Release Notes for Cisco Catalyst 8500 Series Edge Platforms, Release 17.18.x

© 2025 Cisco and/or its affiliates. All rights reserved.

Catalyst 8500 Edge Platform, Release 17.18.x 3
New software features 3
Resolved and open issues 7
ROMmon release requirements 14
What's new in ROMmon release 15
Upgrade ROMmon 16
Related resources 16
Legal information 16

© 2025 Cisco and/or its affiliates. All rights reserved.

Catalyst 8500 Edge Platform, Release 17.18.x

Cisco 17.18.1a is the first release for Cisco Catalyst 8500 Series Edge Platforms in the Cisco IOS XE 17.18.x release series.

The key highlights of this release include these features and enhancements:

- Monitoring & Observability
- Cellular, IPv6, Voice, Virtualization
- SRv6 Enhancements
- Security and SASE enhancements

New software features

This section provides a brief description of the new software features introduced in this release.

New software features in Cisco IOS XE 17.18.5

There are no new software features for this release.

New software features in Cisco IOS XE 17.18.4

There are no new software features for this release.

New software features in Cisco IOS XE 17.18.3a

There are no new software features for this release.

New software features in Cisco IOS XE 17.18.2

Table 1. New software features for Catalyst 8500 Edge Platform, Release 17.18.2

Product impact	Feature	Description
Ease of Setup	IPv6 Rule and Rule Set Support in Security Policies	From Cisco IOS XE 17.18.2, you can configure IPv6 data prefix lists, rule with rule sets, and object groups in security policy using Cisco SD-WAN Manager.
Upgrade	IPv6 GRE-TP tunnel as protected link support for SRv6 TI-LFA with IS-IS	From Cisco IOS XE 17.18.2, this feature extends IPv6 GRE-TP tunnel as protected link support for SRv6 TILFA with ISIS.
Upgrade	IPv4 GRE-TP tunnel as protected link support for SR-MPLS TI-LFA with OSPF	From Cisco IOS XE 17.18.2 this feature extends IPv4 GRE-TP tunnel as protected link support for SR-MPLS TILFA with OSPF.
Upgrade	IPv4 GRE-TP tunnel as protected link support for SR-MPLS TI-LFA with IS-IS	From Cisco IOS XE 17.18.2 this feature extends IPv4 GRE-TP tunnel as protected link support for SR-MPLS TILFA with ISIS.
Security	Resilient Infrastructure	Starting with the Cisco IOS XE 17.18.2 release and in future releases, Cisco software will display warning messages when configuring features or protocols that do

© 2025 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
		not provide sufficient security such as those transmitting sensitive data without encryption or using outdated encryption mechanisms. Warnings will also appear when security best practices are not followed, along with suggestions for secure alternatives. This list is subject to change, but the following is a list of features and protocols that are planned to generate warnings in releases beyond the version Cisco IOS XE 17.18.1. Release notes for each release will describe exact changes for that release: • **Plain-text and weak credential storage**: Type 0 (plain text), 5 (MD5), or 7 (Vigenère cipher) in configuration files. *Recommendation*: Use Type 6 (AES) for reversible credentials, and Type 8 (PBKDF2-SHA-256) or Type 9 (Scrypt) for non-reversible credentials. • **SSHv1** *Recommendation*: Use SSHv2. • **SNMPv1 and SNMPv2, or SNMPv3 without authentication and encryption** *Recommendation*: Use SNMPv3 with authentication and encryption (authPriv). • **MD5 (authentication) and 3DES (encryption) in SNMPv3** *Recommendation*: Use SHA1 or, preferably, SHA2 for authentication, and AES for encryption. • **IP source routing based on IP header options** *Recommendation*: Do not use this legacy feature. • **TLS 1.0 and TLS 1.1** *Recommendation*: Use TLS 1.2 or later. • **TLS ciphers using SHA1 for digital signatures** *Recommendation*: Use ciphers with SHA256 or stronger digital signatures. • **HTTP**

