Release Notes for Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms, Cisco IOS XE Dublin Release 17.12.x

First Published: 2023-08-22

Last Modified: 2026-08-05

Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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: https://www.cisco.com/c/en/us/about/legal/trademarks.html. 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. (1721R)

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 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 Dublin 17.12.1a is the first release for the Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms in the Cisco IOS XE Dublin 17.12.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

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 Hardware Features

Hardware	Description
Cisco C-NIM-8M	The C-NIM-8M are the next generation LAN/WAN NIM modules that provide enhanced security, reliability, and performance. The Cisco C-NIM-8M module provides 2.5 Gbps mGig connectivity and supports UPoE+. Also, Cisco C-NIM-8M supports Layer 2 and Layer 3 configurable Ethernet network.

New and Changed Software Features in Cisco IOS XE 17.12.8

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.12.7b

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.12.6

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.12.5d

There are no new features in this release.

New and Changed Software Features in Cisco IOS XE 17.12.5c

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.12.5b

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.12.5a

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.12.4b

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.12.4a

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.12.2

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.

Table 1: New Software Features

Feature	Description
Cisco Managed Cellular Activation (eSIM)	The Managed Cellular Activation solution provides a programmable subscriber identity module (SIM), called an eSIM, a physical SIM card that you can configure with a cellular service plan of your choice. When ordering a pluggable interface module (PIM) to provide cellular connectivity for your router, choose a PIM model with a preinstalled eSIM. The Managed Cellular Activation solution comes with a "bootstrap" cellular plan to provide internet connectivity with a limited amount of data intended only for Day 0 onboarding of the device to your cellular plan. For information about configuring Cisco SD-WAN Manager with the details of your cellular plan in preparation for onboarding the device, see the Cisco Managed Cellular Activation Configuration Guide. Prepare the configuration in Cisco SD-WAN Manager before powering on and onboarding the device, to avoid running out of the limited data in the bootstrap cellular plan. Added Cisco Managed Cellular Activation (eSIM) support for the following Pluggable Interface Module (PIM) model: • 5G Sub-6 GHz PIM, model P-5GS6-R16-GL **Note** In this context, eSIM refers to a removable SIM pre-installed by Cisco. In other contexts, eSIM can refer to a non-removable SIM embedded in a cellular-enabled device.

New and Changed Software Features in Cisco IOS XE 17.12.1a

Table 2: Software Features in Cisco Catalyst 8200 and Cisco Catalyst 8300 Series Edge Platforms

Feature	Description
IPv6 Unicast Support with DLEP	The IPv6 Unicast Support feature introduces support for IPv6 dataplane to RAR Dynamic Link Exchange Protocol.
Managing the SD-Routing Devices Using Cisco SD-WAN Manager	This feature allows you to perform management operations for SD-Routing devices using Cisco Catalyst SD-WAN Manager. You can use a single network management system (Cisco Catalyst SD-WAN Manager) to monitor all the SD-Routing devices and therefore help in simplifying solution deployments.

Feature	Description
Quantum-Safe Encryption Using Post-Quantum Preshared Keys	This enhancement introduces support for Quantum-Safe Encryption using Post-Quantum Preshared Keys for the following platforms: • Cisco Catalyst 8300 Series Edge Platforms
Segment Routing over IPv6 Dataplane	Segment Routing (SR) can currently be applied on Multiprotocol Label Switching (MPLS) dataplane. From Cisco IOS XE 17.12.1a, SR is supported over the IPv6 dataplane for the following protocols: • Interior Gateway Protocol (IS-IS only) • Border Gateway Protocol (BGP) In addition, the following functionalities are available for Segment Routing over IPv6 dataplane: • Segment Routing Traffic Engineering Policies • Static Routes • Performance Management • Operations, Administration and Maintenance (OAM)
Support for Automatic Log Deletion	This feature allows you to delete the entries from the logging buffer. You can configure the local syslog retention period after which the entries are purged from the device automatically. To enable this feature, use the logging purge-log buffer days command.
TrustSec and Software-Defined Access Scale Measurement	With this feature, the scale numbers for TrustSec and Software-Defined Access (SDA) are measured for the following: • Security Group Tag (SGT) or Destination Group Tag (DGT) Policies • Unidirectional IPv4 SGT Exchange Protocol (SXP) connections • Bidirectional IPv4 SXP connections • IPv4 SGT Bindings • IPv6 SGT Binding • Security Group Access Control Entries (SG ACEs)

ROMMON Compatibility Matrix

The following table lists the ROMMON releases supported in Cisco IOS XE 17.12.x releases.

