmentation fault when per-tunnel qos config withdraw.
CSCwd59722	Unexpected reboot due to IOSXE-WATCHDOG prrocess.
CSCwe70374	Platform punt-policer is not configurable.
CSCwe20008	SNMP MIB OID changing its last index.
CSCwf47563	Device is crashing after importing the trustpoint with rsakeypair.
CSCwe18058	Unexpected reload with IPS.
CSCwd73783	Observed qfp-ucode-wlc crash.
CSCwe39011	GARP on port up/up status from device 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	Headline
CSCwe69783	Device can lose its config during a triggered resync process if lines are in an off-hook state.
CSCwe89404	No way audio when using secure hardware conference with secure endpoints.
CSCwe41234	Device race condition causes no ringing for analog phones.
CSCwa96399	Configuring entity-information xpath filter causes syslogs to print, does not return data.
CSCwe06518	C8500-12X ~23% degradation in IPSEC IPv6 profile for 1400B.
CSCwc89823	Device crashes due to CPUHOG when walking ciscoFlashMIB @snmp_platform_get_flash_file_info.
CSCwe32862	Device IOS-XE crash while executing AES crypto functions.
CSCwf37888	Device packet duplication: duplicate packets are counted on primary tunnel interface statistics.
CSCwd68994	ISAKMP profile doesn't 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.

Open Bugs for Cisco IOS XE 17.9.4

Bug ID	Headline
CSCwf26875	Ten0/0/2 from port-channel going to suspended status applying **platform qos port-channel-aggregate**.
CSCwe95072	Unexpected reload due to memory corruption when modifying and access list.
CSCwf52751	CLI template fails to attach to device with error access-denied.
CSCwf55145	SFP transceiver DOM not working after some time, however interface forwards the traffic as expected.
CSCwf24164	Netflow stops working when flow monitor reaches cache limit in C8500L.
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.
CSCwe25815	Crash due to dtl push/pop on wait loop.
CSCwf55243	Device is crashing while adding a trustpoint to the router.

Bug ID	Headline
CSCwf62757	C8500L interface data report interval issue for physical interface.
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	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 config; but remains in startup config.
CSCwf51206	EVPN: BUM traffic is not flooded to bridge domain interface.
CSCwf31934	C8500L - executing **show platform hardware qfp active fbd-flowdb dump** leads to a crash.
CSCwf11394	IOS XE debug log should mention port-hop and reason prior to DISTLOC.
CSCwe51910	SNMP ifindex persist does not work.

Resolved and Open Bugs for Cisco IOS XE 17.9.3a

Resolved Bugs for Cisco IOS XE 17.9.3a

Bug ID	Headline
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
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
CSCwd89338	Clear ISG existing lite-session upon reception of DHCP packet for same client
CSCwc99823	Fman crash seen in SGACL@ fman_sgacl_calloc
CSCwd71458	Outgoing number of bytes decrease in device interface

Bug ID	Headline
CSCwd44439	Device crashing at fman_sdwan_nh_indirect_delete_from_hash_table
CSCwd25107	Interface VLAN 1 placed in shutdown state when configured with ip address pool
CSCwd05356	Device observing error %HW_FLOWDB-3-HW_FLOWDB_DBLINSTALL_FEATOBJ
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
CSCwd01326	Device crashes with SIGABRT within cio infra under heavy load
CSCwd84391	Device incorrectly drops ip fragments due to reassembly timeout despite fix for CSCwb74917
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
CSCwc14688	Single WAN Interface subslot 0/0 timing
CSCwd07516	Memory leak under linux_iosd-imag related to SNMP.

Open Bugs for Cisco IOS XE 17.9.3a

Bug ID	Headline
CSCwd39257	IOS-XE cpp crash when entering no ip nat create flow-entries
CSCwd63783	Memory leak in process caused device reload
CSCwe19084	NAT: Traffic is not translated to the same global address though PAP is configured.
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
CSCwe28204	Control connection over L3 Tloc extension failing as no NAT table entry created

Bug ID	Headline
CSCwd17272	UTD Packet drop due to fragmentation for ER-SPAN traffic
CSCwe32862	Device crash while executing AES crypto functions
CSCwc28468	Device fails if running in FIPS mode.
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
CSCwe07349	Device goes down with I2C bus stuck
CSCwe38732	IP CEF load sharing command is being changed by device
CSCwd34941	NAT configuration with no-alias option is not preserved after reload