© 2025 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
		Recommendation: Use HTTPS. • **Telnet** *Recommendation*: Use SSH for remote access. • **FTP and TFTP** *Recommendation*: Use SFTP or HTTPS for file transfers. • **On-Demand Routing (ODR)** *Recommendation*: Use a standard routing protocol in place of CDP-based routing information exchange. • **BootP server** *Recommendation*: Use DHCP or secure boot features such as Secure ZTP. • **TCP and UDP small servers (echo, chargen, discard, daytime)** *Recommendation*: Do not use these services on network devices. • **IP finger** *Recommendation*: Do not use this protocol on network devices. • **NTP control messages** *Recommendation*: Do not use this feature. • **TACACS+ using pre-shared keys and MD5** *Recommendation*: Use TACACS+ over TLS 1.3, introduced in release Cisco IOS XE 17.18.1

New software features in Cisco IOS XE 17.18.1

Table 2. New software features for Catalyst 8500 Edge Platform, Release 17.18.1a

Product impact	Feature	Description
Ease of Use	Hosted Edge Services for SD-Routing Devices	Cisco IOS XE 17.18.1a introduces Hosted Edge Services, a new monitoring feature which enables direct management of Cisco IOx applications installed on your SD-Routing edge devices. This feature delivers improved functionalities like tracking resource usage, starting or stopping Cisco IOx applications at a scale directly through Cisco Catalyst SD-WAN Manager.

© 2025 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
Ease of setup	Cisco Secure Routers Swim and Onboarding Tool	Cisco IOS XE 17.18.1a introduces the Cisco Secure Routers Swim and Onboarding tool that helps customers upgrade and onboard autonomous hardware devices to cloud-hosted or on-premises Catalyst Cisco SD-WAN Manager.
Licensing Process	Licensing compliance, reporting, and notification enhancements	From Cisco IOS XE 17.18.1a release, you can view additional information in your licensing report such as out of compliance and the reason for out of compliance, the number of licenses that have been assigned in the network, how many devices have been assigned licenses, per-device license details, and so on. In addition, you can now connect to the Enterprise Agreement (EA) portal directly from the Cisco SD-WAN Manager with your Smart Account credentials. This helps you to generate the required quantities of licenses for the selected Commerce SKU of EA and deposit them to your desired CSSM Virtual Accounts (VA).
Ease of use	Managing NGFW Policies from Security Cloud Control	Security Cloud Control (SCC) is a cloud-based multi-device manager that facilitates management of security policies to achieve consistent policy implementation. SCC helps optimize your security policies by identifying inconsistencies with them and by giving you tools to fix the inconsistencies. From Cisco IOS XE 17.18.1a release, you can integrate Cisco SD-WAN Manager with SCC, which allows you to import existing NGFW policies, security objects, and security profiles into SCC. With this integration, you can share objects and policies as well as make configuration templates to promote policy consistency across devices.
Security	Custom IPS signature sets	From Cisco IOS XE 17.18.1a release, Custom IPS signature sets are supported in Cisco SD-WAN Manager, which allows you to create and deploy personalized Snort3 IPS signature sets. This feature allows direct modification of actions for existing IPS rules within profiles and supports building custom rules using rule groups or existing rules. With Custom IPS signature sets, organizations can gain greater control and precision in tailoring threat detection to their specific security needs.
Ease of Use	Certificate Management on SD-Routing Devices	This feature introduces a new certificate authorization setting, Enterprise Certificate Settings, which unifies certificate configurations for SD-Routing devices. Cisco SD-WAN Manager automates certificate management by leveraging protocols like EST (Enrolment over Secure Transport) and SCEP (Simple Certificate Enrolment Protocol). The feature automates the enrolment, and renewal of certificates.
Upgrade	MVPN Ingress Replication (IR) over SRv6	This feature enables the transport of IPv4 MVPN traffic across an SRv6 network. It simplifies multicast deployment by using the existing SRv6 unicast infrastructure as the underlay. With this feature, the ingress PE router receives multicast traffic and creates a separate unicast SRv6-encapsulated copy for each egress PE router in the multicast group.
Upgrade	SRv6 Path MTU Discovery	This feature introduces a mechanism to determine the maximum transmission unit (MTU) for packets traversing an SRv6 underlay network. It ensures efficient packet forwarding by preventing fragmentation and packet drops, thereby allowing network devices to dynamically adjust packet sizes to avoid exceeding link MTU limits. The system relays ICMP

