Release Notes for Cisco 8200 Series Secure Routers, Release 17.18.x

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco 8200 Series Secure Routers, Release 17.18.x 3
New hardware features 3
Resolved issues 3
Open issues 10
Compatibility 12
Related resources 13
Legal information 13

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco 8200 Series Secure Routers, Release 17.18.x

Cisco IOS XE 17.18.1a is the first release for the Cisco 8200 Series Secure Routers in the Cisco IOS XE 17.18.x release series.

Cisco 8200 Series Secure Routers deliver secure networking simplified. Powered by the all-new secure networking processor and the unified Cisco secure networking platform, Cisco 8200 Series Secure Routers deliver robust, platform-level security, advanced performance engineering via routing and SD-WAN, and on-premises, infrastructure-as-code, or cloud management flexibility that enables businesses to seamlessly scale and grow. Each class of secure routers is designed to deliver risk reduction, enhanced reliability, and future readiness.

For information on the hardware features supported on the Cisco 8200 Series Secure Routers, refer to the Cisco 8200 Series Secure Routers datasheet.

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 17.18.1a

Table 1. New hardware features for Cisco 8200 Series Secure Routers, Release 17.18.1a

Feature	Description
Cisco 8200 Series Secure Routers	From Cisco IOS XE17.18.1a, Cisco 8200 Series Secure Routers are available in these models: ◦ C8231-G2 ◦ C8235-G2 ◦ C8231-E-G2 ◦ C8235-E-G2

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 17.18.5

There are no new features in this release.

New software features in Cisco IOS XE 17.18.4

There are no new features in this release.

New software features in Cisco IOS XE 17.18.3a

There are no new features in this release.

New software features in Cisco IOS XE 17.18.2

Table 2. New hardware features for Cisco 8200 Series Secure Routers, Release 17.18.2

Product impact	Feature	Description
Security	Resilient Infrastructure	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

© 2025 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
		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. 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: • **Plain-text and weak credential storage**: Type 0 (plain text), 5 (MD5), or 7 (Vigenère cipher) in configuration files. Recommendation: Use Type 6 (AES) for reversible credentials, and Type 8 (PBKDF2-SHA-256) or Type 9 (Scrypt) for non-reversible credentials. • **SSHv1** Recommendation: Use SSHv2. • **SNMPv1 and SNMPv2, or SNMPv3 without authentication and encryption** Recommendation: Use SNMPv3 with authentication and encryption (authPriv). • **MD5 (authentication) and 3DES (encryption) in SNMPv3** Recommendation: Use SHA1 or, preferably, SHA2 for authentication, and AES for encryption. • **IP source routing based on IP header options** Recommendation: Do not use this legacy feature. • **TLS 1.0 and TLS 1.1** Recommendation: Use TLS 1.2 or later. • **TLS ciphers using SHA1 for digital signatures** Recommendation: Use ciphers with SHA256 or stronger digital signatures. • **HTTP** Recommendation: Use HTTPS. • **Telnet** Recommendation: Use SSH for remote access. • **FTP and TFTP** Recommendation: Use SFTP or HTTPS for file transfers. • **On-Demand Routing (ODR)** Recommendation: Use a standard routing protocol in place of CDP-based routing information exchange. • **BootP server** Recommendation: Use DHCP or secure boot features such as Secure ZTP. • **TCP and UDP small servers** (echo, chargen, discard, daytime) Recommendation: Do not use these services on network devices. • **IP finger**

© 2025 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
		Recommendation: Do not use this protocol on network devices. • **NTP control messages** Recommendation: Do not use this feature. • **TACACS+ using pre-shared keys and MD5** Recommendation: Use TACACS+ over TLS 1.3, introduced in release Cisco IOS XE 17.18.1
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.
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 TILFA with ISIS.
Ease of use	Configure vDSP	Configure vDSP to enable voice processing functions such as transcoding, conferencing and hardware media termination point services.

