



Release Notes for Cisco Catalyst 8500 Series Edge Platforms, 26.1.x

Contents

Catalyst 8500 Edge Platform, Release 26.1.x.....	3
New software features.....	3
Resolved and open issues	5
ROMmon release requirements.....	6
What's New in the ROMmon release	7
Upgrade ROMmon	7
Related resources.....	8
Legal information	9

Catalyst 8500 Edge Platform, Release 26.1.x

Cisco 26.1.x is the first release for Cisco Catalyst 8500 Series Edge Platforms in the Cisco IOS XE 26.x release series.

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 26.1

Product impact	Feature	Description
Software Reliability	Post Quantum Crypto for IKEv2, SSH and MACsec	Post-Quantum Cryptography (PQC) refers to cryptographic algorithms designed to be secure against attacks from quantum computers which can break many classical encryption methods. Post-Quantum Cryptography is implemented by using the algorithms available as part of Module-lattice based Cryptography. Cisco utilizes a hybrid approach to implement PQC. The hybrid approach to Post-Quantum Cryptography (PQC) combines a quantum-resistant algorithm, such as the module-lattice based ML-KEM (e.g., mlkem768), with a classical elliptic curve key exchange algorithm like NIST P-256 or X25519, along with a hash function such as SHA-256.
Ease of Use	BGP Advertisement Startup Delay	The BGP Advertisement Startup Delay feature addresses this issue by introducing a configurable delay before BGP begins advertising routes to its neighbors. This delay allows sufficient time for routes to be installed in the hardware, ensuring traffic forwarding is ready before new routes are announced.
Security	Resilient Infrastructure	<p>Starting with the Cisco IOS XE 26.1 release and in future releases, Cisco software will display warning messages when configuring features or protocols that do not provide sufficient security such as those transmitting sensitive data without encryption or using outdated encryption mechanisms.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.</p> <p>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:</p> <ul style="list-style-type: none">• Plain-text and weak credential storage: Type 0 (plain text), 5 (MD5), or 7 (Vigenère cipher) in configuration files. <i>Recommendation:</i> Use Type 6 (AES) for reversible credentials, and Type 8 (PBKDF2-SHA-256) or Type 9 (Scrypt) for non-reversible credentials.• SSHv1 <i>Recommendation:</i> Use SSHv2.• SNMPv1 and SNMPv2, or SNMPv3 without

Product impact	Feature	Description
		<p>authentication and encryption</p> <p><i>Recommendation:</i> Use SNMPv3 with authentication and encryption (authPriv).</p> <ul style="list-style-type: none"> • MD5 (authentication) and 3DES (encryption) in SNMPv3 <p><i>Recommendation:</i> Use SHA1 or, preferably, SHA2 for authentication, and AES for encryption.</p> <ul style="list-style-type: none"> • IP source routing based on IP header options <p><i>Recommendation:</i> Do not use this legacy feature.</p> <ul style="list-style-type: none"> • TLS 1.0 and TLS 1.1 <p><i>Recommendation:</i> Use TLS 1.2 or later.</p> <ul style="list-style-type: none"> • TLS ciphers using SHA1 for digital signatures <p><i>Recommendation:</i> Use ciphers with SHA256 or stronger digital signatures.</p> <ul style="list-style-type: none"> • HTTP <p><i>Recommendation:</i> Use HTTPS.</p> <ul style="list-style-type: none"> • Telnet <p><i>Recommendation:</i> Use SSH for remote access.</p> <ul style="list-style-type: none"> • FTP and TFTP <p><i>Recommendation:</i> Use SFTP or HTTPS for file transfers.</p> <ul style="list-style-type: none"> • On-Demand Routing (ODR) <p><i>Recommendation:</i> Use a standard routing protocol in place of CDP-based routing information exchange.</p> <ul style="list-style-type: none"> • BootP server <p><i>Recommendation:</i> Use DHCP or secure boot features such as Secure ZTP.</p> <ul style="list-style-type: none"> • TCP and UDP small servers (echo, chargen, discard, daytime) <p><i>Recommendation:</i> Do not use these services on network devices.</p> <ul style="list-style-type: none"> • IP finger <p><i>Recommendation:</i> Do not use this protocol on network devices.</p> <ul style="list-style-type: none"> • NTP control messages