© 2025 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
		Packet Too Big (PTB) messages from the SRv6 underlay to the IPv6/IPv4 overlay network, supporting both Transit-node and Headend-node PTB relay methods.
Upgrade	SRv6 Flex-Algo with TI-LFA and uLoop Avoidance	From Cisco IOS XE 17.17.1a, Flexible Algorithm enhances SRv6 by including functions like Topology Independent Loop-Free Alternate (TI-LFA) and microloop (uLoop) avoidance. This feature improves network resilience and efficiency.
Licensing Process	Product Analytics for routers	Product Analytics refers to the collection of product telemetry such as product performance and resource usage information directly from IOS-XE-based routing platforms. From Cisco IOS XE 17.18.1a release, Product Analytics is enabled by default when. Use this functionality to gain data insights such as product performance, feature consumption, and the licensing types that suit your requirements best.
Ease of Use	MAP-T Border Router (BR) Enhancements	The Cisco IOS XE 17.18.1a release supports several enhancements to the MAP-T Border Router, an important component in facilitating IPv4 packet transmission over IPv6 networks. These improvements include enhanced support for fragmented ICMP packets during IPv4 to IPv6 transition, robust support for hairpin traffic between devices, and reliable handling of fragmented UDP packets with a checksum value of 0. These enhancements also provide service providers with a more comprehensive and resilient solution for maintaining essential IPv4 connectivity during the transition to an all-IPv6 environment.

Resolved and open issues

This table lists the resolved and open issues in this specific software release.

Note: This software release may contain bug fixes first introduced in other releases. To see additional information, click the bug ID to access the Cisco Bug Search Tool.

Resolved and open issues in Cisco IOS XE 17.18.5

Table 3. Resolved issues for Cisco 8500 Edge Platform, Release 17.18.5

Bug ID	Description
CSCwu97838	RADSEC TLS peer validation fails when unrelated trustpoints share a common PKI Root CA
CSCwv55092	cEdge upgrade rollback due to recursive SNMP BGP trap deprecated-model migration
CSCwq96185	SD-WAN: High Memory Usage and Unexpected Reload Due to a vDaemon Memory Leak
CSCwu97716	Unexpected Device Reload Triggered by DHCP Service Failure During Lease Conflict Scenarios
CSCwu83262	L2TPv3 xconnect session fails to establish when the traffic traverses through IPsec tunnel interface.
CSCwu27070	Unexpected Reload in CPP Server (cpp_sp_svr) Code
CSCwu12631	Posture redirection not working on Sdwan router switch module

