Release Notes for Cisco Catalyst 8500 Series Edge Platforms, Cisco IOS XE Dublin Release 17.12.x

First Published: 2023-11-24

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 Dublin 17.12.1a is the first release for Cisco Catalyst 8500 Series Edge Platforms in the Cisco IOS XE Dublin 17.12.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
- C8500-20X6C

For more information on the features and specifications of Cisco 8500 Series Catalyst Edge Platform, see 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 explicitly made.

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.

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.

New and Changed Software Features in Cisco IOS XE 17.12.8

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.12.7b

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.12.6b

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.12.6

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.12.5d

There are no new features in this release.

New and Changed Software Features in Cisco IOS XE 17.12.5c

There are no new features in this release.

New and Changed Software Features in Cisco IOS XE 17.12.5b

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.12.5a

This release introduces support to update FPGA software for C8500-20x6C devices that use WAN MACsec for encrypting traffic across WAN networks.

For more information, see Upgrade FPGA for C8500-20x6C

New and Changed Software Features in Cisco IOS XE 17.12.4b

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.12.4a

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.12.4

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.12.3

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.12.2

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.

Table 1: New Software Features

Feature	Description
Cisco Managed Cellular Activation (eSIM)	The Managed Cellular Activation solution provides a programmable subscriber identity module (SIM), called an eSIM, a physical SIM card that you can configure with a cellular service plan of your choice. When ordering a pluggable interface module (PIM) to provide cellular connectivity for your router, choose a PIM model with a preinstalled eSIM. The Managed Cellular Activation solution comes with a "bootstrap" cellular plan to provide internet connectivity with a limited amount of data intended only for Day 0 onboarding of the device to your cellular plan. For information about configuring Cisco SD-WAN Manager with the details of your cellular plan in preparation for onboarding the device, see the Cisco Managed Cellular Activation Configuration Guide. Prepare the configuration in Cisco SD-WAN Manager before powering on and onboarding the device, to avoid running out of the limited data in the bootstrap cellular plan. Added Cisco Managed Cellular Activation (eSIM) support for the following Pluggable Interface Module (PIM) model: • 5G Sub-6 GHz PIM, model P-5GS6-R16-GL **Note** In this context, eSIM refers to a removable SIM pre-installed by Cisco. In other contexts, eSIM can refer to a non-removable SIM embedded in a cellular-enabled device.

New and Changed Software Features in Cisco IOS XE 17.12.1a

Table 2: Software Features

Feature	Description
Segment Routing over IPv6 Dataplane	Segment Routing (SR) can currently be applied on Multiprotocol Label Switching (MPLS) dataplane. From Cisco IOS XE 17.12.1a, SR is supported over the IPv6 dataplane for the following protocols:- • Interior Gateway Protocol (IS-IS only)- • Border Gateway Protocol (BGP) In addition, the following functionalities are available for Segment Routing over IPv6 dataplane: • Segment Routing Traffic Engineering Policies • Static Routes • Performance Management • Operations, Administration and Maintenance (OAM)

Feature	Description
TrustSec and Software-Defined Access Scale Measurement	With this feature, the scale numbers for TrustSec and Software-Defined Access (SDA) are measured for the following: • Security Group Tag (SGT) or Destination Group Tag (DGT) Policies • Unidirectional IPv4 SGT Exchange Protocol (SXP) connections • Bidirectional IPv4 SXP connections • IPv4 SGT Bindings • IPv6 SGT Bindings • Security Group Access Control Entries (SG ACEs)
IPv6 Unicast Support with DLEP	The IPv6 Unicast Support feature introduces support for IPv6 dataplane to RAR Dynamic Link Exchange Protocol.
Managing the SD-Routing Devices Using Cisco SD-WAN Manager	This feature allows you to perform management operations for SD-Routing devices using Cisco Catalyst SD-WAN Manager. You can use a single network manage system (Cisco Catalyst SD-WAN Manager) to monitor all the SD-Routing devices and therefore help in simplifying solution deployments.
Quantum-Safe Encryption Using Post-Quantum Preshared Keys	This enhancement introduces support for Quantum-Safe Encryption using Post-Quantum Preshared Keys for the following platforms: • Cisco 1000 Series Integrated Services Routers • Cisco Catalyst 8500 Series Edge Platforms
Support for Automatic Log Deletion	This feature allows you to delete the entries from the logging buffer. You can configure the local syslog retention period after which the entries are purged from the device automatically. To enable this feature, use the **logging purge-log buffer days** command.

Resolved and Open Bugs for Cisco IOS XE 17.12.8

Table 3: Resolved Bugs for Cisco IOS XE 17.12.8

Identifier	Headline
CSCwu02602	DBAL EVENTS crash seen while trying to push config group to device in SDWAN and SD-Routing.

Identifier	Headline
CSCws75769	Netconf process doesn't start on 9130 AP in EWC mode and generates repeated dmiauthd subscription failures for invalid route-map YANG path.
CSCws80808	Loopback interface in Mgmt-intf VRF becomes unreachable via Management interface.
CSCwt87294	mDNS Cache-Flush behavior not consistent.

