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

Contents

Catalyst 8500 Edge Platform, Release 26.1.x

Cisco 26.1.1 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 26.1.1

Product impact	Feature	Description
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.
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.
Ease of use	BGP Advertisement Startup Delay	When a Border Gateway Protocol (BGP) process initializes during a router reload or when BGP routing sessions are reset by using the clear ip bgp* command, it could result in a temporary period of traffic loss. 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.
Software reliability	Resilient Infrastructure	As part of the ongoing commitment to network security, this release introduces secure alternatives to legacy commands. These updates are designed to mitigate potential risks and assist in establishing a more robust and secure operational baseline. The identified insecure commands are categorized as: • Line transport: Updates to secure remote access methods. • Device server configuration: Hardening of server-side settings. • File transfer protocols: Transitioning to encrypted transfer methods. • SNMP: Enhancements to secure management traffic. • Passwords: Strengthening authentication and credential management. • Miscellaneous: General security improvements for various system functions For all detected insecure configurations during device boot or upgrade, error messages are displayed. In Cisco IOS XE 26.1.1 release, all insecure CLI commands are blocked by default to strengthen your network infrastructure. If your environment requires the use of a legacy command, you must enable the system mode insecure command in global configuration mode. • Recommendation: Do not use insecure mode. This mode is temporary and will be removed in a future release. Identify and replace all insecure commands with their secure alternatives. • Upgrade behavior: If you upgrade to Cisco IOS XE 26.1.1 release with insecure commands already present in the running configuration, the system mode insecure command is

Product impact	Feature	Description
		automatically added to your configuration to prevent service disruption For more information, refer this document Routing-SD-WAN Resilient Infrastructure.

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 26.1.1

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. To search for a documented Cisco product issue, type in the browser: <bug_number> site:cisco.com.

Table 1. Resolved issues for Cisco 8500 Edge Platform, Release 26.1.1

Bug ID	Description
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 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	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	CPU Usage due to Memory Pressure exceeds threshold
CSCwo91087	DWDM-SFP10G-C SFP is not working when connecting device through a MUX
CSCwq43883	Converting L2 Routed port channel to L3 is broken
CSCwq98154	Multicast traffic not forwarded over P2P DMVPN phase 1 tunnel

Table 2. Open issues for Catalyst 8500 Edge Platform, Release 26.1.1

Bug ID	Description
CSCws66553	fpmd crash seen with 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	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	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 26.1.1a

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