New software features for Cisco IOS XE 17.18.1a

Table 3. New software features for Cisco 8200 Series Secure Routers, Release 17.18.1a

Product impact	Feature	Description
Licensing Process	Cisco 8200 Series Secure Routers licensing	Cisco 8200 Series Secure Routers supports platform-based licensing, a way of grouping licenses and devices based on platform-classes. A platform class is a hierarchical categorization based on the product family and place in the network. In this platform-based licensing model, Essentials and Advantage licenses are available. License portability is supported across devices within the same platform class and usage of the same license across different modes is also possible.
Ease of Use	Tamper Detection notification	From Cisco IOS XE 17.18.1a, you can identify potential tampering on the Cisco 8200 Series Secure routers by using the platform tamper detection command in config mode.

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.

© 2025 Cisco and/or its affiliates. All rights reserved.

Resolved issues in Cisco IOS XE 17.18.5

Table 4. Resolved issues for Cisco 8200 Series Secure Routers, Release 17.18.5

Bug ID	Description
CSCwu97838	RADSEC TLS peer validation fails when unrelated trustpoints share a common PKI Root CA
CSCwv55092	17.9 to 17.15.4c upgrade rollback due to recursive SNMP BGP trap deprecated-model migration
CSCwq96185	High Memory Usage and Unexpected Reload Due to a vDaemon Memory Leak
CSCwu97716	Unexpected Device Reload Triggered by DHCP Service Failure During Lease Conflict Scenarios
CSCwu83262	L2TPv3 xconnect session fails to establish when the traffic traverses through IPsec tunnel interface.
CSCwu27070	Unexpected Reload in CPP Server (cpp_sp_svr) Code
CSCwu12631	Posture redirection not working on Sdwan router switch module
CSCwt81568	Route-replicate command is present in configuration but is not taking effect after reload.
CSCww06413	PKCS12 re-import silently fails to install a CA certificate
CSCwt42293	Cellular interface flap causing crypto enrollment failure
CSCwr02102	Router intermittently loses ip address dynamically assigned to tunnel interface
CSCwt98537	QoS unsupported configuration makes route processor crash
CSCwq08386	Device platform Tier 3 throughput clarification
CSCwt75037	Device in controller mode crashes with Critical process cpp_ha_top_level_server fault on fp_0_0 (rc=69)
CSCwr69095	DNS requests for vBond fail
CSCwu00043	LSC certificate failure " CRYPTO_PKI: Failed to add ca req pool entry 538" in scale environment
CSCwu61766	SDWAN edge router OMPD crash on malformed SD-WAN identity IP-to-user update from vSmart pxGrid integration
CSCws92932	Unexpected reload due to Segmentation Fault on TPS IPC Process
CSCwu27937	system-report handling has a conflict - unrelated processes may dump core after a cpp/ucode fault.
CSCwt66413	ncsshd process fails to terminate after " no netconf" and netconf refuses connection
CSCwt56693	L2TP: Seeing " protocol l2tpv2 L2TP_CLASS_011" config getting lost with clear ppp all cli
CSCws80808	Loopback interface in Mgmt-intf VRF becomes unreachable via Management interface
CSCwt13176	Memory leak detected in TLS testcase
CSCwt84502	Critical Process cpp_ha_top_level_server crash (rc=69) Crash after adding zone based firewall setup configuration on the router

