Release Notes for Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms, Cisco IOS XE Cupertino 17.9.x

First Published: 2022-08-26

Last Modified: 2024-02-29

Full Cisco Trademarks with Software License

About The Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms

The Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms are best-of-breed, 5G-ready, cloud edge platforms designed for accelerated services, multi-layer security, cloud-native agility, and edge intelligence to accelerate your journey to cloud.

Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms with Cisco IOS XE SD-WAN Software deliver Cisco's secure, cloud-scale SD-WAN solution for the branch. The Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms are built for high performance and integrated SD-WAN Services along with flexibility to deliver security and networking services together from the cloud or on premises. It provides higher WAN port density and a redundant power supply capability. The Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms have a wide variety of interface options to choose from—ranging from lower and higher module density with backward compatibility to a variety of existing WAN, LAN, voice, and compute modules. Powered by Cisco IOS XE, fully programmable software architecture, and API support, these platforms can facilitate automation at scale to achieve zero-touch IT capability while migrating workloads to the cloud. The Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms also come with Trustworthy Solutions 2.0 infrastructure that secures the platforms against threats and vulnerabilities with integrity verification and remediation of threats.

The Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms are well suited for medium-sized and large enterprise branch offices for high WAN IPSec performance with integrated SD-WAN services.

For more information on the features and specifications of Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms, refer to the Cisco Catalyst 8300 Series Edge platforms datasheet.

Note SFP ports on C8200-1N-4T platforms can only support 1 GB speed even though the copper SFP module does support the 10/100M speed.

Note Sections in this documentation apply to all models of Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms unless a reference to a specific model is made explicitly.

Note Cisco IOS XE Cupertino17.9.1a is the first release for the Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms in the Cisco IOS XE Cupertino 17.9.x release series.

Product Field Notice

Cisco publishes Field Notices to notify customers and partners about significant issues in Cisco products that typically require an upgrade, workaround or other user action. For more information, see https://www.cisco.com/c/en/us/support/web/field-notice-overview.html.

We recommend that you review the field notices to determine whether your software or hardware platforms are affected. You can access the field notices from https://www.cisco.com/c/en/us/support/web/tsd-products-field-notice-summary.html#%7Etab-product-categories.

New and Changed Hardware and Software Features

New and Changed Hardware Features

There are no new hardware features in this release.

New and Changed Software Features

Feature Navigator

You can use Cisco Feature Navigator (CFN) to find information about the software features, platform, and software image support on Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/.

Note To access CFN, you do not require an account on cisco.com.

New and Changed Software Features in Cisco IOS XE 17.9.5a

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.9.4a

There are no new features in this release. This release provides a fix for CSCwh87343: Cisco IOS XE Software Web UI Privilege Escalation Vulnerability. For more information, see the Security Advisory: cisco-sa-iosxe-webui-privesc-j22SaA4z.

New and Changed Software Features in Cisco IOS XE 17.9.4

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.9.3a

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.9.2a

There are no new software features in this release.

New Software Features

Table 1: Software Features in Cisco Catalyst 8200 and Cisco Catalyst 8300 Series Edge Platforms IOS XE Cupertino 17.9.1a

Feature	Discription
10G SFP Module Support on Cisco Catalyst 8300 Edge Series Platforms	Cisco Catalyst 8300 Edge Series Platforms now supports newer 10G SFP module. For the complete list of supported SFP modules, see the Optics Compatibility Matrix.
IPsec Dual Stack Support on Non Cisco Devices	This feature provides the capabilities to carry both IPv4 and IPv6 traffic using a single IPsec Security Association (SA) that is tunnelled over IPv4. From IOS XE release 17.9.1a onwards, Cisco supports specific subnets in the access control list when the ingress end of the tunnel interface is configured with a third party IPsec client. With the introduction of the SVTI single security association dual stack feature, you can now manage the business-to-business services and other IOT business efficiently.
Support for BGP additional paths with label-unicast unique mode	This enhancement introduces support for configuring BGP additional paths when label-unicast unique mode is configured.
Support for Unicast-to-Multicast Destination Reflection	This feature introduces support for configuration of unicast-to-multicast destination reflection to facilitate unicast-to-multicast destination translation and unicast-to-multicast destination splitting. It also provides the capability for users to translate externally received unicast destination addresses to multicast addresses.
Smart Licensing Using Policy Features	
New mechanism to send data privacy related information	A new mechanism to send data privacy related information was introduced. This information is no longer included in a RUM report. If data privacy is disabled (**no license smart privacy** {**all**|**hostname**|**version**} command in global configuration mode), data privacy related information is sent in a separate sync message or offline file. Depending on the topology you have implemented, the product instance initiates the sending of this information in a separate message, or CSLU and SSM On-Prem initiates the retrieval of this information from the product instance, or this information is saved in an offline file. For more information, see license smart (global config).