Table 3: 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	17.12.1a	17.3(1r)	17.6(6r)
C8300-2N2S-4T2X|6T	17.12.1a	17.3(1.2r)	17.7(1r)
Catalyst 8200 Series Edge Platforms			
C8200-1N-4T	17.12.1a	17.4(1r)	17.6(8.1r)
C8200L-1N-4T	17.12.1a	17.5(1.1r)	17.6(8.1r)

Resolved and Open Bugs for Cisco IOS XE 17.12.x

Resolved Bugs in Cisco IOS XE 17.12.8

Identifier	Headline
CSCwu02602	DBAL EVENTS crash seen while trying to push config group to device in SDWAN and SD-Routing.
CSCws75769	Netconf process doesn't start on 9130 AP in EWC mode and generates repeated dmiauthd subscription failures for invalid route-map YANG path.
CSCws80808	Loopback interface in Mgmt-intf VRF becomes unreachable via Management interface.
CSCwt87294	mDNS Cache-Flush behavior not consistent.

Open Bugs for Cisco IOS XE 17.12.8

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

Resolved Bugs in Cisco IOS XE 17.12.7b

Identifier	Headline
CSCwr83968	Unexpected Reload on device with Static NAT when polling NAT Translation Data.
CSCwo57783	"NHRP Encap Error for Purge Request" populates on spoke despite correct routing at HUB.
CSCwn85623	Missing Calling-Station-ID in radius messages.

Identifier	Headline
CSCwm62981	Device crashes with PKI "revocation-check ocsp none" enabled.
CSCwp96706	Memory leak in MallocLite and Crypto IKEv2.
CSCwq22471	Device may unexpectedly reboot when importing CA chains.
CSCwq21566	HSL entries are missing when config is pushed via vManage.
CSCwq51358	Device may experience high memory utilization and unexpected reloads during IKEv2 operations.
CSCwn18874	DMVPN spoke crashed at Process = NHRP.
CSCwo14975	Memory leak in DNS Proxy/SKA triggers unexpected reloads.
CSCwj88080	Device continuously crashes after configuring UTD and rebooting.
CSCwp40010	RP crash while debugging IKEv2.
CSCwp38609	CTS Trustpoint loop triggers PKI segfault.
CSCwq49981	Call Failures due to FPI resource leaks.

Open Bugs in Cisco IOS XE 17.12.7b

Identifier	Headline
CSCwi03502	Create CLI to push at#enadis=0 followed with at#reboot to FN980 required when configuring Multi-PDN.
CSCwr00088	Add CLI to change per MPLS label CEF statistics query interval on FMAN FP.
CSCwj33723	Config not synced between active and 3rd member of stack.
CSCwh36635	Device confd / SMP crash.
CSCwn29062	Router may see cosmetic "DATACORRUPTION" logs during IPSec Tunnel Up/Down events.
CSCwk55051	polaris_vconfd_cfgpull_t denials during config push trigger.
CSCwm54978	Selinux: Subject polaris_iosd_t denials.

Resolved Bugs in Cisco IOS XE 17.12.6

Identifier	Headline
CSCwp03641	Multiple inside local addreses are translated to same inside global IP address and port.
CSCwo75362	Device ethernet modules fail to boot after software reload.
CSCwo91955	Endpoint tracker remains up status when DNS is reachable from the other interface.