Open Bugs for Cisco IOS XE 17.12.8

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

Resolved and Open Bugs Cisco IOS XE 17.12.7b

Table 4: Resolved Bugs for Cisco IOS XE 17.12.7b

Identifier	Headline
CSCwr83968	Unexpected reload on device with static NAT when polling NAT translation data
CSCwo57783	NHRP encap error for purge request populates on spoke despite correct routing at the hub
CSCwn85623	Missing calling-station-ID in radius messages
CSCwm62981	Device crashes with PKI revocation-check ocsp none enabled
CSCwp96706	Memory leak in MallocLite and Crypto IKEv2
CSCwq22471	Device May Unexpectedly reboot when importing CA chains
CSCwq21566	HSL entries are missing when config is pushed via vManage
CSCwq51358	Device may experience high memory utilization and unexpected reloads during IKEv2 operations
CSCwn18874	DMVPN spoke crashed at process = NHRP
CSCwo14975	Memory leak in DNS Proxy/SKA triggers unexpected reloads
CSCwj88080	Device continuously crashes after configuring UTD and rebooting
CSCwp40010	RP crash while debugging IKEv2
CSCwp38609	CTS trustpoint loop triggers PKI segfault
CSCwq49981	Call Failures due to FPI resource leaks in 17.12.6

Table 5: Open Bugs for Cisco IOS XE 17.12.7b

Identifier	Headline
CSCws33718	Unicast packets dropped ingress on port-channel sent from Nexus vpc after clearing vpc inconsistency

Identifier	Headline
CSCwr00088	Add CLI to change per MPLS label CEF statistics query interval on FMAN FP
CSCwn29062	Device may see cosmetic datacorruption logs during IPSec tunnel up and down events
CSCwk55051	polaris_vconfd_cfgpull_t denials during config push trigger
CSCwm54978	Polaris_iosd_t denials
CSCwk22312	Input errors and overrun on port channel interface and physical interface

Resolved and Open bugs for Cisco IOS XE 17.12.6b



Important The Cisco IOS XE 17.12.b release is applicable for C8500 Edge Platform only.

Table 6: Resolved Bugs for Cisco IOS XE 17.12.6b

Identifier	Headline
CSCwr90843	Device Crash in cpp_cp_svr process with heavy IPSec traffic load

Open Bugs for Cisco IOS XE 17.12.6b

There are no open bugs in this release.

Resolved and Open bugs for Cisco IOS XE 17.12.6

Table 7: Resolved Bugs for Cisco IOS XE 17.12.6

Bug ID	Headline
CSCwp03641	Multiple inside local addreses are translated to same inside global IP address and port
CSCwo91955	Endpoint tracker remains up status when DNS is reachable from the other interface
CSCwn99822	Large number of BFD sessions stuck due to out of window drops reported with control connections NAT flaps
CSCwp28915	SNMPwalk fails to consistently return tunnel names due to incomplete tunnel setup
CSCwo89784	Unexpected reload of standby during PKI Trustpoint removal
CSCwn99723	Deprecate **request platform software package expand** commands for upgrades
CSCwp12923	IKEv2 fails to parse certain route-set prefix Cisco VSA attributes from Radius server
CSCwo47118	Crash when clearing L2TP tunnels with the command **clear vpdn tunnel l2tp**
CSCwb24403	BFD flap on public IP change on a private color tloc
CSCwo66822	Device reloaded with reason: Critical process cpp_ha_top_level_server fault on fp_0_0 (rc=69)
CSCwo90396	Serial interface configuration lost after reload

Bug ID	Headline
CSCwm33545	FlexVPN - IP address assigned to spoke changes to unassigned
CSCwo12453	Configuring "access-class xx in vrf Mgmt-vrf" on line vty causes the Login Block" to be inactive
CSCwo51627	Unexpected reload due critical process linux_iosd_image fault on rp_0_0 (rc=139)
CSCwn39832	Adding authorization bypass to vDSP EEM scripts
CSCwo03915	Unexpected reload on device due to performance monitor with packet service insertion from spoke
CSCwp81333	Cache coherency rare timing race condition
CSCwo15543	Functional standby reloads after upgrade
CSCwk56650	Unexpected reboot during dialer initialization
CSCwj27134	**ip vrf receive** command adds connected route to vrf table even though interface admin down
CSCwo34430	Device drops protocol sessions upon executing how memory command
CSCwk25731	Device flaps more than once when interface is bounced
CSCwo99641	Out of CGM (Class-Group Manager) memory intermittently with scaled ZBFW policy
CSCwn37412	NTP will not authenticate with open source NTP servers using 32B cmac-aes-128
CSCwk05523	Device crashes with bad magic number in chunk header, with ACL logging hash-generation
CSCwo05166	Memory leak on Chunk Manager via DBAL EVENTS process
CSCwm01063	Unexpected reload due to Segmentation fault on IP SLA DynHostName Process
CSCwp59954	Unexpected reboot on IOS-XE due prune on mcast
CSCwn13851	Device reports %SCOOBY-5-SERIAL_BRIDGE_BLOCK_EVENT error logs
CSCwo70548	Ping failure from VRRP backup to VRRP primary virtual address when enabling security policy
CSCwp35552	Missing Calling-Station-ID (31) in Radius accounting
CSCwn24036	Tx/Rx optical power values diffrent for **show int** and **show hw-module**
CSCwn92855	Breakout port fails to initialize
CSCwn18584	Tracebacks seen on device while applying config on a clean router
CSCwn54648	High CPU on Virtual EXEC and TTY Background
CSCwj60804	ACL delete and reapply removes PBR mapping but TCAM is populated
CSCwo22585	Device crashes when running a NWPI trace initiated from vManage
CSCwi59338	Enable strict-kex support in IOS-SSH
CSCwn92976	PPP is not establishing when L2TP over IPsec
CSCwn59814	FLOWDB_OOM condition can lead to packet loss with GRE non-IPSEC tunnel
CSCwn60286	Memory Leak observed in IPSEC/IKE session bringup with cert-based authentication

