Release Notes for Cisco 8300 Series Secure Routers, Release 17.18.x

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

Contents

Cisco 8300 Series Secure Routers, Release 17.18.x 3
Resolved issues 8
Open issues 13
Compatibility 16
Related resources 16
Legal information 16

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

Cisco 8300 Series Secure Routers, Release 17.18.x

Cisco 17.18.1a is the first release for Cisco 8300 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

For information on the hardware features supported on the Cisco 8300 Series Secure Routers, refer to the Cisco 8300 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 8300 Series Secure Routers, Release 17.18.1a

Feature	Description
Cisco 8300 Series Secure Routers	From Cisco IOS XE 17.18.1a, Cisco Secure Series Routers introduces C8355-G2 routers.
C-NIM-WAN-2X and C-NIM-WAN-4S	The Cisco C-NIM-WAN-2X and C-NIM-WAN-4S are the next generation Form-factor WAN NIM modules that provide enhanced security, reliability, and performance.

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 17.18.5

There are no new features for this release.

New software features for Cisco IOS XE 17.18.4

There are no new features for this release.

New software features for Cisco IOS XE 17.18.3a

There are no new features for this release.

New software features for Cisco IOS XE 17.18.2

Table 2. New software features for Cisco 8300 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

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

Product impact	Feature	Description
		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protocols that do not provide sufficient security such as those transmitting sensitive data without encryption or using outdated encryption mechanisms.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. 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.

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

Product impact	Feature	Description
		• **IP finger** 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.
CUBE		
Hardware Reliability	CUBE and SRST applications support on C8375-E-G2 router platform	From Cisco IOS XE 17.18.2 onwards, UC applications are supported on C8375-E-G2 router platform.

New software features for Cisco IOS XE 17.18.1a

Table 3. New software features for Cisco 8300 Series Secure Routers, Release 17.18.1a

Product impact	Feature	Description
Ease of Use	Support to upgrade Firmware	From Cisco IOS XE 17.18.1a release, you can now upgrade the firmware image for cellular module, LTE module, or Wi-Fi module of supported devices using Cisco Catalyst SD-WAN Manager, without configuring and managing multiple commands for each device and its associated modules.
Licensing Process	Cisco 8300 Series Secure Routers licensing	Cisco 8300 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

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

Product impact	Feature	Description
		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 8300 Series Secure routers by using the platform tamper detection command in config mode.
Ease of Use	Enable Auto-off port LEDs	From Cisco IOS XE 17.18.1a, you can enable or disable the Port LEDs on the Cisco 8300 Series Secure routers using the **hw-module auto-off led** command in config mode. This feature is disabled by default.
Ease of Use	Enable Blue Beacon	From Cisco IOS XE 17.18.1a, you can enable the Blue Beacon LED on the Cisco 8300 Series Secure routers using the **hw-module beacon R0** command, to identify a specific device in environments where multiple devices are installed.
Ease of Use	Managing NGFW Policies from Security Cloud Control	Security Cloud Control is a cloud-based multi-device manager that facilitates management of security policies to achieve consistent policy implementation. Security Cloud Control helps optimize your security policies by identifying inconsistencies with them and by giving you tools to fix the inconsistencies. From Cisco IOS XE 17.18.1a release, you can integrate Cisco SD-WAN Manager with Security Cloud Control, which allows you to import existing NGFW policies, security objects, and security profiles into Security Cloud Control. With this integration, you can share objects and policies as well as make configuration templates to promote policy consistency across devices.
Ease of Use	Hosted Edge Services for SD-Routing Devices	From Cisco IOS XE 17.18.1a release, Cisco Catalyst SD-WAN Manager supports deployment of IOx applications such as Cyber Vision, Thousand Eyes, UTD, and so on. The support to monitor these applications is introduced through Hosted Edge Services monitoring dashboard which offers a simplified user experience for overseeing IOx container applications across multiple devices. The Hosted Edge Services monitoring dashboard is introduced on Cisco Catalyst SD-WAN Manager version 20.18. x.
Ease of setup	Cisco Secure Routers Swim and Onboarding Tool	Cisco IOS XE 17.18.1a introduces the Cisco Secure Routers Swim and Onboarding tool that helps customers upgrade and onboard autonomous hardware devices to cloud-hosted or on-premises Catalyst Cisco SD-WAN Manager.
Licensing Process	Licensing compliance, reporting, and notification enhancements	From Cisco IOS XE 17.18.1a release, you can view additional information in your licensing report such as out of compliance and the reason for out of compliance, the number of licenses that have been assigned in the network, how many devices have been assigned licenses, per-device license details, and so on. In addition, you can now connect to the Enterprise Agreement (EA) portal directly from the Cisco SD-WAN Manager with your Smart Account credentials. This helps you to generate the required quantities of licenses for the selected Commerce SKU of EA and deposit them to your desired CSSM Virtual Accounts (VA).
Ease of use	Managing NGFW Policies from Security Cloud Control	Security Cloud Control (SCC) is a cloud-based multi-device manager that facilitates management of security policies to achieve consistent policy implementation. SCC helps optimize your security policies by identifying inconsistencies with them and by giving you tools to fix the inconsistencies. From Cisco IOS XE 17.18.1a release, you can integrate Cisco SD-WAN Manager with SCC, which allows you to import existing NGFW policies, security objects, and security profiles into SCC. With this