Identifier	Headline
CSCwn99822	Large number of BFD sessions stuck due to out of window drops reported with control connections NAT flaps.
CSCwp28915	SNMPwalk fails to consistently return tunnel names due to incomplete tunnel setup.
CSCwo66822	Device reloaded with reason: Critical process cpp_ha_top_level_server fault on fp_0_0 (rc=69).
CSCwn99723	Device - Deprecate "request platform software package expand" commands for upgrades.
CSCwp12923	IKEv2 fails to parse certain route-set prefix Cisco VSA attributes from Radius server .
CSCwo47118	Crash when clearing L2TP tunnels with the command "clear vpdn tunnel l2tp <ID>".
CSCwb24403	BFD flap on public IP change on a private color tloc.
CSCwo42107	Device crashes when applying a service-policy to a PO interface used as Tunnel source.
CSCwo90396	Serial interface configuration lost after reload.
CSCwm33545	FlexVPN - IP address assigned to spoke changes to unassigned.
CSCwo12453	Configuring "access-class xx in vrf Mgmt-vrf" on line vty causes the âLogin Block" to be inactive.
CSCwn57838	Startup config lost for interfaces NIM-(1|2)GE-CU-SFP.
CSCwo51627	Unexpected reload due Critical process linux_iosd_image fault on rp_0_0 (rc=139).
CSCwn39832	Adding "authorization bypass" to vDSP EEM scripts.
CSCwo03915	Unexpected reload on cEdge due to performance monitor with packet service insertion from spoke.
CSCwp81333	Cache Coherency rare timing race condition.
CSCwo15543	Functional SJC Alpha 9840 eWLC HA- Standby eWLC reloads after upgrade to 17.17.1.
CSCwk56650	cEdge unexpected reboot during dialer initialization.
CSCwj27134	ip vrf receive command adds connected route to vrf table even though interface admin down.
CSCwo34430	Device Terminal Server Drops protocol Sessions upon executing "Show Memory" Command.
CSCwo05166	Memory leak on Chunk Manager via DBAL EVENTS process.
CSCwo99641	Out of CGM (Class-Group Manager) memory intermittently with scaled ZBFW policy.

Identifier	Headline
CSCwn53302	Administrative distance of IPv6 static route to Cellular interface overwrite with 254.
CSCwn37412	NTP will not authenticate with open source NTP servers using 32B cmac-aes-128.
CSCwk05523	Device crashes with "Bad magic number in chunk header", with ACL logging hash-generation.
CSCwm01063	Unexpected reload due to Segmentation fault on IP SLA DynHostName Process.
CSCwp59954	Unexpected reboot on IOS-XE due prune on mcast.
CSCwo89784	Unexpected reload of Standby during PKI Trustpoint removal.
CSCwo70548	Ping failure from VRRP backup to VRRP primary virtual address when enabling security policy.
CSCwp35552	Missing Calling-Station-ID (31) in Radius Accounting.
CSCwn24036	Tx/Rx optical power values diffrent for "show int" and "show hw-module".
CSCwn18584	Traecbacks seen on curie router while applying config on a clean router.
CSCwn54648	Device High CPU on Virtual EXEC and TTY Background.
CSCwj60804	ACL delete and reapply removes PBR mapping but TCAM is populated.
CSCwo22585	Device crashes when running a NWPI trace initiated from vManage on version 20.12.4.
CSCwi59338	Enable strict-kex support in IOS-SSH to address CVE-2023-48795 (aka Terrapin Attack).
CSCwn92976	PPP is not establishing when l2tp over ipsec.
CSCwn59814	FLOWDB_OOM condition can lead to packet loss with GRE non-IPSEC tunnel.
CSCwn60286	Memory Leak observed in IPSEC/IKE session bringup with Cert-based Authentication.
CSCwp15054	Memory leak in nbar-sdavc-scheduler.
CSCwo84747	Tunnel delete/create flaps unexpectedly for PWK case for private control NAT changes
CSCwn15850	Crash When "show running-config full | format" Begins to Print QoS Policy-map Config.
CSCwn50935	Crash occurs during haripin call.
CSCwo98465	Crash when receiving BGP MVPN update/withdraw with BGP MVPN update debug enabled.
CSCwq01226	ESP crash @stile_check_and_run_mpe_after_ft ().
CSCwn93483	Device: confd_cli high cpu utilization after executing "show zbfw-dp sessions | tab".

Identifier	Headline
CSCwq31287	Cisco IOS and IOS XE software SNMP denial of service and remote code execution vulnerability.
CSCwn98779	Multihome DC publication has inconsistent domain and mh id.