Bug ID	Headline
CSCwp15054	Memory leak in nbar-sdavc-scheduler
CSCwo84747	Tunnel delete/create flaps unexpectedly for PWK case for private control NAT changes
CSCwn43979	Overruns caused by extended AR window feature
CSCwn15850	Crash when "show running-config full | format" begins to print QoS Policy-map config
CSCwo13544	QFP Crash in device due to move function while processing flows
CSCwn50935	Crash occurs during haripin call
CSCwo98465	Crash when receiving BGP MVPN update/withdraw with BGP MVPN update debug enabled
CSCwq01226	ESP crash
CSCwn93483	confd_cli high cpu utilization after executing **show zbfw-dp sessions**
CSCwq31287	Cisco IOS and IOS XE Software SNMP Denial of Service and Remote Code Execution Vulnerability.
CSCwn98779	Multihome DC publication has inconsistent domain and mh id

Table 8: Open Bugs for Cisco IOS XE 17.12.6

Bug ID	Headline
CSCwn85623	Missing calling-Station-ID in radius messages
CSCwq22471	Unexpected reload after importing subca chain
CSCwp01089	EPFR-High latency times are observed on the hub device
CSCwq08151	Unexpected reload while running a speed test and leaving the page before it completes
CSCwo57783	NHRP encap error for purge request populates on spoke despite correct routing at hub
CSCwm54978	Selinux: polaris_iosd_t denials 2024-09-16 06:43:22
CSCwp40010	RP crash while debugging IKEv2
CSCwp38609	CTS trustpoint loop triggers PKI segfault

Resolved and Open Bugs for Cisco IOS XE 17.12.5d

Table 9: Resolved Bugs for Cisco IOS XE 17.12.5d

Identifier	Headline
CSCwo38924	Cisco IOS XE Software Secure Boot Bypass Vulnerability
CSCwo38903	Cisco IOS XE Software Secure Boot Bypass Vulnerability
CSCwn48408	Cisco IOS XE Software HTTP API Command Injection Vulnerability
CSCwm57073	Cisco IOS XE Software WebUI Reflected Cross-Site Scripting Vulnerability
CSCwm41327	Cisco IOS XE Software CLI Argument Injection Vulnerability

Identifier	Headline
CSCwm99306	Cisco IOS and IOS XE Software TACACS+ Authentication Bypass Vulnerability
CSCwp03900	Cisco IOS XE Software Simple Network Management Protocol Denial of Service Vulnerability
CSCwq31287	Cisco IOS and IOS XE Software SNMP Denial of Service and Remote Code Execution Vulnerability

Open Bugs for Cisco IOS XE 17.12.5d

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

Resolved and Open Bugs for Cisco IOS XE 17.12.5c

Identifier	Headline
CSCwp81333	Cache coherency rare timing race condition
CSCwp66926	FNF AOR might have double-free risk
CSCwo19997	QFP crash with stuck threads while attempting to lock cft policy under autonomous mode

Resolved and Open Bugs for Cisco IOS XE 17.12.5b

Resolved Bugs for Cisco IOS XE 17.12.5b

Identifier	Headline
CSCwo67161	IPsec-related crash on an IOS-XE device

Open Bugs for Cisco IOS XE 17.12.5b

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

Resolved and Open Bugs for Cisco IOS XE 17.12.5a

Table 10: Resolved Bugs for Cisco IOS XE 17.12.5a

Identifier	Headline
CSCwn22830	vDSP container network mask mismatches with VPG interface
CSCwm80356	LLDP packets dropped when came through active port-channel interface
CSCwm75361	MACSEC XPN on 100G intf traffic not flowing after sometime
CSCwk44078	GETVPN / Migrating to new KEK RSA key doesn't trigger GM re-registration

Identifier	Headline
CSCwk26247	QFP stuck threads crash while handling netflow features under Autonomous mode
CSCwk42190	Config and dp show command don’t match the dp oper output
CSCwj06950	DSL module gets stuck in a booting state
CSCwf79399	Port-channel sub-interface overload. Port-channel interface must be created first and delete
CSCwj80411	Deleting and adding the rules in a ZBFW policy with 510 rules results in traffic drop
CSCwf77488	IOSd crash after device boot up and online
CSCwn38920	Very intermittent, 1 of many 40/100G session stuck (secured, but no traffic)
CSCwn14549	Traffic gets dropped at MAC as mac_filter drop
CSCwm14462	IPv6 flowspec nexthop redirect policy not redirecting the traffic on IOS XE
CSCwm05524	Unexpected Reload due to cpp-mcplo-ucode process when handling fragments with SRv6 routing
CSCwk53892	MKA session secured but ping is not working intermittently
CSCwj84949	Unencrypted traffic due to non-functional IPsec tunnel in FLEXVPN hub & spoke setup
CSCwn07540	Device crashed due to IOSXE_INFRA-2-FATAL_NO_PUNT_KEEPALIVE
CSCwk85577	Traffic goes through on non-MACSEC subintf on 10G intf with must-secure on mainintf
CSCwm98642	OMP is redistributing summary routes in the service VPN even though the exact networks don't exist.
CSCwn15231	Null-way audio within the same layer2
CSCwk53680	Inbound calls results in phantom calls
CSCwk65485	Flap MACSec on one interface causes bfd flap on unrelated macsec interface after reload.
CSCwk88589	Ping stops working on interface at 127th iteration of remove and add interface
CSCwi96187	Modem firmware upgrade failing
CSCwk79454	Endpoint tracker does not fail if default route is removed
CSCwo14912	Replay window programming errors may cause transient protocol flaps (e.g. ISIS)
CSCwk61238	RRI static not populating route after reload if stateful IPSec is configured
CSCwk75459	MGCP GW fails to respond with 250 OK when there's a delay from dataplane in gathering stats