© 2025 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwv37592	Unable to configure no exec under async line or async range IOS-XE SDWAN 17.15
CSCwu21682	Segmentation Fault at Process = SASCheckInit (or other process)
CSCwu93056	Device may reload after remove an endpoint.
CSCwt51797	RIPv2 will stop sending multicast routing updates after interface flap
CSCwu47545	Ucode Code Crash while Printing Log for FW Drop for Packet with Invalid Header
CSCwr74339	Hydra: vman crashed @ __GI___clock_nanosleep in router reload and power cycle test
CSCwr47230	Upgrade failed " Install operation not allowed because verification of image ..... is in progress."
CSCwt69544	QFP Ucode C8500L crash
CSCwu97638	IOS-XE unexpected reload due to ACL pointer corruption with SNMPv3
CSCwt51754	Router reloaded after adding voice related configuration
CSCwt25903	Not able to disable " log" feature in NGFW Policies vManage for " Drop" rules.
CSCwu45273	LISP ITR sources locally-originated control-plane packets from the numerically lowest configured RLOC IP instead of the outbound interface address
CSCwu11498	show interface counter become abnormal
CSCwv39390	IOS-XE router generates FMANRP_ESS-3-ERREVENT logs with tracebacks
CSCwu76495	Crash while updating Adaptive QOS Session Policy due to minimal traffic size
CSCwt34226	SSH Connectivity Issue with On-Demand Next Hop in Segment Routing Traffic Engineering (SR-TE)
CSCwt29648	BadIpChecksum drop when Segment-routing MPLS is configured over IPSEC/GRE over VDSL interface on C8200
CSCwu01733	Rapid memory leak in ompd after ISE integration with vManage
CSCwu49029	Unexpected reload on CGM (Class-Group Manager) when updated
CSCwu51162	Unexpected reload on router in SDWAN CCE (Classifier and Classification Engine)
CSCwv41407	Device: BGP updates that should be suppressed are advertised with incorrect attribute after RPSO
CSCwv97208	LISP xTR may retain a stale Registering ETR session after dual-WAN failback, delaying Map-Register update to the Map-Server for 67 minutes
CSCwt88212	Untagged packets dropped with non-default native VLAN on ISR4K
CSCwq98154	Multicast traffic not forwarded over P2P DMVPN phase 1 tunnel
CSCwr24042	Traffic going to all CEDGES without receivers where Replicator stuck in P MDT
CSCwu99434	Unexpected Device Reload During Rapid Trustpoint Deletion and Creation Events Resulting in Core File Generation

© 2025 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwv25890	Support for GRE+MPLS on tunnel transport mode
CSCwv18610	Packet Reordering for MPLS Flows in GRE+IPSEC tunnels

Resolved issues in Cisco IOS XE 17.18.4

Table 5. Resolved issues for Cisco 8200 Series Secure Routers, Release 17.18.4

Bug ID	Description
CSCwt76906	C9K: Continuous increase in holding memory for CTS CORE
CSCwt47516	WLC crash due to corrupted length field during AAA processing
CSCwt94106	Pubd core generated for C9300
CSCwu04279	System instability and potential service disruption after invalid GPM load
CSCwu03804	C9000: Randomly during operation - Interface VLAN / SVI go missing from " show run" but remain up. Configs are lost upon reload.
CSCwu21451	C9250/C9350: Cluster manager crash for stacked devices with specific mac address combination
CSCwt51443	Controller crashed due to CPUHOG under DBAL_EVENTS
CSCwt86654	IOS-XE: IKEv2 process crash caused by stack buffer overflow during AnyConnect EAP credential parsing
CSCwu02602	DBAL EVENTS crash seen while trying to push config group to C8570-G2/C8500-12x4QC in SDWAN and SD-Routing
CSCwn80721	Unexpected Reboot in Process Sessmgrd
CSCwt87294	mDNS Cache-Flush behavior not consistent

Resolved issues in Cisco IOS XE 17.18.3a

Table 6. Resolved issues for Cisco 8200 Series Secure Routers, Release 17.18.3a

Bug ID	Description
CSCwr90843	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
CSCws95993	Seeing T1 license in use even after configuring T2.

© 2025 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwq60752	Device FP Crash After Clearing NAT Translations
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
CSCwr72709	Router crash in TDM-TDM call when debug voip fpi enabled
CSCws66278	Unable to install Cisco PKI controller certs on MT overlay
CSCws68039	Unable to configure HSRP Groups up to the maximum limit
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 7. Resolved issues for Cisco 8200 Series Secure Routers, Release 17.18.2

Bug ID	Description
CSCwr42950	Device 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	Device may boot up into prev_packages.conf due to power outage.
CSCwr77958	NWPI not capturing self-generated syslog traffic.
CSCwj61730	Device crash when removing SGT caching on an interface.
CSCwq77322	Device sending a 2 Byte packet of FLOW_SAMPLER_RANDOM_INTERVAL instead of a 4-Byte packet.
CSCwr24031	After upgrade to earlier releases sd-wan service-tracker in vrf selects source IP address from GRT when MPLS Inter-AS VPN option B configured.

© 2025 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwr49794	Device exporters with ETA enabled are generating invalid template data errors in SNA.
CSCwq98206	EPBR set interface action get missing after reboot.
CSCwr25077	Device crash when initializing DNS channels.

Resolved issues in Cisco IOS XE 17.18.1a

There are no customer impacting bugs that were fixed in this release.

