Release Notes for Cisco 8000 Series Secure Routers, Release 26.1.x

Contents

Cisco 8000 Series Secure Routers, Release 26.1.x

Cisco IOS XE 26.1.1 is the first release for the Cisco 8000 Series Secure Routers in the Cisco IOS XE 26.1.x release series.

The Cisco® 8000 Series Secure Routers deliver the industry's most complete secure networking experience, combining cutting-edge security, routing, assurance, and SD-WAN capabilities in a unified platform. The Cisco 8000 Series is the foundation for resilient networks that scale with your business needs.

New hardware features

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

New hardware features for Cisco IOS XE 26.1.1

Table 1. New hardware features for Cisco 8000 Series Secure Routers, Release 26.1.1

Feature	Description
Cisco 8100 Series Secure Routers	From Cisco IOS XE 26.1.1, Cisco Secure Series Routers are available in these models: • C8131-G2 • C8130-VAI-G2 • C8130-VAP-G2 • C8151-CVAI-G2 • C8151-CVAP-G2

New software features

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

New software features for Cisco IOS XE 26.1.1

Table 2. New software features for Cisco 8000 Series Secure Routers, Release 26.1.1

Product impact	Feature	Description	Supported platforms
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.	Cisco 8000 Series Secure Routers

Product impact	Feature	Description	Supported platforms
		• 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.	
Software reliability	Post Quantum Crypto for IKEv2 and SSH Sessions	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	Cisco 8000 Series Secure Routers

Product impact	Feature	Description	Supported platforms
		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.	Cisco 8000 Series Secure Routers
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	Cisco 8300 Series Secure Routers (C8375-E-G2)
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.	Cisco 8300 Series Secure Routers (C8375-E-G2)

Resolved issues

This table lists the resolved 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.

Resolved issues in Cisco IOS XE 26.1.1

Table 3. Resolved issues for Cisco 8000 Series Secure Routers, 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 C8500 platform with IPv6 traffic

Bug ID	Description
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
CSCwr71405	C8500-12X/C8500-12X4QC-: Unable to Ping Interfaces Using GLC-GE-100FX SFP also IFSWAP stop failed error seen
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	CPU Usage due to Memory Pressure exceeds threshold
CSCwq98154	Multicast traffic not forwarded over P2P DMVPN phase 1 tunnel
CSCwq43883	Converting L2 Routed port channel to L3 is broken
CSCwt10333	C8500L unexpectedly reloading due to cpp_cp_svr fault
CSCwr87083	C11xx: Not able to onboard sd-routing devices using generic bootstrap file stored in usb

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 4. Open issues for Cisco 8000 Series Secure Routers, Release 26.1.1

Bug ID	Description
CSCwq77458	fman crash after fnf config changes
CSCwt27474	20.18.2 Cisco SPA:The hardcoding of the AS number 64512 needs to be removed and changed to autodetect
CSCwr08462	[C8500L-8S4X] There seems to be an issue where the NAT router is not responding to ARP requests
CSCws66553	fpmd crash seen with 17.12.6B respin image with longer soak + clear sdwan omp events
CSCwr30573	TLOC Extension unable to program due to module boot up timing