Identifier	Headline
CSCwk87452	Procyon synchronize DTL does not wait until complete due to compiler optimization
CSCwk86973	MACSec session stays secured but traffic doesn't flow intermittently
CSCwm76255	With XPN policy configured, rekey still happening frequently
CSCwk50035	Unrelated MACsec go down on configuring macsec on a sub-intf
CSCwm52807	Hub devices reloaded due to UCode crash
CSCwm07396	Few BFD sessions down after clear mka session on client
CSCwh89618	CRC errors seen with MACsec enabled on 100 G ports
CSCwo55206	ISIS hellos drops as delayed packets cause ISIS flap over MACsec interface
CSCwm78956	Device crashes with QFP interrupt
CSCwn65163	BFD session stuck over the MACsec tunnels
CSCwj76501	Data plane crash in ERSPAN processing
CSCwk36578	Packet drops on MACsec enabled sub-interace has Vlan Identifier above 255
CSCwj63794	After SAK rekey, MACSEC session stays secured but traffic stops working
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
CSCwm91175	OOD subscribe with event message-summary is causing memory leak
CSCwm79956	Memory leak under dead caused by AFW_application_proc
CSCwm08791	Dial-peer never recovers an active state if it goes partial or busyout.
CSCwm91190	MWI app not registering on Vcube
CSCwi77331	IOS-XE unexpected reboot after **show sip-ua connection**
CSCwk44855	Cannot dial to/from phone after it reboots in survivability mode
CSCwm01029	CUBE gets forked 180 and 183 with SDP, CUBE is not adding SRTP key when sending 183, causing failure
CSCwm03319	Optimize voip trace handling with tenants
CSCwm32946	CUBE doesn't relay/pass 488 media unacceptable from one leg to another leg for FAX (T.38) Re-INVITEs

Identifier	Headline
CSCwm39795	HA Module DSP_MSP reported failure on standby
CSCwm47634	No audio issue on call transfer and conference
CSCwm73825	Crash observed on device, while performing the conference call
CSCwm79213	mfPthruCrypto NULL showing up excessively in the log
CSCwm82247	CUBE memory leak for SIP out-of-dialog subscriber
CSCwn09710	Memory leak under dead caused by AFW_application_proc
CSCwn13988	CDR file accounting credentials exposure
CSCwn19326	CDR file accounting creates dummy files
CSCwn48914	Device crash during SGW sync in process
CSCwn60303	SIP-ua commands lost after reload
CSCwn49403	Device incorrectly offers rtp instead of srtp in 200 OK for SRTP fallback scenario

Table 11: Open Bugs for Cisco IOS XE 17.12.5a

Identifier	Headline
CSCwn92855	Breakout port fails to initialize
CSCwn97600	Some BFD flapping on PWK ipsec-rekey on all devices
CSCwo55262	Breakout 10g interfaces reported as invalid input upon device reload
CSCwe23188	Upgrade from vmanage declared successful even though device boots up with different version than requested.
CSCwk87338	SNMPv3 user credentials to be stored as part of running-configuration with encryption.

Resolved and Open Bugs for Cisco IOS XE 17.12.4b

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

Resolved and Open bugs for Cisco IOS XE 17.12.4a

Table 12: Resolved Bugs for Cisco IOS XE 17.12.4a

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

Identifier	Headline
CSCwm60651	HTX: UTD snort crash at memif_shm_peek_first_packet (handle=0x0)
CSCwk84047	Memory leak due to security violation by new MAC address and Del Pend object increases - ACE_IPV4
CSCwk54544	ZBFW TCAM misprogramming after rules are reordered on device
CSCwk50488	Memory leak in fman_rp under acl_db
CSCwk45165	fman_fp Memory Leak on device

Open Bugs for Cisco IOS XE 17.12.4a

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

Resolved and Open bugs for Cisco IOS XE 17.12.4

Table 13: Resolved Bugs for Cisco IOS XE 17.12.4

Bug ID	Description
CSCwj70335	Crypto IKEv2 fragmented authentication packets detected as malformed on third party vendor device.
CSCwj44868	GETVPN COOP KS - Wrong severity for rekey acknowledgement configuration mismatch log message.
CSCwi86227	Device reports incorrect DOM values over SNMP.
CSCwi56804	FlowDB Exhaustion
CSCwi16716	Device crashed upon increasing the gatekeeper cache size.
CSCwi88969	Error observed when delete and configure zone-pair back.
CSCwj21653	Kernel crash over continuous reloads.
CSCwi68865	Memory leak in Crypto IKEv2 .
CSCwj09284	Unexpected reboot in device due to SSL.
CSCwj88872	IPSec tunnel fails to establish due to error IPSec policy invalidated proposal.
CSCwi40603	Memory leak in the Crypto IKMP process.
CSCwi82405	mGRE Tunnels with shared IPSec profile cause ucode crash.
CSCwj53986	Extremely poor DMVPN performance on device with TrustSec.
CSCwj34578	NAT46 translations are dropped when NAT64 router is also Carrier Supporting Carrier CE.
CSCwi55183	crypto pki certificate pool in running configuration.

Bug ID	Description
CSCwk15127	Failure to communicate a period of time after the stp status changes.
CSCwh37024	Device PnP gets stuck when cellular backhaul is used.
CSCwj45130	Segmentation Fault - Process IPSec dummy packet process.
CSCwj42249	Disabling PMTU-Discovery with MTU change and BFD flap breaks packet duplication.
CSCwj73113	MGCP GW doesn't respond with 250 OK for a DLCX leading to DLCX loop from CUCM side.
CSCwi59854	**show sdwan policy service-path** command gives inconsistent results with app name specified.
CSCwi89510	Device flow causing overruns.
CSCwh73320	NAT Pool doesn't working under prefix 16.
CSCwi89822	Unexpected reboot due cpp ucode on device.
CSCwh86053	Config Parser Issue for NAT with extendable and redundancy.
CSCwj38106	Only one split-exclude subnet is pushed to client PC with headend for a RA VPN connection.
CSCwj36915	MACsec not working under LACP port-channel member port.
CSCwi78365	Trim installed certificate on upgrade.
CSCwj72888	Reload in tcp_sanity due to l4 pointer not set.
CSCwi93784	FW upgrade does not work properly.
CSCwj33292	IPSec fails when connecting from an RDP user.
CSCwj06622	Segmentation fault and core files are seen in controller-managed device.
CSCwi16111	ipv6 tcp adjust-mss not working after delete and reconfigure.
CSCwj29947	AAA authorization failure during IKEv2 phase negotiation caused unexpected reboot.
CSCwd17906	Device overrun errors on interfaces.
CSCwj04575	Router crashed during SNMP walk when removing SFP.
CSCwj24511	Tunnel QoS incorrect IP precedence classification with MPLS EXP.
CSCwi56114	Secure datawipe should reset the configuration register.
CSCwi80286	100G interface with QSFP 40/100GE SRBD continuously flaps when configured 40G speed.
CSCwf87975	Router crashed when port-channel interface flap with scale of per-tunnel QOS policies.