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 17.18.5

Table 8. Open issues for Cisco 8200 Series Secure Routers, Release 17.18.5

Bug ID	Description
CSCwv71880	SD-WAN redirect-dns Destination NAT session collides with SIG tunnel IKEv2 control plane traffic
CSCws94603	Crashes During CRL Fetch Failure due memory reallocation
CSCwv68329	Static NAT DIA routes intermittently withdrawn/not reinstalled after transport tracker/TLOC flap
CSCwv60786	Intermittent issue with RRI being lost on the Flex Hub
CSCwv73701	Packet reordering observed when application performance-monitor service policy enabled
CSCwt63505	Device crashed while authenticating trustpoint with DNAC

Open issues in Cisco IOS XE 17.18.4

There are no customer impacting bugs that were identified in this release.

Open issues in Cisco IOS XE 17.18.3a

Table 9. Open issues for Cisco 8200 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

© 2025 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwt25957	Issue with editing security policy after controller upgrade.

Open issues in Cisco IOS XE 17.18.2

Table 10. Open issues for Cisco 8200 Series Secure Routers, Release 17.18.2

Bug ID	Description
CSCws30834	Device 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	Device not able to onboard sd-routing devices using generic bootstrap file stored in USB.
CSCws12946	Device port forward issue with multiple ISP.
CSCws18137	Out of sync when CLI Template was attached (missing element: authentication in /ios:native/ios:line/ios:vty[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	Device 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	Device Crashes - CPU Usage due to Memory Pressure exceeds threshold.
CSCwr97784	Slow performance on Netconf RPC on stateless static NAT translation.
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.
CSCwq24119	Traceback seen when detaching the CN railways customer configs.
CSCwm97460	Control Connection to vManage is only Attempted over Highest Priority TLOC.

© 2025 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwr00088	Add CLI to change per MPLS label CEF statistics query interval on FMAN FP.
CSCwr55240	Device experienced Critical process ompd fault on rp_0_0.
CSCwr72709	Device crash in TDM-TDM call when debug voip fpi enabled.
CSCwq98154	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	Periodic Service Restart May Generate Crash Files.
CSCwr64257	Unexpected reload on ftmd SDWAN device.
CSCws26373	Device experiences an unexpected reboot due to NAT in the data-plane after a policy push.
CSCwp97178	Flapping nat will casue bfd session down with ipsec session shown.
CSCwr76176	PMTU Converges Unexpectedly to 970 Bytes After dbg2:1 Event.
CSCwr77083	Device crashed in crypto library.

Open issues in Cisco IOS XE 17.18.1a

Table 11. Open issues for Cisco 8200 Series Secure Routers, Release 17.18.1a

Bug ID	Description
CSCwo53342	Device: bfd may be flapping when save configuration with write cmd.
CSCwq00263	ipv6 ipsec tunnel, ping failed with specific size.
CSCwk74329	Counters are cleared after shut/no shut gi0 interface.
CSCwo44899	selinux: vmanage failed to factory reset device caused by selinux deny.
CSCwq58084	Device: POE module insert time incorrect if reloading with future time and then sync back to correct time source.
CSCwo62154	Crash Encountered During PIM Swap quickly on device.

Compatibility

ROMMON compatibility matrix

The table lists the ROMMON releases supported in Cisco IOS XE 17.18.x releases.

© 2025 Cisco and/or its affiliates. All rights reserved.

Platforms	Cisco IOS XE Release	Minimum ROMMON Release supported for IOS XE	Recommended ROMMON Release supported for IOS XE
C8231-G2	17.18.1a	17.18(1.5r).s1.cp	17.18(1.12r).s1.cp
C8235-G2	17.18.1a	17.18(1.5r).s1.cp	17.18(1.12r).s1.cp
C8231-E-G2	17.18.1a	17.18(1.12r).s1.cp	17.18(1.12r).s1.cp
C8235-E-G2	17.18.1a	17.18(1.12r).s1.cp	17.18(1.12r).s1.cp

Related resources

- Hardware Installation Guide for Cisco 8200 Series Secure routers
- Cisco 8000 Series Secure Routers Licensing
- Cisco 8200 Series Secure Routers Software Configuration Guide

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.