© 2025 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwt81568	Route-replicate command is present in configuration but is not taking effect after reload.
CSCwu69080	HTX Crash observed in Service Node - Device
CSCwt97257	Device - Packets classified as runts post macsec-decryption
CSCww06413	PKCS12 re-import silently fails to install a CA certificate
CSCwt42293	Device: Cellular interface flap causing crypto enrollment failure
CSCwr02102	Router intermittently loses ip address dynamically assigned to tunnel interface
CSCwt98537	QoS unsupported configuration makes route processor crash
CSCwq08386	Device platform Tier 3 throughput clarification
CSCwu49029	Unexpected reload on CGM (Class-Group Manager) when updated
CSCwt75037	Device in controller mode crashes with Critical process cpp_ha_top_level_server fault on fp_0_0 (rc=69)
CSCwr69095	DNS requests for vBond fail
CSCwu00043	LSC certificate failure " CRYPTO_PKI: Failed to add ca req pool entry 538" in scale environment
CSCwu61766	SDWAN edge router OMPD crash on malformed SD-WAN identity IP-to-user update from vSmart pxGrid integration
CSCws92932	Unexpected reload due to Segmentation Fault on TPS IPC Process
CSCwu27937	system-report handling has a conflict - unrelated processes may dump core after a cpp/ucode fault.
CSCwt66413	ncsshd process fails to terminate after " no netconf" and netconf refuses connection
CSCwt56693	L2TP: Seeing " protocol l2tpv2 L2TP_CLASS_011" config getting lost with clear ppp all cli
CSCws80808	Loopback interface in Mgmt-intf VRF becomes unreachable via Management interface
CSCwt13176	Memory leak detected in TLS testcase
CSCwt84502	Critical Process cpp_ha_top_level_server crash (rc=69) Crash after adding zone based firewall setup configuration on the router
CSCwv37592	Unable to configure no exec under async line or async range IOS-XE SDWAN
CSCwu21682	Segmentation Fault at Process = SASCheckInit (or other process)
CSCwu89497	Device modify fragment IPV6 identifier
CSCwu93056	Device may reload after remove an endpoint.
CSCwt51797	RIPv2 will stop sending multicast routing updates after interface flap
CSCwu47545	Ucode Code Crash while Printing Log for FW Drop for Packet with Invalid Header

© 2025 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwt45748	Crash while processing packet in AppNav Tunnel
CSCwr74339	vman crashed @ __GI___clock_nanosleep in router reload and power cycle test
CSCwr47230	Upgrade failed " Install operation not allowed because verification of image ..... is in progress."
CSCwt69544	QFP Ucode device crash
CSCwu97638	Unexpected reload due to ACL pointer corruption with SNMPv3
CSCwt51754	Router reloaded after adding voice related configuration
CSCwt25903	Not able to disable " log" feature in NGFW Policies vManage for " Drop" rules.
CSCwu45273	LISP ITR sources locally-originated control-plane packets from the numerically lowest configured RLOC IP instead of the outbound interface address
CSCwu11498	show interface counter become abnormal
CSCwv39390	Router generates FMANRP_ESS-3-ERREVENT logs with tracebacks
CSCwv74258	Device: infra timer expiry with high traffic rate
CSCwu76495	SDWAN: Crash while updating Adaptive QOS Session Policy due to minimal traffic size
CSCwt34226	SSH Connectivity Issue with On-Demand Next Hop in Segment Routing Traffic Engineering (SR-TE)
CSCwt29648	BadIpChecksum drop when Segment-routing MPLS is configured over IPSEC/GRE over VDSL interface on C8200
CSCwu01733	Rapid memory leak in ompd after ISE integration with vManage
CSCwt94337	cpp_cp_svr crashes with SIGSEGV whle printing packet trace data
CSCwu51162	Unexpected reload on router in SDWAN CCE (Classifier and Classification Engine)
CSCwv41407	Device: BGP updates that should be suppressed are advertised with incorrect attribute after RPSO
CSCwv97208	LISP xTR may retain a stale Registering ETR session after dual-WAN failback, delaying Map-Register update to the Map-Server for 6-7 minutes
CSCwu32769	Device Reload Due to CPP Stuck Threads in BFD SD-WAN Transmit Path
CSCwt88212	Untagged packets dropped with non-default native VLAN on ISR4K
CSCwq98154	Multicast traffic not forwarded over P2P DMVPN phase 1 tunnel
CSCwr24042	Traffic going to all CEDGES without receivers where Replicator stuck in P MDT
CSCwu99434	Unexpected device reload during Rapid Trustpoint Deletion and Creation Events Resulting in core file generation
CSCwv25890	Support for GRE+MPLS on tunnel transport mode

© 2025 Cisco and/or its affiliates. All rights reserved.