Bug ID	Description
CSCwj30334	Device rebooted when attempting merge .
CSCwi62239	%IOSXE_MGMTVRF-3-INTF_ATTACH_FAIL error after configuring loopback managment .
CSCwj05013	CUBE Media Proxy(CMP) dual forking not working after upgrade
CSCwj23804	Password created with **key config-key password-encrypt** ending with a "\" are lost after reload
CSCwj59262	SIPREC Secure media forking -1 of 2 audio streams is encrypted due to same key sent for both streams
CSCwj61168	Device experiences memory leak in ucode_pkt_PPE0 process
CSCwi69071	Unexpected reload caused by crash
CSCwh81312	No memory seen in standby device while checkpointing.
CSCwj23735	RTP port range configuration lost under **voice service voip** after reload
CSCwj26668	IOS XE wrong audio rtp packet marking for SCCP SRST
CSCwj41553	SGW calling to TDM, AOR is not getting changed to number
CSCwj54666	SIP cause code incorrect for CCAPI cause code 31
CSCwj75508	SRST running on device fails to register SCCP phones after reload
CSCwj82258	Device may crash during transfer call flow in SRST
CSCwj93967	History-Info header compatibility between CUBE and MS Direct Routing
CSCwj95128	Incorrectly change dtmf payload in asymmetric case
CSCwj98360	Media forking not working in CUBE
CSCwk08864	**authentication** command under dial-peer is missing challenge

Table 14: Open Bugs for Cisco IOS XE 17.12.4

Bug ID	Description
CSCwi03502	Create CLI to configuring Multi-PDN.
CSCwk31560	NAT command not readable after reloaded.
CSCwk44078	GETVPN / Migrating to new KEK RSA key doesn't trigger GM re-registration
CSCwk26247	QFP stuck threads crash while handling netflow features under Autonomous mode.
CSCwj06950	DSL module gets stuck in a booting state.
CSCwj21653	Kernel crash over continuous reloads.

Bug ID	Description
CSCwk58303	Watchdog crash during IPv6 CEF adjacency routine.
CSCwk63722	Startup configuration failure post PKI server enablement.
CSCwj77594	WAN IP is allowed to be configured as system IP.
CSCwk25731	Device flaps more than once when interface is bounced with SRBD optics
CSCwk54544	TCAM misprogramming after rules are reordered on device
CSCwj76501	Data plane crash in ERSPAN processing.
CSCwj84949	Unencrypted traffic due to non-functional IPSec tunnel in FLEXVPN Hub & Spoke setup
CSCwi56641	Device reports link-flap error when peer reloads
CSCwk20583	Interfaces with breakout configurations flap after reload.
CSCwj90614	High CPU utilisation for confd_cli
CSCwk03686	Crash due a segmentation fault due a negative value.
CSCwj92560	STCAPP command removed after reload
CSCwk31715	After deleting a NAT configuration, the IP address still shows up in routing table.
CSCwh45389	Key manager crash after hostname change with usage keys.
CSCwk12524	Device reloaded due to ezManage mobile app service.
CSCwk53680	Inbound calls results in phantom calls
CSCwk65071	Unexpected reboot due to IOSXE-WATCHDOG DBAL EVENTS after Cellular interface flap
CSCwf91481	IR1835 crashed unexpectedly after a successful WGB/AP config deployment from OD
CSCwi96187	P-5GS6-GL FN980 modem fW upgrade failing when two modems onIR1800
CSCwh91136	IOS XE:Traffic not encrypted and droped over IPSEC SVTI tunnel
CSCwk52677	C1118-8P / DSL router crashing due to %PLATFORM-3-ELEMENT_CRITICAL memory level / iomd process
CSCwb47658	Repeated and endless messages "Network change event - activated 4G Carrier Aggregation."
CSCwh89618	C8500-20X6C: CRC errors seen with macsec enabled on 100G ports
CSCwk30527	IKEv2 session is down after reload if identity local address is assigned to interface on Switch

Bug ID	Description
CSCwk22312	C8500-12X & C8500-12X4QC: Input errors and overrun on Port Channel interface and Physical Interface
CSCwi31110	Traceback seen @_nhrp_cache_delete due to negative global cache count.
CSCwk33173	EzPM application-performance profile may cause memory leak with certain long-lived idle TCP flows.
CSCwk52106	SNMP reports incorrect transmit power / receive power values for 100G AOC cables.
CSCwj86794	Device crashes while processing an NWPI trace.
CSCwk22942	Unable to build two IPSec SAs where one peer has PAT set up.
CSCwk56504	In NAT64 scenario, IPv4 packets that needs translation might be dropped by device.
CSCwk57979	emd fault on cc_0_0 (rc=134) due to ensor has exceeded it's maximum number of read errors.

Resolved Bugs - Cisco IOS XE 17.12.3a

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

Bug ID	Description
CSCwk21189	Template attach fail with unknown element: ssh-version in /ios:native/ios:ip/ios:ssh
CSCwk20843	PPPoE with NAT DIA feature validation failed post upgrade.