Open Bugs in Cisco IOS XE 17.12.6

Identifier	Headline
CSCwn85623	Missing Calling-Station-ID in radius messages.
CSCwq22471	Unexpected reload after importing subca chain.
CSCwh36635	Device: confd / SMP crash.
CSCwq08151	Unexpected reload while running a Speed Test from vManage and leaving the page before it completes.
CSCwo57783	"NHRP Encap Error for Purge Request" populates on spoke despite correct routing at HUB.
CSCwm54978	Device: Subject polaris_iosd_t denials.
CSCwp40010	RP crash while debugging IKEv2.
CSCwp38609	CTS Trustpoint loop triggers PKI segfault.
CSCwq49981	Call Failures due to FPI resource leaks.

Resolved Bugs in Cisco IOS XE 17.12.5d

Identifier	Headline
CSCwo38924	Cisco IOS XE Software Secure Boot Bypass Vulnerability
CSCwo38903	Cisco IOS XE Software Secure Boot Bypass Vulnerability
CSCwn48408	Cisco IOS XE Software HTTP API Command Injection Vulnerability
CSCwm57073	Cisco IOS XE Software WebUI Reflected Cross-Site Scripting Vulnerability
CSCwm41327	Cisco IOS XE Software CLI Argument Injection Vulnerability
CSCwm99306	Cisco IOS and IOS XE Software TACACS+ Authentication Bypass Vulnerability
CSCwp03900	Cisco IOS XE Software Simple Network Management Protocol Denial of Service Vulnerability
CSCwq31287	Cisco IOS and IOS XE Software SNMP Denial of Service and Remote Code Execution Vulnerability

Open Bugs in Cisco IOS XE 17.12.5d

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

Resolved Bugs in Cisco IOS XE 17.12.5c

Identifier	Headline
CSCwp66926	FNF AOR might have double-free risk.
CSCwj01917	After upgrade to 17.9.4a, Cellular Interface IP ADDRESS NEGOTIATED mismatch.
CSCwn78740	Silent reboot with "cpp_ha_top_level_server fault on fp_0_0", CpuCatastrophicError.

Open Bugs in Cisco IOS XE 17.12.5c

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

Resolved Bugs - Cisco IOS XE 17.12.5b

Identifier	Headline
CSCwo67161	IPsec-related crash on an IOS-XE device.

Open Bugs - Cisco IOS XE 17.12.5b

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

Resolved Bugs in Cisco IOS XE 17.12.5a

Bug ID	Description
CSCwn22830	vDSP container network mask mismatches with VPG interface.
CSCwj90434	Ping failed on cellular interface - tail drop observed on Cellular interface.
CSCwk44078	GETVPN / Migrating to new KEK RSA key doesn't trigger GM re-registration.
CSCwk42190	Config and dp show command don’t match the dp oper output.
CSCwj06950	Device DSL module gets stuck in a booting state.
CSCwf79399	IOS-XE Port-channel sub-interface overload Port-channel interface must be created first and delete.
CSCwj80411	Deleting and adding the rules in a ZBFW policy with 510 rules results in traffic drop.
CSCwn36839	Software crash on device - Last reload reason: Critical software exception.
CSCwj63533	Found Core files in device for suit cEdgePolicy_serv_ipv6_trans_ipv4.
CSCwf77488	IOSd crash after radium boot up and online.
CSCwm14665	Enable BFD L2 messages in the Punt path for devices.