Table 4. Open issues for Catalyst 8500 Edge Platform, Release 17.18.5

Bug ID	Description
CSCwv71880	SD-WAN redirect-dns Destination NAT session collides with SIG tunnel IKEv2 control plane traffic
CSCws94603	Crashes During CRL Fetch Failure due memory reallocation
CSCwv68329	Static NAT DIA routes intermittently withdrawn/not reinstalled after transport tracker/TLOC flap
CSCwv60786	Intermittent issue with RRI being lost on the Flex Hub
CSCwv73701	Packet reordering observed when application performance-monitor service policy enabled
CSCwq26818	Device: Link May Stay Down After Swapping 10G To 1G Optics
CSCwt63505	Device crashed while authenticating trustpoint with DNAC

Resolved and open issues in Cisco IOS XE 17.18.4

Table 5. Resolved issues for Cisco 8500 Edge Platform, Release 17.18.4

Bug ID	Description
CSCwt76906	C9K: Continuous increase in holding memory for CTS CORE
CSCwt47516	WLC crash due to corrupted length field during AAA processing
CSCwt94106	Pubd core generated for C9300
CSCwu04279	System instability and potential service disruption after invalid GPM load
CSCwu03804	C9000: Randomly during operation - Interface VLAN / SVI go missing from " show run" but remain up. Configs are lost upon reload.
CSCwu21451	C9250/C9350: Cluster manager crash for stacked devices with specific mac address combination
CSCwt51443	Controller crashed due to CPUHOG under DBAL_EVENTS
CSCwt86654	IOS-XE: IKEv2 process crash caused by stack buffer overflow during AnyConnect EAP credential parsing
CSCwu02602	DBAL EVENTS crash seen while trying to push config group to C8570-G2/C8500-12x4QC in SDWAN and SD-Routing
CSCwn80721	Unexpected Reboot in Process Sessmgrd
CSCwt87294	mDNS Cache-Flush behavior not consistent

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

Resolved and open issues in Cisco IOS XE 17.18.3a

Table 6. Resolved issues for Cisco 8500 Edge Platform, Release 17.18.3a

© 2025 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCws72902	C8200/C8300/C8500L: Overrun drops due to uneven GRE traffic distribution across data plane cores
CSCwr90843	SD-WAN Edge: Device may reload unexpectedly under heavy IPSec Traffic Load
CSCws85423	C8500-20x6C: HSRP forwarding failure on 100G interfaces in scaled setup
CSCws28994	CPP crash while processing QoS rate profile
CSCwt10333	C8500L unexpectedly reloading due to cpp_cp_svr fault
CSCwr84985	dmiauthd process crashes, due to which the configuration does not sync between startup-config and the running-config.
CSCws32994	8500L device crashing due to stuck threads when Netflow is enabled.
CSCws30718	Dataplane Crash Observed on CGN NAT Scale Router after " clear ip nat translation *"
CSCwt18839	Segmentation Fault in cpp_cp_svr while Printing FIA Trace Data
CSCws77372	Software crash with fman_fp core due to NAT-related show commands
CSCwr44547	SDWAN Manager: Reporting abnormal loss value for tunnel stats in the UI
CSCws80232	SD-WAN Edge: Zone-Based Firewall Not Programmed Correctly Resulting in Class-Default Match
CSCwt46335	MAP-E: stop sending IPv4 traffic during MAP rule refresh
CSCwq60752	Catalyst 8000 FP Crash After Clearing NAT Translations
CSCws58529	When the name server is specified using IPv6, half entries are created due to unintended NAT.
CSCws76668	Memory leak udner " fman_fp_image" on CAT8500 routers when NAT is enabled.
CSCwt22873	High QFP Caused by " all-host" Limit in - Carrier Grade NAT mode

Table 7. Open issues for Catalyst 8500 Edge Platform, Release 17.18.3a

Bug ID	Description
CSCwt69544	QFP Ucode Fugazi crash on 17.15.4c
CSCwt45748	Crash while processing packet in AppNav Tunnel
CSCwq96185	SD-WAN: High Memory Usage and Unexpected Reload Due to a vDaemon Memory Leak