Resolved and Open bugs for Cisco IOS XE 17.12.3

Table 15: Resolved Bugs for Cisco IOS XE 17.12.3

Bug ID	Description
CSCwh73350	Device keeps crashing when processing a firewall feature.
CSCwh18120	The diagnose feature for IKEv2 is consuming 11% CPU during the session initiation phase.
CSCwh68508	Unexpected reboot after establishing the control plane of EVPN MPLS and receiving packets.
CSCwi28227	NAT HSL logging with VRF filtering is not functioning correctly.
CSCwh22414	Warning and critical CPU utilization thresholds are not recalculated when using data-plane-heavy mode.
CSCwi01046	PoE module does not provide sufficient power to activate the ports after an unexpected reload.

Bug ID	Description
CSCwh77221	SNMP unable to poll tunnel data after a minute.
CSCwh96578	SKA_PUBKEY_DB leak in TDL.
CSCwh69765	Security policy with IPS external syslog configuration fails to generate for specific devices.
CSCwi06843	Endpoint tracker triggers a CPU Hog.
CSCwh87619	ZBFW is unable to detect packets on TenGig interface for device.
CSCwh10813	Add verbose log to indicate grant when grant ra-auto configuration unconfigures grant auto in the PKI server.
CSCwi60312	Device can't boot up in full configuration.
CSCwh93257	Device creates incorrect NAT entry if two or more IP phones from NAT outside register to the same server.
CSCwi59121	Mobile application causing excessive authorization attempts with a null username on a specific device.
CSCwi08171	Device may crash due to Crypto IKMP process.
CSCwi49231	Audio loss experienced for four seconds on a Voice Gateway device.
CSCwi06404	PKI service crash following an unsuccessful CRL fetch.
CSCwh50510	Device crash with segmentation fault (11), Process = NHRP when processing NHRP traffic.
CSCwh75800	Device unexpectedly reloads during Trustpool retrieval for SIP TLS certificate.
CSCwi28781	EPBR generates an error when the policy is added and deleted multiple times.
CSCwi49240	One-way RTP issue including DSP timeout messages (63.2.0 / 62.3.1).
CSCwh45169	Unexpected reboot while displaying information from a cleared SSS session.
CSCwh70449	PMTUD is not properly converging as it does not attempt to learn a higher MTU value.
CSCwh96415	Inability to disable DMVPN logging on recent software versions.
CSCwi25737	Device should discard IKE Notification messages with incorrect DOI.
CSCwh50628	Race condition crash on device.
CSCwf86207	Frame Relay DTE device crashes due to EXMEM exhaustion.
CSCwh72869	cpp_mcplo_ucode crash with Port-channel and NAT configurations.
CSCwh99399	ftmd crash observed in ENCS platform while running PWK suite.

Bug ID	Description
CSCwi76087	ATO: Session fails to come up when the tunnel is repeatedly shut and no shut (similar to a customer unplugging and replugging a cable).
CSCwi55379	IPSec traffic is being dropped strongSwan when PPK is implemented.
CSCwi63042	Packet drops observed between LISP EID over GRE Tunnel.
CSCwi79584	Upgrade failure on a device via management system due to a system configuration error.
CSCwi30529	AAA template push fails when AAA authorization is configured for local use.
CSCwh62116	Performance improvement for packet duplication.
CSCwi05232	Traceback observed when a Dialer interface is not present or a peer is down.
CSCwh22451	Packets appeared out of order when using Embedded Packet Capture on the device.
CSCwh85803	MACsec session is in the secured state but remains stuck without transmitting any traffic.
CSCwh28680	Packet duplication performance improvement in device.
CSCwi58732	IPSec FlowDB showing duplicate flow entries.
CSCwh32386	Unexpected reload on device due to a critical process fman_fp_image.

Table 16: Open Bugs for Cisco IOS XE 17.12.3

Bug ID	Description
CSCwi03502	Create CLI push followed with reboot required when configuring Multi-PDN on a device.
CSCwj08744	Unexpected reload when using **show running-config full | format** command.
CSCwi16111	IPv6 TCP adjust-MSS not working after deletion and reconfiguration.
CSCwi46997	NAT command not readable after reload.
CSCwi67621	Critical process cpp_ha_top_level_server fault on fp_0_0 (rc=69).
CSCwh89618	CRC errors observed with MACsec enabled on 100G ports.

Resolved and Open bugs for Cisco IOS XE 17.12.2

Table 17: Resolved Bugs for Cisco IOS XE 17.12.2

Bugs	Description
CSCwh96700	Carrier Grade NAT reaching max host entries and failing to translate due to gatekeeper

Bugs	Description
CSCwf74668	HSEC licenses incrementing
CSCwf65696	Non-fabric load the minimal bootstrap configs again if device rebooted without saving the configs
CSCwh87343	Cisco IOS XE Software Web UI Privilege Escalation Vulnerability. For more information, see Security Advisory: cisco-sa-iosxe-webui-privesc-j22SaA4z
CSCwf67564	Device observes memory leak at process SSS Manager.
CSCwf60151	Memory leak with pubd.
CSCwh60190	**ip name-server** command not pushed.
CSCwf56463	IOS process crash during VRRP hash table lookup.
CSCwh11858	Device running IOS-XE crashes when removing FQDN ACL.
CSCwf99906	NTP authentication removed after reload using more than 16 bytes.
CSCwf59173	Segmentation fault at IPv6 BGP backup route notification.
CSCwf67351	Cisco IOx application hosting environment privilege escalation vulnerability.
CSCwf68612	WLC unexpected ueload due to segmentation fault in WNCD process.
CSCwh00963	Unable to migrate from ADSL to VDSL without reboot.
CSCwf41084	Extranet multicast code improvements for better handling of data structure.
CSCwh04884	VC down due to control-word negotiation.
CSCwf26494	BDI + NTP configuration puts DMI process in degraded mode.