Feature	Discription
Hostname support	Support for sending hostname information was introduced. If you configure a hostname on the product instance and disable the corresponding privacy setting (**no license smart privacy hostname** command in global configuration mode), hostname information is sent from the product instance, in a separate sync message or offline file. Depending on the topology you have implemented, the hostname information is received by CSSM, CSLU, and SSM On-Prem. It is then displayed on the corresponding user interface. For more information, see license smart (global config). **Note** With the introduction of this enhancement, the hostname limitation which existed from Cisco IOS XE Amsterdam 17.3.2 to Cisco IOS XE Cupertino 17.8.x – is removed. In these earlier releases, hostname information is not sent or displayed on various licensing utilities (CSSM, CSLU, and SSM On-Prem).

Feature	Discription
RUM Report Throttling	For all topologies where the product instance initiates communication, the minimum reporting frequency is throttled to one day. This means the product instance does not send more than one RUM report a day. The affected topologies are: *Connected Directly to CSSM*, *Connected to CSSM Through CSLU* (product instance-initiated communication), *CSLU Disconnected from CSSM* (product instance-initiated communication), and *SSM On-Prem Deployment* (product instance-initiated communication). This resolves the problem of too many RUM reports being generated and sent for certain licenses. It also resolves the memory-related issues and system slow-down that was caused by an excessive generation of RUM reports. You can override the reporting frequency throttling, by entering the **license smart sync** command in privileged EXEC mode. This triggers an on-demand synchronization with CSSM or CSLU, or SSM On-Prem, to send and receive any pending data. RUM report throttling also applies to the Cisco IOS XE Amsterdam 17.3.6 and later releases of the 17.3.x train, and Cisco IOS XE Bengaluru 17.6.4 and later releases of the 17.6.x train. From Cisco IOS XE Cupertino 17.9.1, RUM report throttling is applicable to *all* subsequent releases.
Virtual Routing and Forwarding (VRF) Support	On a product instance where VRF is supported, you can configure the **license smart vrf** *vrf_string* command and use a VRF to send licensing data to CSSM, or CSLU, or SSM On-Prem. **Note** When using a VRF, the supported transport types are **smart** and **cslu** only.) For more information, see license smart (global config).

ROMMON Compatibility Matrix

The following table lists the ROMMON releases supported in Cisco IOS XE 17.9.x releases.

Table 2: Minimum and Recommended ROMMON Releases Supported on Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms respectively

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	17.9.4	17.3(1r)	17.6(6r)
C8300-2N2S-4T2X|6T	17.9.4	17.3(1.2r)	17.6(6.1r)
Catalyst 8200 Series Edge Platforms			
C8200-1N-4T	17.9.4	17.4(1r)	17.6(6r)
C8200L-1N-4T	17.9.4	17.5(1.1r)	17.6(6r)

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Resolved Bugs - Cisco IOS XE 17.9.5a

Identifier	Headline
CSCwh73350	Router keeps crashing when processing a firewall feature.
CSCwh06834	Using special characters in the password while generating TP generates an invalid TP.
CSCwf23291	Device: write or do write saves configuration but RSA keys /SSH lost after reload.
CSCwc79115	Policy commit failure notification and alarm from Cisco Catalyst SD-WAN Controller.
CSCwh68508	Unexpected reboot after establishing control plane of EVPN MPLS and receiving packets.
CSCwi28227	NAT HSL logging vrf-filter is not working.
CSCwf82676	CPU usage mismatch between the **show sdwan system status** and **show proc cpu platform** commands.
CSCwf03193	Device crashes with crashinfo files when generated with the segmentation fault, process IPSEC key engine.
CSCwh08434	OMP route is advertised although the route is not available.
CSCwf26875	Ten0/0/2 from port-channel suspends the status when applying the **platform qos port-channel-aggregate** command.
CSCwf24164	Netflow stops working when flow monitor reaches cache limit.