Resolved issues in Cisco IOS XE 17.18.2

Table 8. Resolved issues for Cisco 8500 Edge Platform, Release 17.18.2

© 2025 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwr42950	SDWAN On-Demand Tunnels Do Not Expire When UMTS Is Enabled
CSCwq51935	NAT64 static entry removed when command to delete non-existent entry is applied.
CSCwe19394	Device may boot up into prev_packages.conf due to power outage
CSCwr77958	NWPI not capturing self-generated syslog traffic
CSCwj61730	Device crash when removing SGT caching on an interface
CSCwq77322	Device sending a 2 Byte packet of FLOW_SAMPLER_RANDOM_INTERVAL instead of a 4-Byte packet
CSCwr24031	After upgrade sd-wan service-tracker in vrf selects source IP address from GRT when MPLS Inter-AS VPN option B configured
CSCwr49794	ISR exporters with ETA enabled are generating invalid template data errors in SNA
CSCwq98206	EPBR set interface action get missing after reboot
CSCwr25077	vDaemon crash when initializing DNS channels

Table 9. Open issues for Catalyst 8500 Edge Platform, Release 17.18.2

Bug ID	Description
CSCws30834	Device ignore the keepalive command under the SIG tunnel interface pushed by the vmanage
CSCwr90843	Device seeing crash @cd_sw_ipsec_op_inline with traffic soak
CSCwq77458	fman crash after fnf config changes
CSCwr87083	Not able to onboard sd-routing devices using generic bootstrap file stored in usb
CSCws12946	Device port forward issue with multiple ISP
CSCws18137	Out of sync when CLI Template was attached (missing element: authentication in /ios:native/ios:line/ios:vty[ios:first='0']/ios:login/ios:authentication)
CSCwr64075	During Soak run observed memif_ring_free_count thread
CSCwr76580	Strange behavior with the Cisco Umbrella SIG tunnels configured from vManage to Umbrella.
CSCwr30573	TLOC Extension unable to program due to module boot up timing
CSCws25557	Cipher Suites TLS 1.2 for control connections
CSCwr95551	Router crashes when configuring SSL VPN with Policy-Based Routing (PBR) and NAT
CSCwr51615	Unexpected reload under a C8500L in controller mode
CSCwr08462	There seems to be an issue where the NAT router is not responding to ARP requests
CSCwr97784	Slow performance on Netconf RPC on stateless static NAT translation

© 2025 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwr88206	FIB table routes: Next Hop (NH) ID 0 is getting corrupted and assigned to a value other than Blackhole
CSCwr84985	dmiauthd process crashes, due to which the configuration does not sync between startup-config and the running-config.
CSCwq24119	Traceback seen when detaching the CN railways customer configs
CSCwm97460	Control Connection to vManage is only attempted over Highest Priority TLOC
CSCwr00088	Add CLI to change per MPLS label CEF statistics query interval on FMAN FP
CSCwr55240	C8000v experienced critical process ompd fault on rp_0_0
CSCwr72709	Router crash in TDM-TDM call when debug voip fpi enabled
CSCwq98154	Multicast traffic not forwarded over P2P DMVPN phase 1 tunnel
CSCwr49475	BFD sessions flapping and not recovering - SYMNAT port not updating to data-plane
CSCwo42664	Periodic Service Restart May Generate Crash Files
CSCwr64257	Unexpected reload on ftmd SDWAN device
CSCws26373	Device experiences an unexpected reboot due to NAT in the data-plane after a policy push
CSCwp97178	Flapping nat will cause bfd session down with ipsec session shown
CSCwr76176	PMTU Converges Unexpectedly to 970 Bytes After dbg2:1 Event
CSCwr77083	C8000v crashed in crypto library

Resolved issues in Cisco IOS XE 17.18.1

Table 10. Resolved issues for Cisco 8500 Edge Platform, Release 17.18.1a

Bug ID	Description
CSCwn12594	SIG zscaler ipsec - vpn credentials for primary tunnel not created
CSCwn42496	SDWAN-SIT: Encore crashed @bfd_send_and_detect_sleep_time during soak run
CSCwn69868	Unable to come up control connections with Controllers after Controllers added and down/up
CSCwo72675	All BFD sessions for dialer interfaces are down. SA ID is 0 for all of them.
CSCwo84428	Memory leak under vdaemon process with DTLS on SNMP polling
CSCwp07901	CPP crash while processing fragments of a jumbo frame
CSCwp24639	Device reload after vpn config changes on SDWAN

