Release Notes for Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms, Release 26.1.x

Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms, Release 26.1.x

Cisco 26.1.1 is the first release for Cisco Catalyst 8200 and Catalyst 8300 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.

Table 1. New software features for Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms, Release 26.1.1

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

Product impact	Feature	Description
Upgrade	Firmware Upgrade	From Cisco IOS XE 26.1 release, you can use Cisco Catalyst SD-WAN Manager to select a device that either has a Wi-Fi module or Cellular module and perform firmware upgrade only for the specific device.
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.
CUBE Features		
Upgrade	Advanced TLS security compliance and control	From Cisco IOS XE 26.1.1 onwards, weaker TLS versions (v1.0, v 1.1) and associated ciphers are not supported in default configurations. However, these insecure configurations are supported in " insecure operation-mode" for CUBE and SRST, and support for non-compliant ciphers has been discontinued in both platforms.
Upgrade	Dual certificate support for SIP trunk client and server functionality	From Cisco IOS XE 26.1.1 onwards, the feature allows provisioning and assigning separate certificates for client and server roles on each SIP trunk in CUBE.

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

Resolved issues in Cisco IOS XE 26.1.1

Table 2. Resolved issues for Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms, 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 device 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

Bug ID	Description
	requests.
CSCws62501	IOSd crash with " match authen-status unauthenticated" configured.
CSCwr44921	Device crashes CPU Usage due to Memory Pressure exceeds threshold.
CSCwq98154	Multicast traffic not forwarded over P2P DMVPN phase 1 tunne.l
CSCwq43883	Converting L2 Routed port channel to L3 is broken in Aurora2.

Open issues

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

Note: This software release may contain open bugs first identified 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.

Open issues in Cisco IOS XE 26.1.1

Table 3. Open issues for Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms, Release 26.1.1

Bug ID	Description
CSCws72902	Overruns on interfaces and QFP spikes with GRE tunnels on device.
CSCws66553	fpmd crash seen 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.
CSCws95993	Seeing T1 license in use even after configuring T2.
CSCwt22873	High QFP Caused by " all-host" Limit in - Carrier Grade NAT mode
CSCwt02712	Cy3 Relops image Curie(Radium) platform : Observed degradation in the CP CPU.
CSCwt28048	Preferred-color-group restrict is not honored in data policy.
CSCws99246	Regarding the operation enabling communication from outside the NAT.
CSCwt29648	BadIpChecksum drop when Segment-routing MPLS is configured over IPSEC/GRE over VDSL interface on device.
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	BFD SD-WAN PMTUD: PMTU Converges Unexpectedly to 970 Bytes After dbg2:1

Bug ID	Description
	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.

Compatibility

ROMMON Compatibility Matrix

The table lists the ROMMON releases supported in Cisco IOS XE 26.x releases.

Platforms	Cisco IOS XE Release	Minimum ROMMON Release supported for IOS XE	Recommended ROMMON Release supported for IOS XE
Catalyst 8300 Series Edge Platforms			
C8300-1N1S-4T2X|6T	26.1	17.3(4.2r)	26.1(1r)
C8300-2N2S-4T2X|6T	26.1	17.3(4.1r)	17.18(2r)
Catalyst 8200 Series Edge Platforms			
C8200-1N-4T	26.1	17.6(8.1r)	26.1(1r)
C8200L-1N-4T	26.1	17.6(8.1r)	26.1(1r)

NOTE: If the systems do not have the minimum ROMMON version as specified in the table, we recommend booting the 17.12.5 IOS XE image. This will enable the systems to automatically upgrade to the required ROMMON versions. Once upgraded, the customer can successfully boot the 17.18.1a image.

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 ROMMON Compatibility Matrix 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 address*ROMmon 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 8200 Series Edge Platforms
- Hardware Installation Guide for Catalyst 8300 Series Edge Platforms
- Smart Licensing Using Policy for Cisco Enterprise Routing Platforms
- Cisco Catalyst 8000 Edge Platforms Family Licensing
- Cisco Catalyst 8300 and 8200 Series Edge Platforms Software Configuration Guide

Legal information