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

First Published: 2023-11-24

Last Modified: 2024-08-16

Full Cisco Trademarks with Software License

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 17.12.4

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)
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.

Feature	Description
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 17.12.4

Table 3: 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 .

Table 4: 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.
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

Bug ID	Description
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
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 5: 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.
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.

Bug ID	Description
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.
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 6: 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.

Bug ID	Description
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 7: 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
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 8: 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.
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.

Bugs	Description
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.
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.

Bugs	Description
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.
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

Bug ID	Headline
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
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

Bug ID	Headline
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
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

Bug ID	Headline
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 9: 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)	17.10(1r)
C8500L-8S4X	-	17.10(1r) - available from Cisco IOS XE 17.9.1a release	-
	-	17.10(1r)- available from Cisco IOS XE 17.10.1a release	-

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 10: 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

ROMmon Release for C8500-12X4QC, C8500-12X	Fixes
17.10 (1r)	Added support for new platform C8500-20X6C
17.11(1r)	Fixed a issue in data wipe feature

ROMmon Release for C8500L-8S4X	Fixes
17.10(1r)	CSCwa41877 - Fixes for Intel 2021.2 IPU CSCwb67177 - Fixes for Intel 2022.1 IPU CSCwb60723 - Fixes for CPU temperature CSCwb60863- Fixes for TAM_LIB_ERR_WRITE_FAILURE error

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 impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Documentation Feedback

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

Troubleshooting

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

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