© 2025 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwm27749	Speed test download / Throughput issue on device seen with IPSEC ESP-NULL transform using Zscaler
CSCwm72336	CXP with Data Policy redirect-DNS via Overlay causes Blackhole
CSCwn26353	BFD sessions via TLOC-Ext do not come up when IPv6 is dynamically changed
CSCwo05703	VFR is not Dynamically Disables After ZBFW Removal
CSCwo75657	Maximum control connection not equal to maximum omp sessions - cEdge
CSCwp91064	FTMD cero pointer dereference leading to crash

Table 11. Open issues for Catalyst 8500 Edge Platform, Release 17.18.1a

Bug ID	Description
CSCwp12196	Device unexpectedly reloads due to memory corruption on a notification queue in FTMd
CSCwq27426	BFD session down due to unencrypted outbound BFD packets despite active IPsec SA
CSCwe19394	Device may boot up into prev_packages.conf due to power outage
CSCwo42664	17.12 - keyman core files on cEdge
CSCwo66099	SDWAN cEdge Service Side BFD flaps
CSCwp01089	EPFR-High latency times are observed on the hub device (Cisco Catalyst 8500-12X Edge Platform).
CSCwp81539	Memory leak under cfgmgr process on SNMP polling
CSCwq20326	Device does not install service-side static route to CEF after upgrade
CSCwq40026	Unexpected Reboot due to Process FTMD

ROMmon release requirements

This section lists the ROMmon version required for your Catalyst 8500 model:

Table 12. Compatibility information for Catalyst 8500 Edge Platform, Release 17.18.1a

	DRAM	Minimum ROMmon	Recommended ROMmon
C8500-12X4QC and C8500-12X	16 GB(default)	17.2(1r)	17.11(1r)
	32GB	17.2(1r)	17.11(1r)
	64GB	17.3(2r)	17.11(1r)

© 2025 Cisco and/or its affiliates. All rights reserved.

	DRAM	Minimum ROMmon	Recommended ROMmon
C8500-20X6C	All variants	17.10(1r)	17.15(1r) **Note:** Downgrading to a ROMmon version lower than 17.15(1r) is not supported.
C8500L-8S4X	-	17.10(1r)	17.14(1r)* **Note:** 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.

What's new in ROMmon release

This section lists changes in the ROMmon package.

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.

© 2025 Cisco and/or its affiliates. All rights reserved.

ROMmon Release for C8500-20X6C	Fixes
17.15(1r)	CSCwf98335 - Evaluation of all_routing_iosxe for Intel 2023.3 IPU and SMRAM vulnerabilities. CSCwd96405 - ASR1k:BL and ML hashes not seen in the " Show system intergrity" CLI for Aikido based platforms. Additional minor fixes.

Upgrade ROMmon

To upgrade the ROMmon version of your device, use these steps:

1. Check the existing version of ROMmon by using **show rom-monitor r0** command. If you are installing Cisco IOS XE software on a new device, skip this step.
2. Review *Minimum and Recommended ROMmon Releases* to identify the recommended version of ROMmon software for the device you plan to upgrade.
3. Go to https://software.cisco.com/# and download the ROMmon package file.
4. Copy the ROMmon file to flash drive:

   copy ftp:// *username:password@IP addressROMmon package file* **flash**:
5. Upgrade the ROMmon package using the following command:

   upgrade rom-monitor filename bootflash: *ROMmon package name* **all**
6. Execute **reload** command to complete the ROMmon upgrade process
7. Execute **show rom-monitor r0** command to ensure the ROMmon software is upgraded.

Related resources

- 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

Legal information

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: www.cisco.com/go/trademarks. 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. (1110R)

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.

© 2025 Cisco Systems, Inc. All rights reserved.