Bug ID	Description
CSCwi85934	Device: C-NIM-1M with 1G; Memb-intf add to portchannel fails with 'Error: Interface type mismatch'.
CSCwm14462	IPv6 flowspec nexthop redirect policy not redirecting the traffic on IOS XE.
CSCwm05524	Unexpected reload due to "cpp-mcplo-ucode" Process when handling fragments with SRv6 routing.
CSCwj84949	Unencrypted traffic due to Non-Functional IPsec tunnel in FLEXVPN hub & spoke setup.
CSCwn07540	Device crashed due to IOSXE_INFRA-2-FATAL_NO_PUNT_KEEPALIVE.
CSCwm98642	OMP is redistributing summary routes in the service VPN even though the exact networks don't exist.
CSCwi59183	C-NIM-1X sometimes print "FPGA firmware is upgraded. Need to reload the module".
CSCwn15231	Device null-way audio within the same layer2.
CSCwk53680	Inbound calls through VG400 results in phantom calls (64.3.0, 60.1.4, 62.3.3).
CSCwm80356	LLDP packets dropped when came through active port-channel interface.
CSCwi96187	P-5GS6-GL FN980 modem fW upgrade failing when two modems on device.
CSCwk79454	Endpoint Tracker does not fail if default route is removed.
CSCwk27099	Cellular connection is picking the wrong profile.
CSCwk61238	RRI static not populating route after reload if stateful IPSec is configured.
CSCwk75459	MGCP GW fails to respond with 250 OK when there's a delay from dataplane in gathering stats.
CSCwk87452	Procyon synchronize DTL does not wait until complete due to compiler optimization.
CSCwm79570	Cisco IOS and IOS XE SNMP Denial of Service Vulnerabilities.
CSCwm89600	Cisco IOS, IOS XE, and IOS XR SNMP Denial of Service Vulnerabilities.
CSCwm79581	Cisco IOS and IOS XE SNMP Denial of Service Vulnerabilities.
CSCwm79554	Cisco IOS and IOS XE SNMP Denial of Service Vulnerabilities.
CSCwm79596	Cisco IOS and IOS XE SNMP Denial of Service Vulnerabilities.
CSCwm79577	Cisco IOS and IOS XE SNMP Denial of Service Vulnerabilities.
CSCwm08791	Dial-peer never recovers an active state if it goes partial or busyout.
CSCwm08791	Dial-peer never recovers an active state if it goes partial or busyout.

Bug ID	Description
CSCwm01029	CUBE gets forked 180 and 183 with SDP, CUBE is not adding SRTP key when sending 183, causing failure.
CSCwn49403	CUBE incorrectly offers rtp instead of srtp in 200OK for srtp fallback scenario.
CSCwn19326	CDR file accounting creates dummy files.
CSCwm03319	Optimize voip trace handling with tenants.
CSCwm73825	Crash observed on router, while performing the conference call.
CSCwn48914	Router crash during SGW sync in VOICE REG BG Process.
CSCwm32946	CUBE doesn't relay/pass 488 Media Unacceptable from one leg to another leg for FAX (T.38) Re-INVITEs.
CSCwi77331	IOS-XE unexpected reboot after CLI "show sip-ua connection".
CSCwn09710	Memory leak under *Dead* caused by AFW_application_proc.
CSCwn60303	Router cube sip-ua commands lost after reload.
CSCwn13988	CDR file accounting credentials exposure.
CSCwm91190	MWI app not registering on Vcube.
CSCwk44855	Cannot dial to/from phone after it reboots in survivability mode.
CSCwm82247	CUBE memory leak for SIP out-of-dialog SUBSCRIBE under CCSIP_SPI_CONTROL process.
CSCwm79213	"setPthruCryptoData: mfPthruCrypto NULL" showing up excessively in the log.
CSCwm91175	OOD Subscribe with event message-summary is causing memory leak on CUBE.
CSCwm47634	No audio issue on call transfer and conference.
CSCwm39795	HA Module DSP_MSP reported CALL_MODIFY RECREATE failure on standby.
CSCwm79956	Memory leak under *Dead* caused by AFW_application_proc.

Open Bugs in Cisco IOS XE 17.12.5a

Identifier	Headline
CSCwn92855	Device Breakout Port fails to initialize.
CSCwn97600	BFD flapping on PWK ipsec-rekey on all cEdge.
CSCwe23188	Upgrade from vmanage declared successful even though device boots up with different version than requested.
CSCwk87338	SNMPv3 user credentials to be stored as part of running-configuration with encryption.

Resolved Bugs - Cisco IOS XE 17.12.4b

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

Open Bugs - Cisco IOS XE 17.12.4b

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

Resolved Bugs in Cisco IOS XE 17.12.4a

Identifier	Headline
CSCwm30984	ZBFW TCAM misprogramming after rules are reordered on the device - CCE changes.
CSCwi87546	CPP unexpectedly reboot due to QFP CPP stuck at waiting for rw_lock - Lock id of 0 released.
CSCwj40589	Endpoint tracker using DNS does not log "DOWN" message when DNS server reachability is lost.
CSCwm60651	HTX: UTD snort crash at memif_shm_peek_first_packet (handle=0x0).
CSCwk84047	Memory Leak due to security violation by new MAC address and '"Del Pend" object increases - ACE_IPV4.
CSCwk54544	ZBFW TCAM misprogramming after rules are reordered on the device.
CSCwk50488	Memory leak in fman_rp under acl_db.
CSCwm73524	SAP traffic impacted by UTD security on the device.
CSCwm81900	CPP crashed during UTD security policy config on the device.