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

Product impact	Feature	Description
		integration, you can share objects and policies as well as make configuration templates to promote policy consistency across devices.
Security	Custom IPS signature sets	From Cisco IOS XE 17.18.1a release, Custom IPS signature sets are supported in Cisco SD-WAN Manager, which allows you to create and deploy personalized Snort3 IPS signature sets. This feature allows direct modification of actions for existing IPS rules within profiles and supports building custom rules using rule groups or existing rules. With Custom IPS signature sets, organizations can gain greater control and precision in tailoring threat detection to their specific security needs.
Ease of Use	Certificate Management on SD-Routing Devices	This feature introduces a new certificate authorization setting, Enterprise Certificate Settings, which unifies certificate configurations for SD-Routing devices. Cisco SD-WAN Manager automates certificate management by leveraging protocols like EST (Enrolment over Secure Transport) and SCEP (Simple Certificate Enrolment Protocol). The feature automates the enrolment, and renewal of certificates.
Ease of use	Configure cellular band select for cellular interfaces on SD-Routing devices	You can select specific frequency bands to which the device can connect to, allowing optimized connection depending on location and network availability. This configuration can be done using Feature Parcels in Catalyst Cisco SD-WAN Manager.
Ease of use	Configure logging of crash dump events for cellular interfaces on SD-Routing devices	You can configure the device to collect the crash dump logs by enabling the boot-and-hold mode on the device using the lte modem crash-action boot-and-hold command.
Ease of use	Reset cellular profile for cellular interfaces on SD-Routing devices	You can reset the cellular network profile settings on a specific interface to a factory default state using the cellular<slot> lte profile reset command.
Ease of use	Enable diagnostic monitoring for SD-Routing devices	You can enable diagnostic monitoring log capture for devices with cellular interfaces using Catalyst Cisco SD-WAN Manager.
Ease of Use	Show drops command	The *show drops* command is introduced in Cisco IOS XE 17.18.1a. This command consolidates multiple platform and protocol-specific debugging tools into a single, user-friendly interface, enabling network operators to efficiently identify the root causes of packet drops. By streamlining the troubleshooting process, this feature significantly improves operational efficiency and network performance.
Upgrade	MVPN Ingress Replication (IR) over SRv6	This feature enables the transport of IPv4 MVPN traffic across an SRv6 network. It simplifies multicast deployment by using the existing SRv6 unicast infrastructure as the underlay. With this feature, the ingress PE router receives multicast traffic and creates a separate unicast SRv6-encapsulated copy for each egress PE router in the multicast group.
Upgrade	SRv6 Path MTU Discovery	This feature introduces a mechanism to determine the maximum transmission unit (MTU) for packets traversing an SRv6 underlay network. It ensures efficient packet forwarding by preventing fragmentation and packet drops, thereby allowing network devices to dynamically adjust packet sizes to avoid exceeding link MTU limits. The system relays ICMP Packet Too Big (PTB) messages from the SRv6 underlay to the IPv6/IPv4 overlay network, supporting both Transit-node and Headend-node PTB relay methods.

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

Product impact	Feature	Description
Upgrade	SRv6 Flex-Algo with TI-LFA and uLoop Avoidance	From Cisco IOS XE 17.18.1a, Flexible Algorithm enhances SRv6 by including functions like Topology Independent Loop-Free Alternate (TI-LFA) and microloop (uLoop) avoidance. This feature improves network resilience and efficiency.
Licensing Process	Product Analytics for routers	Product Analytics refers to the collection of product telemetry such as product performance and resource usage information directly from IOS-XE-based routing platforms. From Cisco IOS XE 17.18.1a release, Product Analytics is enabled by default when. Use this functionality to gain data insights such as product performance, feature consumption, and the licensing types that suit your requirements best.
Ease of use	Crypto Throughput Logging	Starting with Cisco IOS XE 17.18.1a, network administrators can monitor and manage crypto throughput drops on Cisco Catalyst 8300 and Catalyst 8200 Series Edge Platforms. This feature sends syslog messages to notify you when crypto throughput drops, offering better visibility and management.
CUBE Features		
Ease of use	Enhanced support for serviceability in SIP recording	From Cisco IOS XE 17.18.1a onwards, serviceability is enhanced to display consolidated information on forked and associated anchor call legs.
Upgrade	Third-Party GUID capture for correlation between call transfers and SIP-based recording	From Cisco IOS XE 17.18.1a onwards, the Third-Party GUID capture for correlation between calls and SIP-based recording is extended to support transmission of globally unique identifiers (GUIDs) to the recording server during call transfers.
Upgrade	IOS UC apps reports smart licensing flex subscription entitlement tag	From Cisco IOS XE 17.18.1a onwards, CUBE and SRST smart licensing reports flex subscription entitlement tag on all the supported platforms.