Identifier	Headline
CSCwh63061	Modem (P-5GS6-GL) is showing four additional NR bands support - 1, 3, 7, and 28.
CSCwf65540	Running tests on ThousandEyes Agent causes tracebacks on device running TE in docker container.
CSCwe14885	VPN is established although the peer is using a revoked certificate for authentication.
CSCwd17272	UTD packet drop due to fragmentation for ER-SPAN traffic.
CSCwf55243	Device is crashing while adding a trustpoint to the router .
CSCwh49644	CSDL Compliance failure : Use of 3DES by IPSec is denied.
CSCwh32386	Unexpected reload on device due to critical process fman_fp_image.
CSCwf67564	Device observes memory leak at process SSS Manager.
CSCwf78735	Device uses the NIM-1T/4T card for interconnection, and NAT+ GRE over IPsec cannot be applied.
CSCwh30377	Device data plane crash in Umbrella/OpenDNS processing due to incorrect UDP length.
CSCwf34171	The **configure replace** command fails due to the license *UDI PID XXX SN:XXXX* line on IOS-XE devices.
CSCwh20734	Crypto PKI-CRL-IO_0 process crash when PKI trustpoint is requested and deleted.
CSCwf96980	Unexpected reboot after configuring application redundancy.
CSCwh01425	ITU channel configuration seems not working on the device.
CSCwh20577	Crashed by Track Client thread at access invalid memory location.
CSCwh00963	Unable to migrate from ADSL to VDSL without reboot.
CSCwh36801	Crash in IP Input process during tunnel encapsulation.
CSCwh96415	DMVPN logging cannot be disabled.
CSCwe85301	Crypto PKI-CRL-IO_0 process crash when PKI trustpoint is deleted.
CSCwf05980	Device dropping Speedtest/IPerf packets with drop reason DROP 19 (Ipv4NoRoute).
CSCwf71557	IPv4 connectivity over PPP not restored after reload.
CSCwf63706	The device HSRP received unexpected active hello packet when interface is recovered.
CSCwf11394	Vdaemon debug log must mention port-hop and reason prior to Distloc.
CSCwf04866	Keyman process crash seen while re-generating SSH key in the device.
CSCwh00332	B2B NAT: when configration IP Nat inside/outside on Vasi intereface, ack/seq number abnormal.

Identifier	Headline
CSCwh08948	Device: **show platform hardware throughput crypto** command displays ambiguous outputs.

Open Bugs - Cisco IOS XE 17.9.5a

Identifier	Headline
CSCwf84960	C-NIM-2T: LED L remains green after port shutdown.
CSCwh18120	IKEv2 - diagnose feature is taking 11% CPU during session bring up.
CSCwf67983	Device platform USB will not work once the USB is removed and inserted.
CSCwh22414	Warning and critical CPU utilization thresholds not recomputed when using data-plane-heavy mode.
CSCwi01046	PoE module is not providing enough power to bring the ports after an unexpected reload.
CSCwc30418	Segmentation fault observed in ikev2_dupe_delete_reason.
CSCwh12093	Enable SoS/ROC feature for DSL.
CSCwi06843	Endpoint tracker triggers a CPU Hog.
CSCwh80441	Cosmetic 3G issue causing distress - device is displayed as unknown.
CSCwi29637	SFP interface shut down, but the opposing device interface is still up and running.
CSCwi06404	PKI crash after failing a CRL Fetch.
CSCwi46997	NAT command is not readable after being reloaded.
CSCwi33168	DSP reporting out of range utilization values in SNMP.
CSCwi59834	EntSensorThresholdValue OID for PDU1 is missing.
CSCwi08171	Device crashes due to crypto IKMP process.
CSCwi53951	Packets with unicast MAC are dropped on a port channel L2 sub-intf after the device is rebooted.
CSCwb25507	CWMP: Add vendor specific parameter for NBAR protocol pack version .
CSCwi25737	Device must discard IKE Notification messages with incorrect DOI.
CSCwh50510	Device crashes with segmentation fault(11), process = NHRP when processing NHRP traffic.
CSCwi10735	ZBF drops transit WAAS PSH/ACK packet due to invalid ACK number.
CSCwi53306	Unknown appID in ZBFW HSL log.

Identifier	Headline
CSCwh91136	Traffic not encrypted and droped over IPsec SVTI tunnel.
CSCwe24491	Static NAT with HSRP stops working after removing /adding standby.
CSCwi14899	Device dropping IPsec traffic when SVI is used as source for DMVPN tunnel.
CSCwh41497	DDNS update retransmission timer fails to work with a traceback error.
CSCwi51326	CPP CP SVR crashes after decoding all packets to text (using l2 copy) on fia trace .
CSCwi04547	Cisco SD-WAN custom application is marked as invalid .
CSCwi16111	IPv6 TCP adjust-mss not working after delete and reconfigure.
CSCwi63042	Packet drops observed between LISP EID over GRE tunnel.
CSCwi59202	C-NIM-2T cannot boot up in IOS.
CSCwi30529	AAA: Template push fails when aaa authorization is set to local.

Resolved Bugs - Cisco IOS XE 17.9.4a

All resolved bugs for this release are available in the Cisco Bug Search Tool.