Bug ID	Description
CSCws40263	uCode Crash due to Stuck Thread during NAT Session DB Walk
CSCwt07572	Radius packet silently consumed by utd
CSCwr44921	SDWAN C-Edge Router Crashes - CPU Usage due to Memory Pressure exceeds threshold
CSCwr88206	FIB table routes: Next Hop (NH) ID 0 is getting corrupted and assigned to a value other than Blackhole
CSCws95387	PCG config is not getting deleted from FP
CSCwq00263	ipv6 ipsec packets dropped in svti AH in transport mode - ping failed with specific size packet
CSCwq24119	IR1835: Traceback seen when detaching the CN railways customer configs in 17.19
CSCwm97460	17.9 cEdges - Control Connection to vManage is only Attempted over Highest Priority TLOC
CSCwt18839	Segmentation Fault in cpp_cp_svr while Printing FIA Trace Data
CSCws98086	Update " reason for state change: MAX" in BFD Syslog
CSCwq98154	[XE MCAST] Multicast traffic not forwarded over P2P DMVPN phase 1 tunnel
CSCwt22006	Web UI bootstrapping failure due to invalid configuration causes persistent config merge errors despite subsequent corrections
CSCwt29648	BadIpChecksum drop when Segment-routing MPLS is configured over IPSEC/GRE over VDSL interface on C8200
CSCwt28048	Preferred-color-group restrict is not honored in data policy
CSCws99246	Regarding the operation enabling communication from outside the NAT
CSCwp97178	v1718/polaris: flapping nat will casue bfd session down with ipsec session shown
CSCwr76176	BFD SD-WAN PMTUD: PMTU Converges Unexpectedly to 970 Bytes After dbg2:1 Event
CSCwt22873	High QFP Caused by " all-host" Limit in - Carrier Grade NAT mode
CSCwt60648	FIPS support for DC in 26.1.2 throttle.
CSCwt87499	Device not sending ICMPv6 Parameter Problem messages in response to incorrect headers on SVI interface

Compatibility

ROMMON compatibility matrix for Cisco 8200 and Cisco 8300 Series Secure Routers

This table lists the ROMMON requirements for Cisco 8200 and Cisco 8300 Series Secure Routers only. There are no separate ROMMON requirements for these routers:

- Cisco 8400 Series Secure Routers
- Cisco 8500 Series Secure Routers

Table 5. Supported ROMMON release for Cisco IOS XE 26.1.x releases

Platforms	Cisco IOS XE Release	Minimum ROMMON Release supported for IOS XE	Recommended ROMMON Release supported for IOS XE
Cisco 8100 Series Secure Routers			
C8130-G2	26.1.1	17.18(1r)	26.1(2r)
C8140-G2	26.1.1	17.18(1r)	26.1(2r)
C8151-G2	26.1.1	17.18(1r)	26.1(2r)
C8161-G2	26.1.1	17.18(1r)	26.1(2r)
C8131-G2	26.1.1	26.1(4r)	26.1(4r)
C8130-VAI-G2	26.1.1	26.1(3r)	26.1(3r)
C8130-VAP-G2	26.1.1	26.1(3r)	26.1(3r)
C8151-CVAI-G2	26.1.1	26.1(3r)	26.1(3r)
C8151-CVAP-G2	26.1.1	26.1(3r)	26.1(3r)
Cisco 8200 Series Secure Routers			
C8231-G2	26.1.1	17.18(1.5r).s1.cp	17.18(1.12r).s1.cp
C8235-G2	26.1.1	17.18(1.5r).s1.cp	17.18(1.12r).s1.cp
C8231-E-G2	26.1.1	17.18(1.5r).s1.cp	17.18(1.12r).s1.cp
C8235-E-G2	26.1.1	17.18(1.5r).s1.cp	17.18(1.12r).s1.cp
Cisco 8300 Series Secure Routers			
C8375-E-G2	26.1.1	17.15(3.2r).s2.cp	17.15(3.3r).s2.cp
C8355-G2	26.1.1	17.15(1.18r).s2.cp	17.15(3.3r).s2.cp

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

Paltform	Guides
Cisco 8100 Series Secure Routers	Hardware Installation Guide for Cisco 8100 Series Secure Routers Software Configuration Guide for Cisco 8100 Series Secure Routers
Cisco 8200 Series Secure Routers	Hardware Installation Guide for Cisco 8200 Series Secure routers Cisco 8200 Series Secure Routers Software Configuration Guide
Cisco 8300 Series Secure Routers	Hardware Installation Guide for Cisco 8300 Series Secure Routers Software Configuration Guide for Cisco 8300 Series Secure Routers
Cisco 8400 Series Secure Routers	Hardware Installation Guide for Cisco 8400 Series Secure Routers Software Configuration Guide for Cisco 8400 Series Secure Routers
Cisco 8500 Series Secure Routers	Hardware Installation Guide for Cisco 8500 Series Secure Routers Software Installation Guide for Cisco 8500 Series Secure Routers
Licensing	Cisco 8000 Series Secure Routers Licensing

Legal information