Open Bugs in Cisco IOS XE 17.12.4a

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

Resolved Bugs in Cisco IOS XE 17.12.4

Identifier	Headline
CSCwj70335	Fragmented authentication packets in the Crypto IKEv2 protocol are being identified as malformed by devices from third-party vendors.
CSCwj74260	Default setting of Global Punt Policer burst needs to be increased.
CSCwj44868	GETVPN COOP KS: Incorrect severity level for rekey acknowledgement configuration mismatch log message.
CSCwi16716	Device: Router crashed on increasing the gatekeeper cache size.
CSCwj68151	Device: Port-channel with service instances down on C-NIM-2T module.
CSCwi53616	UCS-E160S module remains in a booting state with the device.

Identifier	Headline
CSCwj02246	The SFP EN LED on the device does not light up after the interface is enabled with the **no shutdown** command.
CSCwj21653	Device: Kernel crash over continuous reloads.
CSCwi29637	The SFP interface on the device is shut down, but the interface on the connected device remains up.
CSCwj09284	Unexpected reboot in WLC due to SSL.
CSCwi98707	Device: PCM captures on voice-port fail or cause NIM module reloads.
CSCwi40603	Memory leak in the crypto IKMP process .
CSCwj36946	Device: ROMMON 17.6(8.1r) release for auto-upgrade.
CSCwj34578	NAT46 translations are dropped when the NAT64 router also functions as a Carrier Supporting Carrier (CSC) Customer Edge (CE) device.
CSCwi55183	"crypto pki certificate pool" in the running configuration.
CSCwk15127	Failure to communicate a period of time after the stp status changes.
CSCwh37024	The IR1800 PnP process gets stuck when using Verizon cellular backhaul.
CSCwj45130	Segmentation Fault - The process causing the issue is the IPSec dummy packet process.
CSCwj88872	IPsec tunnel fails to establish due to error IPSec policy invalidated proposal.
CSCwj73113	MGCP GW does not respond with 250 OK for a DLCX leading to DLCX loop from CUCM side.
CSCwi59854	**show sdwan policy service-path** command displays inconsistent results with app name specified.
CSCwj38106	Only one split-exclude subnet is pushed to client PC with IOS-XE headend for a RA VPN connection.
CSCwh73320	The NAT pool is not functioning under a 16 prefix. The number of available addresses is zero.
CSCwi89822	Unexpected reboot due cpp ucode on device.
CSCwh09033	Router unable to boot with C-NIM-8T module.
CSCwi68865	Memory leak in Crypto IKEv2 due to C_NewObject.
CSCwf87975	The router crashed when the port-channel interface flapped while using a large number of per-tunnel QoS policies.
CSCwi59834	Device: In IOS XE 17.9, the entSensorThresholdValue OID for PDU1 is missing.
CSCwh86053	Enhancement: Configuration parser issue for NAT with extendable and redundancy options.