Resolved and Open Bugs for Cisco IOS XE 17.9.2a

Resolved Bugs for Cisco IOS XE 17.9.2a

CSCwc21739	NAT not requesting further for low ports after initial allocation when cli knob reserved-ports is set
CSCwc39012	Crash saving tracelogs after too many open files error
CSCwc03478	VTCP does not support L2 correctly
CSCwc82140	QFP crash When ZBFW Configuration Features log dropped-packets configuration
CSCwd12591	Device 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 throttle
CSCwc44851	Bootstrap failing on device
CSCwc96444	Device is not programming correct next-hop for unicast prefix with multicast config present
CSCwc49715	carsh @ 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
CSCwc43794	Device VRF+NAT Outside Source Static - Drop packets during FTP (Active-mode) execution.
CSCwc77183	Packet duplication is causing drops in payment transactions with device.
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	Multiple devices experienced crashes every 4-5min
CSCwc52538	Device flows are not distributed and load-balanced evenly and consistently

CSCwc45950	ZBFW self zone policy drops ssh session on Mgmt-intf 512 ports
CSCwb90252	Automatically freeing up filesystems stale image or recovered folder (lost+found)
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	Device fails with error: 'Error: on line 48: line-mode single-wire line 0'
CSCvz91309	Crash due to IOSXE-WATCHDOG due to management port traffic storm
CSCvz89354	Device crashes due to CPU HOG
CSCwc39865	Subscriber session getting stuck and needs clearing it manually
CSCwb48953	Device failing with device error: Speed test in progress
CSCwd11365	Needs cert update - Azure CGW creation fails due to NVA provisioning failure
CSCwc72923	ERROR info: Device configuration failed:interface Serial0/1/0:23 isdn switch-type primary-ntt
CSCwc84967	Intermittent double DTMF due to changing timestamp on a DTMF event
CSCwb08057	Number of lite sessions conversion in progress counter not decrementing on failed account-logon
CSCwc29629	Crashes when virtual-cccess tries to bring-up/bring-down OSPFv3 ipsec crypto session authentication
CSCwd13352	SSH from device 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
CSCwb67406	The IPSLA udp-jitter V3 (optimize timestamp+precision microseconds) does not work on
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 for Cisco IOS XE 17.9.2a

CSCwd45363	IPsec throughput level / ambiguous outputs
CSCwd33966	Unable to configure the local BGP as-path-list.
CSCwd23810	IOS XE: A high CPU utilization caused by NHRP
CSCwd44006	Control Connection on device doesn't come-up with reverse proxy using enterprise certificate
CSCwa14636	Device stopped forwarding traffic. Suspect OMPd is busy
CSCwd38626	Repeating SYS-2-PAK_SUBBLOCK_BADSIZE: 4 -Process= ""
CSCvz55282	Serviceability enhancements for config migration failures between releases
CSCwd17381	NAT/DIA traffic is skipping UTD in forward direction after SSNAT path from service-side
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

CSCwd15560	With two sequences, should not skip if the match is different and action is same
CSCwd36621	CERM may kick in due to IPSec sessions initiated for on-demand tunnels
CSCwd44586	Login banner config is changed after upgrade
CSCwd37410	0365 and MS Teams applications access issues
CSCwc28468	Device always fails to push any template to device if device is running in FIPS mode.
CSCwc99823	Fman crash seen in SGACL@ fman_sgacl_calloc
CSCwd29334	Upgrade failures due to inability to establish netconf connection to upgrade-confirm
CSCwd45508	Device does not form BFD across serial link when upgrading
CSCwd17579	Device crashing with reason CPU usage due to memory pressure exceeds threshold(Reboot)
CSCwd34941	NAT configuration with no-alias option is not preserved after reload
CSCwd12330	Invalid TCP checksum in SYN flag packets passing through device

Resolved and Open Bugs for Cisco IOS XE 17.9.1a

Resolved Bugs for Cisco IOS XE 17.9.1a

Bug ID	Headline
CSCvz65764	Peer MSS value showing incorrect
CSCwa95092	When Object-group used in a ACL is updated, it takes no effect
CSCwb33968	Device failed to display active flows when flow count is high on the device.
CSCwa98144	No negotiation auto command changing to negotiation auto after reload
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 does not work)
CSCwa84919	"Revocation-check crl none" does not failover to NONE DNAC-CA
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 drops return packets from Zscalar tunnel post upgrade.
CSCwa49101	OMP origin protocol comparison cleanup
CSCwb17282	Router crashing when clearing a VPDN session

Bug ID	Headline
CSCwa94158	Device media type is not correct after removing an SFP
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 on device with NAT
CSCwb31587	Subject-alt-name attribute in certificate trustpoint causes Windows NDES/CA to reject SCEP requests
CSCwb51238	Device 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
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
CSCvz81664	Enabling or Disabling OMP Overlay AS prevents connected routes from being advertised in OMP
CSCwa49721	Device with firewall configured incorrectly dropping return packets when routing between VRFs
CSCwb43423	IOS XE image installation fails
CSCwa08847	ZBFW policy stops working after modifying the zone pair
CSCwb15331	Keyman memory leak using public keys
CSCvw50622	Nhrp network resolution not working with link-local ipv6 address.
CSCwb59736	BFD tunnel are zero
CSCwa57873	Incorrect reload reason - Last reload reason: Netconf Initiated request
CSCwb51595	Missing IOS config (voice translation rule) on upgrade
CSCwb18315	Umbrella DNS security policy doesn't work on device with SIG tunnels