Bug ID	Description
CSCwh87343	Cisco IOS XE Software Web UI Privilege Escalation Vulnerability. For more information, see Security Advisory: cisco-sa-iosxe-webui-privesc-j22SaA4z

Open Bugs in Cisco IOS XE 17.9.4a

Identifier	Headline
CSCwe95072	Unexpected reload due to memory corruption when modifying and access list.
CSCwf52751	CLI template fails to attach to CG418-E with error access-denied.
CSCwf24164	Netflow stops working when flow monitor reaches cache limit in the Device.
CSCwd61988	Output packet Bytes calculation biase when we enable QoS on port channel.
CSCwf41492	NHRP BFD flaps randomly with dynamic tunnel (NHRP phase 3) in DMVPN.
CSCwe14885	VPN is established although the peer is using a revoked certificate for authentication.
CSCwc86434	Static NAT DIA inside static routes being advertised over OMP to remote sites.
CSCwd17272	UTD Packet drop due to fragmentation for ER-SPAN traffic.
CSCwf55243	Device is crashing while adding a trustpoint to the router.
CSCwe85301	Crypto PKI-CRL-IO_0 process crash when PKI trustpoint is being deleted.

Identifier	Headline
CSCwf34171	The **Configure replace** command fails due to the "license udi PID XXX SN:XXXX" line on Cisco IOS XE devices.
CSCwf41450	Device reloads changing the resource profile.
CSCvz82148	%CRYPTO_SL_TP_LEVELS-6-VAR_NEW_VALUE message is observed in each write config with same crypto value.
CSCwf25735	QoS more than four remark with set-cos not work.
CSCwf00276	Packets with L2TP headers cause device to crash
CSCwd39257	Cisco IOS XE cpp crash is seen when entering **no ip nat create flow-entries** command
CSCwf03193	Device crashes with crashinfo files were generated with segmentation fault, process IPSEC key engine.
CSCwf63706	HSRP received unexpected active hello packet when interface recovered.
CSCwf60120	Static NAT entry gets deleted from running config; but remains in startup configiration.
CSCwf51206	EVPN: BUM traffic is not flooded to bridge domain interface.
CSCwf11394	Cisco IOS XE - debug log should mention port-hop and reason prior to DISTLOC
CSCwe51910	SNMP ifindex persist does not work.

Resolved Bugs in Cisco IOS XE 17.9.4

Identifier	Headline
CSCwf48808	FlexVPN: Stale client routes stuck in RIB on FlexServer.
CSCwe93905	NAT ALG is changing the Call-ID within SIP message header causing calls to fail.
CSCwf02225	Device freezes for **show sdwan** command.
CSCwe28204	Control connection over L3 Tloc extension failing as no NAT table entry created.
CSCwe18124	MACsec remains marked as SECURED, but randomly the traffic stops working.
CSCwe25076	ALG breaks NBAR recognition impacting application firewall performance.
CSCwd87195	NAT configuration with redundancy, mapping id and match-in-vrf options with no-alias support.
CSCwf08698	Device crashes unexpectedly due to a fault in the TLSCLIENT_PROCESS.
CSCwd34941	NAT configuration with no-alias option is not preserved after reload.
CSCwf47796	NHRP cache entries flood matching a /32 default route.
CSCwf09758	Watchdog crashes while importing a large CRL file into switch.

Identifier	Headline
CSCwe41946	DTMF is failing through IOS MTP during call on-hold.
CSCwe37123	Device uses excessive memory when configuring ACLs with Large Object Groups.
CSCwe12194	Auto-update cycle incorrectly deletes certificates.
CSCwd49309	Ucode crash is seen on device with traffic pointing to segfault in coff handler.
CSCwe33793	Memory allocation failure with extended antireplay enabled.
CSCwe66318	NAT entries expire on standby router.
CSCwe31471	Segmentation fault in SD-WAN PB rx when per-tunnel QoS config withdraw.
CSCwd59722	Unexpected reboot due to Cisco IOS XE WATCHDOG: Process = Crypto IKMP.
CSCwe70374	Device platform punt-policer is not configurable.
CSCwf47563	Device is crashing after importing the trustpoint with RSA key pair.
CSCwe18058	Unexpected reload with IPS configured.
CSCwd73783	Observed qfp-ucode-wlc crash.
CSCwe39011	GARP on port up/up status from the router is not received by remote peer device.
CSCwf39490	MCID (Malicious Call Identification) gets broken due to custom prefix setting under STCAPP FAC.
CSCwe19084	NAT: Traffic is not translated to the same global address though PAP is configured.
CSCwe89404	No way audio when using secure hardware conference with secure endpoints.
CSCwa96399	Configuring *entity-information xpath* filter causes syslogs to print, does not return data.
CSCwe06518	Device: ~23% degradation in IPSEC IPv6 profile in CCO for 1400B.
CSCwc89823	Router crashes due to CPUHOG when walking Cisco FlashMIB @snmp_platform_get_flash_file_info.
CSCwe32862	Cisco IOS XE crashes while executing AES crypto functions.
CSCwf37888	Packet Duplication: Duplicate packets are counted on primary tunnel interface statistics.
CSCwd68994	ISAKMP profile does not match as per configured certificate maps.
CSCwd35047	Failed to ping gateway while configuring SharedLOM with console telnet interface until router reload.
CSCwd49177	ISG Layer 2 Connected Subscriber: IPv6 prefix delegation is not reachable when packet are switched.
CSCwe88689	C8200: ROMMON 17.6(6r) release for auto-upgrade.