Identifier	Headline
CSCwj42249	Disabling PMTU Discovery along with an MTU change and BFD flap disrupts packet duplication.
CSCwj36915	C-NIM-2T: macsec not working under LACP port-channel member port.
CSCwi78365	Trim installed certificate on upgrade.
CSCwj72888	Reload in tcp_sanity due to l4 pointer not set.
CSCwi93784	(SWI Case 01257768) Firmware upgrade does not work properly on P-LTE-MNA with IOS versions 17.12.1a and 17.12.2.
CSCwj33292	AnyConnect connection trough IPSec fails when connecting from an RDP user to an IOS/IOS-XE headend.
CSCwj06622	Segmentation fault and core files are seen on IOS-XE in controller-manged SD-WAN due to speedtest.
CSCwi16111	ipv6 tcp adjust-mss not working after delete and reconfigure.
CSCwj29947	AAA authorization failure during IKEv2 phase negotiation caused unexpected reboot.
CSCwj79197	Device: Unexpected reload when using the packet trace feature.
CSCwj13681	Device can only store 64 FQDN patterns, but config accepts more than 64.
CSCwj23735	CUBE - "rtp port range" configuration lost under "voice service voip" after reload.
CSCwj26668	Wrong audio rtp packet marking for SCCP SRST.
CSCwj23804	Password created with "key config-key password-encrypt" ending with a "\" are lost after reload.
CSCwj59262	SIPREC Secure media forking -1 of 2 Audio Streams is encrypted due to same key sent for both streams.
CSCwj95128	CUBE incorrectly changes the dtmf payload in asymmetric case.
CSCwj93967	History-Info header compatibility between CUBE and MS Direct Routing.
CSCwj05013	CUBE Media Proxy(CMP) dual forking not working after upgrade.
CSCwj82258	Router may crash during transfer call flow in SRST.
CSCwi69071	Unexpected reload caused by crash in 'Skinny Msg Server' process.
CSCwj98360	Media forking not working in CUBE.
CSCwj54666	SIP cause code incorrect for CCAPI cause code 31.
CSCwk08864	"authentication" command under dial-peer is missing "challenge.
CSCwj61168	Router experiences memory leak in ucode_pkt_PPE0 process.

Identifier	Headline
CSCwh81312	No memory seen in standby router .
CSCwj41553	AOR is not updating the number, when SGW initiates a call to TDM.
CSCwj75508	After reload, SRST running on router fails to register SCCP phones.

Open Bugs in Cisco IOS XE 17.12.4

Identifier	Headline
CSCwh86922	Unconfiguring EVC will not restore the original MAC filter table entries on the interface.
CSCwi03502	Create CLI to push at#enadis=0 followed with at#reboot to FN980 required when configuring Multi-PDN.
CSCwk31560	After the device is reloaded, the NAT (Network Address Translation) command becomes unreadable or is not displayed correctly.
CSCwk44078	GETVPN / Migrating to new KEK RSA key does not trigger GM re-registration.
CSCwj06950	DSL module gets stuck in the booting state.
CSCwk53296	UCSE interface shutdown setting mismatch.
CSCwj21653	Kernel crash after continuous reloads.
CSCwi31110	Traceback observed @_nhrp_cache_delete due to negative global cache count.
CSCwk22942	Unable to build two IPSec SAs w/same source/destination where one peer is PAT'd through the other
CSCwk23723	Mean queue calculation is incorrect on WRED hierarchical QoS.
CSCwk58303	Watchdog crash during IPv6 cef adjacency routines.
CSCwk63722	Startup configuration failure post PKI server enablement.
CSCwj77594	IOS XE Controller Mode: WAN IP can be configured as the SYSTEM IP.
CSCwh36635	17.13 : 8300 2 RU : confd / SMP crash.
CSCwi85934	C-NIM-1M with 1G; Memb-intf add to portchannel fails with the error: Interface type mismatch.
CSCwj16153	10G front-panel port does not go down on single-mode fiber when the Rx side goes down.
CSCwk54544	SD-WAN ZBFW TCAM misprogramming occurs after rules are reordered on the device.
CSCwj84949	Unencrypted traffic due to a non-functional IPsec tunnel in a FlexVPN hub-and-spoke setup.

Identifier	Headline
CSCwi56641	100G/40G QSFP fiber link reports a link-flap error when the peer device reloads.
CSCwj90614	High CPU utilisation for confd_cli.
CSCwk03686	Crash due a segmentation fault due to a negative value.
CSCwj92560	The STCAPP command is no longer present in the configuration after the device undergoes a reload.
CSCwi59183	C-NIM-1X occasionally prints "FPGA firmware is upgraded. Need to reload the module."
CSCwk31715	After deleting a NAT configuration, the IP address still shows up in routing table.
CSCwh45389	Key manager crashes after changing the hostname with usage keys.
CSCwk12524	Device reloaded due to ezManage mobile app service.
CSCwk53680	Inbound calls through VG400 results in phantom calls (64.3.0, 60.1.4, 62.3.3)
CSCwk65071	Unexpected reboot due to IOSXE-WATCHDOG DBAL EVENTS after Cellular interface flap.
CSCwf91481	Device crashed unexpectedly after a successful WGB/AP configuration deployment from OD.
CSCwi96187	FN980 modem firmware upgrade fails when two modems are present on the device.
CSCwh91136	IOS XE: Traffic is not encrypted and is dropped over the IPSEC SVTI tunnel.
CSCwk52677	C1118-8P / DSL router crashing due to %PLATFORM-3-ELEMENT_CRITICAL memory level / iomd process.
CSCwb47658	Repeated and endless messages "Network change event - activated 4G Carrier Aggregation."
CSCwk30527	IKEv2 session goes down after a reload if the local identity address is assigned to an interface on the switch.

