



Release Notes for Cisco 8500 Series Secure Routers, Release 17.18.x

Cisco 8500 Series Secure Routers, Release 17.18.x	3
New hardware features.....	3
New software features.....	3
Resolved issues	5
Open issues.....	6
Related resources.....	8
Legal information	8

Cisco 8500 Series Secure Routers, Release 17.18.x

Cisco IOS XE 17.18.2 is the first release for Cisco 8500 Series Secure Routers 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

This document describes the features and issues for Cisco 8500 Series Secure Routers, Release 17.18.x.

For more information on the features and specifications of Cisco 8500 Series Secure Routers, see the [Cisco 8500 Series Secure Routers Datasheet](#)

New hardware features

There are no new hardware features in this release.

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 17.18.3a

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 Cisco 8500 Series Secure Routers, Release 17.18.2

Product impact	Feature	Description
Software Reliability	High availability for DHCP servers	In a high availability set up DHCP servers are deployed in an active/standby deployment model where two Cisco IOS XE DHCP servers synchronize DHCP bindings (IP address records). This synchronization ensures that if the active device fails, the standby device seamlessly assumes the Active role, preserving IP address records and maintaining uninterrupted network service.
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 OSPFv2	From Cisco IOS XE 17.18.2 this feature extends IPv4 GRE-TP tunnel as protected link support for SR-MPLS TILFA with OSPFv2.

Product impact	Feature	Description
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 TI-LFA with IS-IS.
Security	Resilient Infrastructure	<p>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 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 authentication and encryption <i>Recommendation:</i> Use SNMPv3 with authentication and encryption (authPriv). • MD5 (authentication) and 3DES (encryption) in SNMPv3 <i>Recommendation:</i> Use SHA1 or, preferably, SHA2 for authentication, and AES for encryption. • IP source routing based on IP header options <i>Recommendation:</i> Do not use this legacy feature. • TLS 1.0 and TLS 1.1 <i>Recommendation:</i> Use TLS 1.2 or later. • TLS ciphers using SHA1 for digital signatures <i>Recommendation:</i> Use ciphers with SHA256 or stronger digital signatures. • HTTP <i>Recommendation:</i> Use HTTPS. • Telnet

Product impact	Feature	Description
		<p><i>Recommendation:</i> Use SSH for remote access.</p> <ul style="list-style-type: none"> • FTP and TFTP <i>Recommendation:</i> Use SFTP or HTTPS for file transfers. • On-Demand Routing (ODR) <i>Recommendation:</i> Use a standard routing protocol in place of CDP-based routing information exchange. • BootP server <i>Recommendation:</i> Use DHCP or secure boot features such as Secure ZTP. • TCP and UDP small servers (echo, chargen, discard, daytime) <i>Recommendation:</i> Do not use these services on network devices. • IP finger <i>Recommendation:</i> Do not use this protocol on network devices. • NTP control messages <i>Recommendation:</i> Do not use this feature. • TACACS+ using pre-shared keys and MD5 <i>Recommendation:</i> Use TACACS+ over TLS 1.3, introduced in release Cisco IOS XE 17.18.1

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 17.18.3a

Table 2. Resolved issues for Cisco 8500 Series Secure Routers, Release 17.18.3a

Bug ID	Description
CSCwr90843	SD-WAN Edge: Device May Reload Unexpectedly Under Heavy IPSec Traffic Load
CSCws28994	CPP crash while processing QoS rate profile
CSCwt22873	High QFP Caused by "all-host" Limit in - Carrier Grade NAT mode
CSCws72902	Overrun drops due to uneven GRE traffic distribution across data plane cores
CSCwq60752	Device FP Crash After Clearing NAT Translations

Bug ID	Description
CSCws30718	Dataplane Crash Observed on CGN NAT Scale Router after " clear ip nat translation *"
CSCws76668	Memory leak udner " fman_fp_image" on CAT8500 routers when NAT is enabled.
CSCws77372	Software crash with fman_fp core due to NAT-related show commands
CSCwt18839	Segmentation Fault in cpp_cp_svr while Printing FIA Trace Data
CSCwr44547	SDWAN Manager : Reporting abnormal loss value for tunnel stats in the UI
CSCwr84985	dmiauthd process crashes, due to which the configuration does not sync between startup-config and the running-config.
CSCws58529	When the name server is specified using IPv6, half entries are created due to unintended NAT.
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

Resolved issues in Cisco IOS XE 17.18.2

Table 3. Resolved issues for Cisco 8500 Series Secure Routers, Release 17.18.2

Bug ID	Description
CSCwr42950	SD-WAN 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	cEdge: device may boot up into prev_packages.conf due to power outage.
CSCwr77958	NWPI not capturing self-generated syslog traffic.
CSCwi61730	Device crash when removing SGT caching on an interface.
CSCwq77322	Router sending a 2 Byte packet of FLOW_SAMPLER_RANDOM_INTERVAL instead of a 4-Byte packet.
CSCwr24031	After upgrade to 17.15 for earlier releases 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	Crash when initializing DNS channels .

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 17.18.3a

Table 4. Open issues for Cisco 8500 Series Secure Routers, Release 17.18.3a

Bug ID	Description
CSCwq96185	SD-WAN: High Memory Usage and Unexpected Reload Due to a vDaemon Memory Leak
CSCwt69544	QFP Ucode device crash on 17.15.4c
CSCwt45748	Crash while processing packet in AppNav Tunnel
CSCwt25957	Issue with editing security policy after controller upgrade.

Open issues in Cisco IOS XE 17.18.2

Table 5. Open issues for Cisco 8500 Series Secure Routers, Release 17.18.2

Bug ID	Description
CSCws30834	cEdge ignore the keepalive command under the SIG tunnel interface pushed by the vmanage.
CSCws13857	Incorrect NAT translation from service-vrf to global for self-generated ICMP 11 (Time Exceeded) packets.
CSCwq77458	fman crash after fnf config changes.
CSCwr87083	Not able to onboard sd-routing devices using generic bootstrap file stored in usb.
CSCws12946	cEdge port forward issue with multiple ISP.
CSCws18137	Out of sync when CLI Template was attached (missing element: authentication in /ios:native/ios:line/ios:vtty[ios:first='0']/ios:login/ios:authentication).
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.
CSCwr08462	There seems to be an issue where the NAT router is not responding to ARP requests.
CSCwr44921	SDWAN cEdge Router Crashes - CPU Usage due to Memory Pressure exceeds threshold.
CSCwr97784	Slow performance on Netconf RPC on 17.15.2a on stateless static NAT translation.

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.
CSCwrm97460	17.9 cEdges - 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	Router experienced Critical process ompd fault on rp_0_0.
CSCwr72709	Router crash in TDM-TDM call when debug voip fpi enabled.
CSCwq98154	[XE MCAST] 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	SD-WAN Edge: Periodic Service Restart May Generate Crash Files.
CSCwr64257	Unexpected reload on ftdm SDWAN device.
CSCws26373	cEdge experiences an unexpected reboot due to NAT in the data-plane after a policy push.
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.
CSCwr77083	Router crashed in crypto library.

Related resources

- [Hardware Installation Guide for Cisco 8500 Series Secure Routers](#)
- [Software Installation Guide for Cisco 8500 Series Secure Routers](#)
- [Cisco 8000 Series Secure Routers Licensing](#)

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.