Identifier	Headline
CSCvy60823	PCIe Bus and Kernel Errors, Interfaces go down when these errors are seen.

Open Bugs in Cisco IOS XE 17.9.4

Identifier	Headline
CSCwe95072	Unexpected reload due to memory corruption when modifying and access list.
CSCwf52751	CLI template fails to attach to CG418-E with error access-denied.
CSCwf24164	Netflow stops working when flow monitor reaches cache limit in the Device.
CSCwd61988	Output packet Bytes calculation biase when we enable QoS on port channel.
CSCwf41492	NHRP BFD flaps randomly with dynamic tunnel (NHRP phase 3) in DMVPN.
CSCwe14885	VPN is established although the peer is using a revoked certificate for authentication.
CSCwc86434	Static NAT DIA inside static routes being advertised over OMP to remote sites.
CSCwd17272	UTD Packet drop due to fragmentation for ER-SPAN traffic.
CSCwf55243	Device is crashing while adding a trustpoint to the router.
CSCwe85301	Crypto PKI-CRL-IO_0 process crash when PKI trustpoint is being deleted.
CSCwf34171	The **Configure replace** command fails due to the "license udi PID XXX SN:XXXX" line on Cisco IOS XE devices.
CSCwf41450	Device reloads changing the resource profile.
CSCvz82148	%CRYPTO_SL_TP_LEVELS-6-VAR_NEW_VALUE message is observed in each write config with same crypto value.
CSCwf25735	QoS more than four remark with set-cos not work.
CSCwf00276	Packets with L2TP headers cause device to crash
CSCwd39257	Cisco IOS XE cpp crash is seen when entering **no ip nat create flow-entries** command
CSCwf03193	Device crashes with crashinfo files were generated with segmentation fault, process IPSEC key engine.
CSCwf63706	HSRP received unexpected active hello packet when interface recovered.
CSCwf60120	Static NAT entry gets deleted from running config; but remains in startup configiration.
CSCwf51206	EVPN: BUM traffic is not flooded to bridge domain interface.
CSCwf11394	Cisco IOS XE - debug log should mention port-hop and reason prior to DISTLOC
CSCwe51910	SNMP ifindex persist does not work.
CSCwh60848	CUBE - SIP Message Queuing Fails to Resume Transmission

Resolved Bugs in Cisco IOS XE 17.9.3a

Identifier	Headline
CSCwd45402	MSR unicast to multicast not working if destination and source are the same in service reflect configuration.
CSCwd07516	Memory leak under linux_iosd-imag related to SNMP.
CSCwd90168	Unexpected reload after running **show voice dsp** command while an ISDN Call disconnects.
CSCwd16559	ISG FFR: ARP request to reroute nexthop IP is not triggered if ARP entry not in ARP table.
CSCwd45363	IPSEC throughput level / ambiguous outputs.
CSCwc27307	Service engine YANG support for Zone-based Firewall.
CSCwd16664	GetVPN Long SA - GM re-registration after encrypting 2^32-1 of packets in one IPSEC SA.
CSCwd81357	QoS Classification not working for DSCP or ACL + MPLS EXP.
CSCwd89338	Clear ISG existing lite-session upon reception of DHCP packet for same client.
CSCwc99823	Fman crash seen in SGACL@ fman_sgacl_calloc.
CSCwd25107	Interface VLAN1 placed in shutdown state when configured with **ip address pool** command.
CSCwd61255	Data plane crash is seen on the device when making per-tunnel QoS configuration changes with scale.
CSCwe01015	IKEv2/IPSec - phase 2 rekey failing when peer is behind NAT.
CSCwd03869	CEF DPI load-balancing causes out of order packets.
CSCwc65697	vCube crashing and restarting during call flow.
CSCwd84599	Dataplane memory utilization issue - 97% QFP DRAM memory utilization.
CSCwc99453	Enable **license feature hseck9** command on the device.
CSCwe03614	CWMP : MAC address of ATM interface is not included in inform message.
CSCwd38943	GETVPN: KS reject registration from a public IP.
CSCwd06372	Unconditional excessive logging in eogre tunnel error handling case.
CSCvy14316	MPLS VPN traffic dropped due FDB OOM with cause FIAError under scale flow number.
CSCwd85580	Device reloads unexpectedly after **set ospfv3 authentication null** command.
CSCwd33202	DHCP behavior issue when BDI interface is enabled on WAN and SVI interface.