Table 18: Open Bugs for Cisco IOS XE 17.12.2

Bugs	Description
CSCwh84068	Device crashes after changing NAT HSL configuration.
CSCwh80341	Upgrade from device boot level is not preserved
CSCwh71278	Device license boot level config lost in running-config after upgrade
CSCwh74249	IPv6 PMTUD packet is fragmented at 1494 bytes
CSCwh98527	Device match ICMP traffic to VRF 65528 causing ping to not be completed
CSCwh58252	IPv6 SPD min/max defaulting to values 1 and 2.
CSCwh14083	High CPU due to MPLS MIB poll.
CSCwh22981	WNCD process crashes.

Bugs	Description
CSCwh99513	VPLS IRB not working when traffic came from VPNv4 and next-hop is learned over VPLS.
CSCwh90851	pubd process showing high CPU utilization.
CSCwh83532	1Gig int on device using GLC-SX-MMD are down after changing connection.
CSCwh96891	Memory leak with pubd.
CSCwh91085	Convergence improvement after device reboot with mVPN profile 14.
CSCwh58919	NETCONF: DMI enters degraded mode caused by BGP neighbor configured under the SCOPE command.
CSCuu85298	FIB/LFIB inconsistency after BGP flap.
CSCwf83684	IOS XE router may experience "%FMANRP_QOS-4-MPOLCHECKDETAIL:" errors.
CSCwh59926	EEM is running daily instead of weekly or monthly if special strings @weekly or @monthly are used.
CSCwh24280	Mismatch between the resource allocation and "app-resource profile custom" configuration.
CSCwh82668	Incorrect local MPLS label in CEF after BGP flap.
CSCwh95036	Cisco IOS-XE IPv6 based subscription telemetry does not work.
CSCwh99464	Guestshell connectivity not working with NAT overload.
CSCwh30928	SDA - using spt-threshold infinity and having LHR+FHR can cause the S,G to be pruned on the RP.
CSCwh01738	Unexpected reload when using rsh/rcmd.
CSCwh04124	Locally generated traffic received on incorrect interface inbound and dropped by ACL.
CSCwh67285	WLC unable to get telemetry data due to pubd unexpected reload and fail.
CSCwh96332	Device crash due to dhcpd_binding_check.
CSCwh56940	Site tag change wncd working/failing EAP-TLS.
CSCwh44418	ARP incomplete in VRF Mgmt-intf - G0/0/0 - Switch -G0.
CSCwh46559	LLDP location information not sent when configured.
CSCuv36790	**clear bgp** command does not consider AFIs when used with update-group option.
CSCwh02698	Device sending incomplete SGT to ISE.
CSCwh05869	Only portion of HSRP config being pushed via CLI ADDON template.
CSCwf53750	"match pktlen-range" does not work with GRE/IPSEC GRE.

Bugs	Description
CSCwh60107	In the show tech file, enable secret does not get hidden.
CSCwh45579	Unexpected reload on device ucode core @l2_dst_output_goto_output_feature_ext_path.
CSCwh95024	ISIS crash in local uloop.
CSCwh41155	Wrong /32 self, complete map-cache entry for fabric hosts on iBN when overlapping summary exists.
CSCwh31485	Member interface config not applied with mis-match in pcakages.conf files.
CSCwh72437	WLC not sending accounting start for user auth after machine auth on 9105AXW RLAN dot1x port.
CSCwi00680	Router unexpectedly reloads while using DHCP for ISG.
CSCwh96823	IOS-XE router not installing classless-static-routes from DHCP option 121.
CSCwh77706	SVL, 10G link on the active chassis will go down after reload.
CSCwh02592	Device sync fails when device prompt comes along with device banner and TACACS is used.
CSCwh84850	Unexpected reboot in device due to SISF and STP initialization.
CSCwh64903	Crash on device polling SPA sensor data.
CSCwh53432	VLAN name mismatch when authorizing vlan name from radius server and enable vlan fallback.
CSCwh21796	Password getting visible for the mask-secret in show logging.
CSCwh50104	Upgrade failing with config check track-id-name.
CSCwf59929	CTS CORE process crash after configuring role based ACL.
CSCwh81471	IPv6 traffic is passing through when the client is in Webauth Pending state (CWA).
CSCwh93772	Option 121 never requested by IOS-XE client.
CSCwh06087	[IPv6 BGP] multiple sourced paths present for the same prefix.
CSCwh29120	IP SPD queue thresholds are out of range.
CSCwh14953	CBQoS polling for the object cbQosCMPostPolicyBitRate returns incorrect value.
CSCwh89096	Device unexpected reload.
CSCwh99597	After migration MAC/IP only MAC is advertised.
CSCwh75992	BGP Router process crash.
CSCwh48058	Memory leak under MallocLite/AAA proxy with NETCONF/RESTCONF.

Bugs	Description
CSCwh76920	Memory leak in linux_iosd-imag due to SNMP.
CSCwh75112	After a reboot, EAP-FAST/PEAP does not authenticate unless credentials are changed.