Product impact	Feature	Description
		<p><i>Recommendation:</i> Do not use this feature.</p> <ul style="list-style-type: none"> • TACACS+ using pre-shared keys and MD5 <p><i>Recommendation:</i> Use TACACS+ over TLS 1.3, introduced in release Cisco IOS XE 17.18.1</p>
Ease of use	One minute granularity interface statistics using Cisco Catalyst SD-WAN Manager	This feature enables the collection of granular interface statistics from devices every minute, providing real-time insights for effective troubleshooting and ensuring optimal performance.
Licensing Process	Enhancements for NGFW in Policy Groups	This feature introduces support for NGFW Policy Groups, that includes import and export of firewall policies, display of rule hit counts, drag-and-drop rule reordering to update priority, visibility of policy and object usage references in the NGFW Dashboard, and retention of rule and policy names in the running CLI configuration.

Resolved and open issues

This table lists the resolved 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 26.1

Table 1. Resolved issues for Cisco 8500 Edge Platform, Release 26.1

Bug ID	Headline
CSCws40263	uCode Crash due to Stuck Thread during NAT Session DB Walk
CSCwr30573	TLOC Extension unable to program due to module boot up timing
CSCws89172	Crash @cft_engine_handle_vrf_associate_if_needed on C8500 platform with IPv6 traffic
CSCwr11064	Speed test session Timeout not clear enough for user to get details
CSCwq77458	fman crash after fnf config changes
CSCwr00088	Add CLI to change per MPLS label CEF statistics query interval on FMAN FP
CSCwr06399	Certificate verify fails & id cert not installed (after reload of device), of certs with EC Key 521
CSCwr08462	[C8500L-8S4X] There seems to be an issue where the NAT router is not responding to ARP requests
CSCws62501	IOSd crash with " match authen-status unauthenticated" configured
CSCwr44921	SDWAN C-Edge Router Crashes - CPU Usage due to Memory Pressure exceeds threshold
CSCwo91087	DWDM-SFP10G-C SFP is not working when connecting C8500L-8S4X through a MUX
CSCwq43883	Converting L2 Routed port channel to L3 is broken in Aurora2
CSCwq98154	[XE MCAST] Multicast traffic not forwarded over P2P DMVPN phase 1 tunnel

Table 2. Open issues for Catalyst 8500 Edge Platform, Release 26.1

Bug ID	Headline
CSCws66553	fpmd crash seen with 17.12.6B respin image with longer soak + clear sdwan omp events
CSCwt22006	Web UI bootstrapping failure due to invalid configuration causes persistent config merge errors despite subsequent corrections
CSCwt07572	Radius packet silently consumed by utd
CSCwt22873	High QFP Caused by "all-host" Limit in - Carrier Grade NAT mode
CSCwt28048	Preferred-color-group restrict is not honored in data policy
CSCws99246	Regarding the operation enabling communication from outside the NAT
CSCwt27474	20.18.2 Cisco SPA:The hardcoding of the AS number 64512 needs to be removed and changed to autodetect
CSCwt18839	Segmentation Fault in cpp_cp_svr while Printing FIA Trace Data
CSCws95387	PCG config is not getting deleted from FP
CSCwr76176	BFD SD-WAN PMTUD: PMTU Converges Unexpectedly to 970 Bytes After dbg2:1 Event
CSCws98086	Update "reason for state change: MAX" in BFD Syslog
CSCwq00263	ipv6 ipsec packets dropped in svti AH in transport mode - ping failed with specific size packet

ROMmon release requirements

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

Table 3. 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)
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.

	DRAM	Minimum ROMmon	Recommended ROMmon

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 the 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.

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 integrity" 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.