Identifier	Headline
CSCwd06923	Stale ip alias left after NAT statement got removed.
CSCwd47123	ISG uses identifier mac-address 0000.0000.0000 when DHCP LQ does not reply.
CSCwd72312	GETVPN : Traffic drops is seen on GM after rekey installing policies.
CSCwc14688	Single WAN interface subslot 0/0 timing.

Open Bugs in Cisco IOS XE 17.9.3a

Identifier	Headline
CSCwd39257	IOS-XE cpp crash when entering **no ip nat create flow-entries** command.
CSCwd63783	Memory leak on vdaemon process caused router reload.
CSCwd97077	Device leaking memory in MallocLite because of telemetry subscription to collect FNF cache.
CSCwe09805	OID for SNMP monitoring of DSP resources are not working as expected.
CSCwe25076	ALG breaks NBAR recognition impacting application firewall performance.
CSCwe14885	VPN is established although the peer is using a revoked certificate for authentication.
CSCwe24491	Static NAT with HSRP stops working after removing and adding standby.
CSCwd17272	UTD Packet drop due to fragmentation for ER-SPAN traffic.
CSCwe32862	Device crashes while executing AES crypto functions.
CSCwe19084	NAT: Traffic is not translated to the same global address though PAP is configured.
CSCwe12652	Incorrect return MIB for ciscoWanCellExtMIB and ciscoWan3gMIB.
CSCwd68994	Unable to match on customer profile based on certificate-map.
CSCwc06327	PFP policy in SRTE, RIB resolution in FC bring down ipsec tunnel interface- stuck at linestate down.
CSCwe38732	IP CEF load sharing command is being changed by the device.
CSCwe39011	GARP on port up/up status from the device is not received by remote peer device.
CSCwd34941	NAT configuration with no-alias option is not preserved after reload.
CSCwh60848	CUBE - SIP Message Queuing Fails to Resume Transmission

Resolved Bugs in Cisco IOS XE 17.9.2a

Identifier	Headline
CSCwc21739	NAT not requesting further for low ports after initial allocation when cli knob "reserved-ports" set.
CSCwc39012	Crash saving tracelogs after "Too many open files" error.
CSCwc03478	VTCP does not support Layer2 correctly.
CSCwc82140	QFP crashes when ZBFW configuration geatures "log dropped-packets" configuration.
CSCwd12591	Device ucode crash is seen during FW classification and the session is becomes free.
CSCwc99668	Device added by IKEV2 is getting deleted at responder.
CSCwc23077	Firewall drop is seen stating “FirewallL4” seen on the device.
CSCwc78528	DSPware 60.1.1 release targeting v179_throttle.
CSCwc44851	Bootstrap is failing on the device.
CSCwc96444	Device is not programming correct next-hop for unicast prefix with multicast config present.
CSCwc49715	Carsh is seen @ UNIX-EXT-SIGNAL: Aborted(6), Process = Check heaps, having PPPoe with cwmp configs.
CSCwb52324	Device unexpected reload due to QFP ucode crash.
CSCwc77183	Packet duplication is causing drops in payment transactions with SdwanGenericDrop code.
CSCwc20170	Device reloads unexpectedly due to critical FTMd fault when VRF configuration is pushed
CSCwb89958	Unified Policy HSL not sending properly NBAR application information.
CSCwc89328	Multiple devices experience crashes every 4 to 5 miniutes.
CSCwc11376	CefcFRUPowerOperStatus false report on the device.
CSCwc45950	ZBFW self zone policy drops SSH session on Mgmt-intf 512 ports.
CSCwc43794	Device VRF+NAT Outside Source Static - Drop packets during FTP (Active-mode) execution.
CSCwc28587	Crashed without generating any core (Critical process plogd fault on rp_0_0 (rc=75).
CSCwc32595	BFD sessions remains down if interface flap form up/down/up.
CSCwb90252	Automatically freeing up filesystems stale image or recovered folder (lost+found).
CSCvz89354	Device crashes due to CPUHOG when walking ciscoFlashMIB.

Identifier	Headline
CSCwc39865	Subscriber session getting stuck and needs clearing it manually.
CSCwb48953	Device speed test failing with "Device Error: Speed test in progress".
CSCwc72923	ERROR information: Device r configuration failed:interface Serial0/1/0:23 isdn switch-type primary-ntt.
CSCwc84967	Intermittent double DTMF due to changing timestamp on a DTMF event.
CSCwb08057	ISG: Number of lite sessions conversion in progress counter not decrementing on failed account-logon.
CSCwd11365	Needs cert update - Azure CGW creation fails due to NVA provisioning failure.
CSCwc79145	Throughput degrades when Local TLOC specified in Data Policy goes down.
CSCwc29629	Crashes when Virtual-Access tries to bring-up/bring-down OSPFv3 ipsec crypto session authentication.
CSCwd13352	SSH from device tgetting closed after the device is updated.
CSCwc77177	BFD and control packets are dropped when ACL is applied on gigi to which loopback is bind.
CSCwc68132	SIG tunnel tracker packets are dropped by firewall with self zone policy.
CSCwd56336	BFD sessions are not coming up after flapping the interface due to low ftm rate.
CSCwd56015	UTD skipped when interface UTD config is used to enable/disable UTD.