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 17.18.5

Table 4. Resolved issues for Cisco 8300 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

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

Bug ID	Description
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
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

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

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

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

Resolved issues in Cisco IOS XE 17.18.4

Table 5. Resolved issues for Cisco 8300 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 8300 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
CSCws95993	Seeing T1 license in use even after configuring T2.
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 routers when NAT is enabled.
CSCws77372	Software crash with fman_fp core due to NAT-related show commands

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

Bug ID	Description
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 8300 Series Secure Routers, Release 17.18.2

Bug ID	Description
CSCwr42950	On-Demand Tunnels do not expire when UMTS Is enabled.
CSCwq51935	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 for earlier releases sd-wan service-tracker in vrf selects source IP address from GRT when MPLS Inter-AS VPN option B configured.
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.

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

Resolved issues in Cisco IOS XE 17.18.1a

Table 8. Resolved issues for Cisco 8300 Series Secure Routers, Release 17.18.1a

Bug ID	Description
CSCwo05703	VFR is not dynamically disabled after ZBFW removal.
CSCwn26353	BFD sessions via TLOC-Ext do not come up when IPv6 is dynamically changed.
CSCwo84428	Memory leak under vdaemon process with DTLS on SNMP polling.
CSCwm27749	Speed test download / Throughput issue on device seen with IPSEC ESP-NULL transform using Zscaler.
CSCwo75657	Maximum control connection not equal to maximum omp sessions.
CSCwp15042	Module stays down without hw slot reload.
CSCwm72336	CXP with Data Policy redirect-DNS via Overlay causes Blackhole.
CSCwn69868	Unable to come up control connections with controllers after controllers added and down/up.
CSCwp24639	Devices reload after vpn config changes.
CSCwn42496	Encore crashed @bfd_send_and_detect_sleep_time during soak run.
CSCwo72675	All BFD sessions for dialer interfaces are down. SA ID is 0 for all of them.
CSCwp91064	FTMD cero pointer deference leading to crash.

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 9. Open issues for Cisco 8300 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

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

Bug ID	Description
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 10. Open issues for Cisco 8300 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
CSCwu39475	C8375-E-G2 reloads due to IOSd DBAL EVENTS segfault in lldp_state_ios_oper/dbal after SD-WAN template push
CSCwt25957	Issue with editing security policy after controller upgrade.

Open issues in Cisco IOS XE 17.18.2

Table 11. Open issues for Cisco 8300 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	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.

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

Bug ID	Description
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 device: 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	Device - 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	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	Device: Periodic service restart may generate crash files.
CSCwr64257	Unexpected reload on ftmd 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	BFD SD-WAN PMTUD: 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 12. Open issues for Cisco 8300 Series Secure Routers, Release 17.18.1a

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

Bug ID	Description
CSCwq40026	Unexpected Reboot due to Process FTMD.
CSCwq20326	Device does not install service-side static route to CEF after upgrade.
CSCwe19394	Device may boot up into prev_packages.conf due to power outage.
CSCwo42664	Keyman core files on device.
CSCwp01089	EPFR-High latency times are observed on the hub device.
CSCwp12196	Device unexpectedly reloads due to memory corruption on a notification queue in FTMd.
CSCwq27426	BFD session down due to unencrypted outbound BFD packets despite active IPsec SA.
CSCwq68385	TLOC Disabled After Link Down No Automatic Tunnel Recovery After Link Restores and TLOC State Is Up.
CSCwo85218	Device takes more than 20s for rekey in sdwan ipsec scale setup

Compatibility

ROMMON compatibility matrix

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

Platforms	Cisco IOS XE Release	Minimum ROMMON Release supported for IOS XE	Recommended ROMMON Release supported for IOS XE
C8375-E-G2	17.18.1a	17.15(3.2r).s2.cp	17.15(3.3r).s2.cp
C8355-G2	17.18.1a	17.15(3.2r).s2.cp	17.15(3.3r).s2.cp

Related resources

- Hardware Installation Guide for Cisco 8300 Series Secure routers
- Smart Licensing Using Policy for Cisco Enterprise Routing Platforms
- Cisco 8300 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.