Resolved and Open Bugs for Cisco IOS XE 17.12.1a

Resolved Bugs for Cisco IOS XE 17.12.1a

Bug ID	Headline
CSCwe82666	Not all HSL entries get pushed to device if more than 1 HSL entries are configured
CSCwe31226	Issues/discrepancies around CPU alarms generated and sent to device
CSCwe43341	TLS control-connections down, traffic from device dropped
CSCwe18124	MACsec remains marked as secured, but the traffic randomly stops working
CSCwe18276	Route-map not getting effected when its applied in OMP for BGP routes
CSCwf83850	With Pure IPv6, minimal bootstrap unable to onboard non-fabric - IPv6 config missing in WAN int G1
CSCwb74821	Unexpected behavior due to unstable power source
CSCwe79007	Unexpected reload when doing ips test with UTD ips engine
CSCwe81182	(EPC, packet-trace) for IPsec running COFF (Crypto Offload)
CSCwe38296	Procyon packets drop due to MACsec post-encryption padding behavior
CSCwe93905	NAT ALG is changing the Call-ID within SIP message header causing calls to fail
CSCwe85195	AAR: BoW feature ignoring color preference from Tiered Transport preference configuration
CSCwe14885	VPN is established although the peer is using a revoked certificate for authentication
CSCwd53710	Crash seen when name_lookup takes > 30 sec
CSCwe66318	NAT entries expire on standby router
CSCwd35047	Failed to ping gateway while configuring SharedLOM with console , te1 interface. until router reload
CSCwd84599	Dataplane memory utilization issue - 97% QFP DRAM memory utilization
CSCwd59722	Unexpected reboot due to IOSXE-WATCHDOG: Process = Crypto IKMP
CSCwe70374	Platform punt-policer is not configurable
CSCwf05405	Traceback seen after BDI interface is configured
CSCwe73408	For some error condition platform_properties may double free
CSCwd42523	Same label is assigned to different VRFs
CSCwe37123	Device uses excessive memory when configuring ACLs with large object groups
CSCwe12194	Auto-Update cycle incorrectly deletes certificates

Bug ID	Headline
CSCwd90056	C8500-12X4QC : P2MP WAN MACsec does not allow traffic to pass on the link
CSCwe09298	C8500L sees the increase of input errors without any other specifc errors increasing under **show interface**
CSCvz82148	%CRYPTO_SL_TP_LEVELS-6-VAR_NEW_VALUE message is observed in each write config with same crypto value
CSCwe85421	BFD session down with interface flap
CSCwe95606	Double GR_Additional log enablement defect
CSCwe31471	Segmentation fault in device when per-tunnel QoS config withdraw
CSCwe89404	No way audio when using secure hardware conference with secure endpoints
CSCwd39257	IOS-XE cpp crash when entering **no ip nat create flow-entries**
CSCwe63222	Certificate output is not getting changed on renew when Cloud Certificate Authorization is Automated
CSCwe70642	AAR overlay actions are applied to DIA traffic
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
CSCwe31281	Autotunnel Ipsec tracker:Tracker does not come up at all on device
CSCwe39157	During soak run, On C8500L-8S4X, Memif channel's were missing and causing SC-SN state down
CSCwd93401	AppNav-XE: Policy-map edit on cluster with multiple service context fails to program TCAM
CSCwf65696	Non-fabric- Load the minimal bootstrap configs again if device rebooted without saving the configs
CSCwd76648	Port-channel DPI Load-Balancing not utilizing all the member-links
CSCwe39011	GARP on port up/up status from device is not received by remote peer device
CSCwb39206	Enable VFR CLI
CSCwe85022	Device is showing 4 additional NR bands support - 1, 3, 7, and 28

Open Bugs for Cisco IOS XE 17.12.1a

Bug ID	Headline
CSCwf70854	Changes to speed on the interface via CLI/GUI dont go through unless first done via shell access.
CSCwh06834	Using special characters in the password while generating TP generates an invalid TP
CSCwf87292	Punt keep alive failure crash on controller managed device apparently due to data packets
CSCwf94294	Misprograming during vpn-list change under data policy.
CSCwf55145	SFP transceiver DOM not working after some time, however interface forwards the traffic as expected

Bug ID	Headline
CSCwf94052	BFD going down for newly onboarded device
CSCwh01095	Rapid memory leak on ngiolite process
CSCwf80927	Speed tests to internet from C8500 device triggered will fail sometimes
CSCwf84522	C8500L Unexpected rebooted while classifying packet with CTF (Common Flow Table)
CSCwh00320	Show commands in sync after removing GigabitEthernet3
CSCwf44703	NAT64 prefix is not originated into OMP
CSCwf99947	Crash when modifying tunnel after running **show crypto** commands
CSCwf77252	SIP calls not working on device with ZBFW enabled
CSCwf62757	C8500L Interface data report interval issue for physical interface
CSCwf96416	Couldn't access any show commands at all.
CSCwf67564	Device observes memory leak at process SSS Manager
CSCwf34171	**Configure replace** command fails due to the license udi PID XXX SN:XXXX line on IOS-XE devices
CSCwh00963	Unable to migrate from ADSL to VDSL without reboot on device
CSCwf69062	SDRA-SSLVPN : The SSLVPN session closes with re-authentication error after some interval of time
CSCwf79264	In device traffic forwarded to wrong VPN hence, traffic gets wrong zonepair matched and gets dropped.
CSCwf71557	IPv4 connectivity over PPP not restored after reload
CSCwf45486	OMP to BGP redistribution leads to incorrect AS_Path Installation on chosen next-hop
CSCwh01313	Unexpected reboot due QFP UCode due to IPsec functions
CSCwf95527	BFD entries removed
CSCwe26895	Router has LocalSoftADR crash, writes flat core, and reloads
CSCwh01318	Multiple crashes observed on device platform due to memory exhaustion
CSCwf71116	Static route keep advertising via OMP even though there is no route.
CSCwf60120	Static NAT entry gets deleted from running config; but remains in startup config
CSCwh00332	B2B NAT: when configration ip nat inside/outside on VASI intereface,ack/seq number abnormal
CSCwh67812	Unable to configure crypto map on a physical interface due to which crypto map-based VPN's cannot be formed

ROMmon Release Requirements

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

Table 19: 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 20: 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.

© 2023–2026 Cisco Systems, Inc. All rights reserved.