Open Bugs in Cisco IOS XE 17.9.2a

Identifier	Headline
CSCwd45508	Device does not form BFD across Serial link when upgrading.
CSCwd23810	IOS-XE: A high CPU utilization caused by NHRP.
CSCwd45402	MSR Unicast-To-Multicast not working if the destinatio and source are the same in service reflect configuration.
CSCwd45363	IPSEC throughput level ambiguous outputs.
CSCwd13050	After upgrade, device moved into out of sync status.
CSCwd12955	NAT translation is not correctly sent to hub router from branch when SSNAT and UTD are configured.
CSCwc28468	Template is not pushed to the device if device is running in FIPS mode.
CSCwc99823	Fman crash is seen in SGACL@ fman_sgacl_calloc.
CSCwd34941	NAT configuration with no-alias option is not preserved after reload.

Identifier	Headline
CSCwd15560	With 2 sequences, should not skip if the match is different and action is same.
CSCwd33966	Unable to configure the local BGP.
CSCwd37410	0365 and MS Teams applications access issues when using DIA with app-list match in data-policy.
CSCvz55282	Serviceability enhancements for config migration failures between releases.
CSCwd36621	CERM may kick in due to IPSec sessions initiated for on-demand tunnels.
CSCwd44006	Control Connection on the device does not come-up with reverse proxy using enterprise certificate.
CSCwd29334	Upgrade failures due to inability to establish netconf connection.
CSCwd11124	Device kernel crash - kernel NULL pointer dereference - error_code(0x0010) - not-present page.
CSCwa14636	Device stopped forwarding traffic. Suspect OMPd is busy.
CSCwd38626	Repeating SYS-2-PAK_SUBBLOCK_BADSIZE: 4 -Process= "<interrupt level>".
CSCwd33202	DHCP behavior issue is seen when BDI interface is enabled on WAN and SVI interface.
CSCwd17381	NAT and DIA traffic is skipping UTD in forward direction after SSNAT path from service-side.
CSCwd34860	Device see the increase of "Input errors" without any other specifc errors increasing under **show interface** command.
CSCwd12330	Invalid TCP checksum in SYN flag packets passing through device.
CSCwd18028	After delete CSP, new CCM bring up on existing CSP is stuck in "Initializing CCM" on MT cluster.

Resolved Bugs in Cisco IOS XE 17.9.1a

Identifier	Headline
CSCvz65764	Peer MSS value showing incorrect.
CSCwa95092	When Object-group used in a ACL is updated, it takes no effect.
CSCwb33968	Device failed to display active flows when flow count is high on the device.
CSCwb02142	Traceback: fman_fp_image core after clearing packet-trace conditions.
CSCwb49857	Memory leaks on keyman process when key is not found.
CSCwa65728	Large number of DH failures.
CSCwb11389	NAT translation stops suddenly(ip nat inside does not work).

Identifier	Headline
CSCwa84919	Revocation-check crl none" does not failover to NONE DNAC-CA
CSCwb39098	Router crashed after new IPv6 address assigned when router use specific configuration.
CSCwa69101	ISG: initiator unclassified ip-address LQipv4 command has no effect.
CSCwa67886	UDP based DNS resolution does not work with IS-IS EMCP on IOX-XE.
CSCvz84588	Destination prefix packets getting dropped because forwarding plane is not programming the next hop.
CSCwb27486	New Key for NBAR app and NBAR category without OGREF optimized.
CSCwa72273	ZBFW dropping return packets from Zscalar tunnel post cedge upgrade to 17.3.4.
CSCwb32934	Device does not use QAT when malloc failure.
CSCwa49101	OMP origin protocol comparison clean-up.
CSCwb17282	Router crashing when clearing a VPDN session.
CSCwa49721	Deviee hub with firewall configured incorrectly dropping return packets when routing between VRFs.
CSCwb21645	NAT traffic gets dropped when default route changes from OMP to NAT DIA route
CSCwa98617	Memory Leak in AEM chunks related to Firewall.
CSCwb18223	SNMP v2 community name encryption problem.
CSCwb16723	Traceroute not working on cEdge with NAT.
CSCwb31587	Subject-alt-name attribute in certificate trustpoint causes Windows NDES/CA to reject SCEP requests.
CSCwb51238	Router reload unexpectedly two times when enter **netflow show** command.
CSCwb12647	Device crashes for stuck threads in cpp on packet processing.
CSCwa48512	CoR intercepted DNS reply packets dropped with drop code 52 (FirewallL4Insp) if UTD enabled.
CSCwa93664	ThousandEyes container may fail to get installed on the device.
CSCvz28950	DMVPN phase 2 connectivity issue between two spokes.
CSCwa78348	Traceback: IOS-XE reload after Segmentation fault on Process = SSS Manager
CSCvz81664	Enabling or Disabling OMP Overlay AS Prevents Connected Routes from Being Advertised in OMP.
CSCwb43423	IOS XE image installation fails.
CSCwa08847	ZBFW policy stops working after modifying the zone pair.