Open Bugs for Cisco IOS XE 17.9.1a

Bug ID	Headline
CSCwc39012	Crash saving tracelogs after Too many open files error
CSCwc56896	crash in ipv6_tunnel_macaddr while adding/removing gre multi-point tunnel mode
CSCwc18977	Crash with "IPE_CPE_U14_CSR32_IPE_CPE_ERR_CPE_MISC_LEAF_INT__INT_CPE_MALGN_ADDR_ERR " error
CSCwb89958	Unified Policy HSL not sending properly NBAR application information.

Bug ID	Headline
CSCwc27208	BFD sessions not coming up because of ANTI-REPLAY-FAILURES
CSCwb74821	yang-management process confd is not running
CSCwc44851	bootstrap failing on device
CSCwc55684	Layer 7 health check doesn't work on Loopback interfaces
CSCwc52538	Device 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
CSCwb55514	Crash seen after enabling platform qos port-channel-aggregate
CSCwc20170	Dvice reloads unexpectedly due to critical FTMd Fault when VRF Configuration is pushed
CSCwb88621	Device unable to establish control connection due to out of order DTLS packets.
CSCwc37465	Static NAT configuration in CLI with the no-alias keyword cannot be retrieved via NETCONF/YANG
CSCwc50477	Device crashed in ipv4_nat_create_out2in_session_entry
CSCwc67465	Device can not be upgraded
CSCwc19171	High cpu on sip (mip100) due to mcpcc-lc-ms caused by link up/down interrupts
CSCwc26669	TLB miss for lock address during FNF cache lookup
CSCwc32595	BFD sessions remains down if interface flap form up/down/up
CSCvz91309	Crash due to IOSXE-WATCHDOG due to management port traffic storm
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 it manually
CSCwc53885	IOS-XE no ip nat config is allowed to be committed and removes nat routes among other nat config
CSCwc55467	BFD Tunnel on device is not staying up, 1 out of 40 tunnels
CSCwc42978	Device looses 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
CSCwc29629	Crashes when virtual-access tries to bring-up/bring-down OSPFv3 ipsec crypto session authentication
CSCwc23077	Firewall drop seen stating FirewallL4 seen on device
CSCwc68132	SIG tunnel tracker packets are dropped by firewall with self zone policy
CSCwb67406	The IPSLA udp-jitter V3 (optimize timestamp+precision microseconds) does not work on device
CSCwc70511	Device reloaded unexpectedly

ROMmon Release Requirements

Use the following tables to determine the ROMmon version required for your Catalyst 8500 model:

Table 8: Minimum and Recommended ROMmon Releases

	DRAM	Minimum ROMmon	Recommended ROMmon
C8500-12X4QC & C8500-12X	16GB(default)	17.2(1r)	17.11(1r)
	32GB	17.2(1r)	17.11(1r)
	64GB	17.3(2r)	17.11(1r)
C8500-20X6C	All variants	17.10(1r)	17.15(1r) **Important** Downgrading to a ROMmon version lower than 17.15(1r) is not supported.
C8500L-8S4X	-	17.10(1r) -	17.14(1r)* **Important** This version of ROMmon is only available with Cisco IOS XE 17.15.1a onwards

Note In case of C8500L-8S4X platform, the ROMmon image is bundled with the Cisco IOS XE software image which ensures that when the device is booted up, the ROMmon image is also automatically upgraded to the recommended version.

Table 9: What's New in the ROMMon Release

ROMmon Release for C8500-12X4QC, C8500-12X	Fixes
17.3(1r)	Supports 64GB DRAM for C8500-12X4QC & C8500-12X
17.10 (1r)	Added support for new platform C8500-20X6C

ROMmon Release for C8500L-8S4X	Fixes
17.14(1r)	CSCwf98337 - Evaluation of C8500L-8S4X for Intel 2023.3 IPU and SMRAM vulnerabilities CSCwe21026 - Evaluation of C8500L-8S4X for Intel 2023.1 IPU and SMM vulnerabilities

ROMmon Release for C8500-20X6C	Fixes
17.15(1r)	CSCwf98335 Evaluation of all_routing_iosxe for Intel 2023.3 IPU and SMRAM vulnerabilities. CSCwd96405 ASR 1000 BL and ML hashes not seen in the "Show system intergrity" CLI for Aikido based platformsAdditional minor fixes.

Related Documentation

- Hardware Installation Guide for Catalyst 8500 Series Edge Platforms
- Hardware Installation Guide for Catalyst 8500L Series Edge Platforms
- Smart Licensing Using Policy for Cisco Enterprise Routing Platforms
- Software Configuration Guide for Catalyst 8500 Series Edge Platforms

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business results 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.