Identifier	Headline
CSCwb15331	Keyman memory leak using public keys.
CSCvw50622	NHRP network resolution not working with link-local ipv6 address.
CSCwb59736	BFD tunnel are zero with SDWAN version 17.03.03.0.7.
CSCwa57873	Incorrect reload reason - Last reload reason: LocalSoft for Netconf Initiated request.
CSCwb51595	Missing IOS config (voice translation rule) on upgrade from 17.3 to 17.6.
CSCwb18315	Umbrella DNS security policy doesn't work with Cloud onRamp with SIG tunnels.

Open Bugs in Cisco IOS XE 17.9.1a

Identifier	Headline
CSCwc39012	Crash saving tracelogs after "Too many open files" error.
CSCwc20075	Unable to switch the technology from 4g to 3g.
CSCwb89958	Unified Policy HSL not sending properly NBAR application information.
CSCwc23077	Firewall drop seen stating “FirewallL4” seen on the device.
CSCwb74821	Yang-management process confd is not running, controller mode 17.6.2a.
CSCwc44851	Bootstrap failing on c8300 on 17.9.
CSCwc55684	SIG GRE: Layer 7 Health check doesn't work on Loopback interfaces.
CSCwc56896	Crash is seen in ipv6_tunnel_macaddr while adding/removing gre multi-point tunnel mode.
CSCwc52538	SDWAN flows are not distributed and load-balanced evenly and consistently.
CSCwc55260	Memory leak due to FTMd process.
CSCwc69881	Device lost configuration due to multiple power cycles on site.
CSCwc20170	Device reloads unexpectedly due to critical FTMd fault when VRF configuration is pushed.
CSCwb88621	Device unable to establish control connection with vBond due to out of order DTLS packets.
CSCwc37465	Static NAT configuration in CLI with the no-alias keyword cannot be retrieved via NETCONF/YANG.
CSCwc59598	Device statistics collection causing service-side BFD to flap on every collection interval.
CSCwc50477	Device crashed in ipv4_nat_create_out2in_session_entry
CSCwc67465	Device cannot be upgraded to 17.8.

Identifier	Headline
CSCwc59650	The show sdwan app-fwd cflowd flows vpn X format table does not show all flows for vpn X
CSCwc32595	BFD sessions remains down if interface flap form up/down/up
CSCwc38529	Traffic seems not inspected by UTD when umbrella is set.
CSCwc63563	Unable to set specific speed and duplex values on SFP ports on IOS-XE routing platforms.
CSCwc39865	Subscriber Session getting stuck and needs clearing it manually.
CSCwc43973	DLC is not completing after upgrading to Smart licensing from CSL
CSCwc55467	BFD Tunnel on the router is not staying up, 1 out of 40 tunnels.
CSCwc42978	Device looses all BFD sessions with Invalid SPI.
CSCwc67171	Tracebacks at cgm_avlmgr_class_init and cpuhog_key_init
CSCwb08057	ISG: Number of lite sessions conversion in progress counter not decrementing on failed account-logon.
CSCwc63337	Destination not reachable if configured as a next for a static route resolvable via non /32 OMP.
CSCwc29629	Crashes when Virtual-Access tries to bring-up/bring-down OSPFv3 ipsec crypto session authentication.
CSCwc27208	BFD sessions not coming UP because of ANTI-REPLAY-FAILURES.
CSCwc68132	SIG tunnel tracker packets are dropped by firewall with self zone policy.
CSCwc70468	CPA fail to send SIP Update for AsmT before "maxTermToneAnalysis" expiration.
CSCwc70511	URGENT ISR4331/K9 | Version 17.06.02 | Router Reloaded Unexpectedly.

Related Documentation

- 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 8300 and 8200 Series Edge Platforms Software Configuration Guide

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.

- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

Troubleshooting

For the most up-to-date, detailed troubleshooting information, see the Cisco TAC website at https://www.cisco.com/en/US/support/index.html.

Go to **Products by Category** and choose your product from the list, or enter the name of your product. Look under **Troubleshoot and Alerts** to find information for the issue that you are experiencing.