Resolved Bugs - Cisco IOS XE 17.12.3a

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

Bug ID	Description
CSCwk21189	Template attach fail with unknown element: ssh-version in /ios:native/ios:ip/ios:ssh
CSCwk20843	PPPoE with NAT DIA feature validation failed post upgrade.

Resolved Bugs in Cisco IOS XE 17.12.3

Identifier	Headline
CSCwh73350	Device keeps crashing when processing a firewall feature.
CSCwh18120	IKEv2 - diagnose feature is taking 11% CPU during the session bring up.
CSCwf67983	Platform USB disable will not work once USB is removed and inserted in a device.
CSCwi28227	NAT HSL logging vrf-filter does not work on the device.
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.
CSCwh77221	SNMP unable to poll SD-WAN tunnel data after a minute.
CSCwh96578	SKA_PUBKEY_DB leak in TDL.
CSCwh69765	Security policy w/IPS external syslog config failing generation for specific device models.
CSCwi06843	Endpoint tracker triggers a CPU hog.
CSCwh87619	ZBFW is not able to detect packets on TenGig interface.
CSCwh10813	Adding verbose log to indicate grant ra-auto un configures grant auto in PKI server.
CSCwi60312	C-NIM-2T cannot boot up in full configuration: 6x C-NIM-2T + IOS 17.12.02.
CSCwh93257	When two or more IP phones located on the NAT outside network register with the same server, the device generates incorrect or malformed NAT entries.
CSCwi59121	Mobile-app causing excessive authorization attempts with a Null Username.
CSCwh68508	The system experienced an unexpected reboot after setting up the control plane for EVPN MPLS and is starting to receive packets.
CSCwi08171	Device may crash due to Crypto IKMP process.
CSCwi49231	VG410 audio loss for 4 seconds.
CSCwi06404	PKI crash after failing a CRL fetch.
CSCwh50510	Device crash with segmentation fault(11), Process = NHRP when processing NHRP traffic.
CSCwh75800	CUBE device unexpectedly reloads while fetching certificate trustpool for SIP TLS.
CSCwi28781	Epbr will generate error when the policy is added and deleted multiple times.
CSCwi49240	One-way RTP issue including DSP Timeout Messages.

Identifier	Headline
CSCwh45169	Unexpected reboot while dispalying information from cleared SSS session .
CSCwh70449	PMTUD incorrectly converging without attempting to learn a higher MTU.
CSCwh96415	Cannot disable DMVPN logging in IOS-XE 17.8 and higher.
CSCwi25737	Device should discard IKE notification messages with incorrect DOI.
CSCwi14899	Device dropping IPsec traffic when SVI is used as source for DMVPN tunnel.
CSCwh50628	Race condition crash on device.
CSCwf86207	Frame Relay DTE router crashes due to EXMEM exhaustion.
CSCwh72869	cpp_mcplo_ucode crash with port-channel and NAT.
CSCwh99399	ftmd crash observed in ENCS platform while running PWK suite.
CSCwi76087	When attempting an ATO (Assured Tactical Operations), the session fails to establish through the tunnel after repeatedly shutting down and re-enabling the connection in a loop, which simulates unplugging and plugging back in the cable on the customer's end.
CSCwi55379	IPsec traffic is being dropped on Strongswan when PPK is implemented.
CSCwi63042	Packet drops observed between LISP EID over GRE tunnel.
CSCwi79584	Failed to upgrade device via Cisco SD-WAN Manager due to error: system config has been modified.
CSCwi59202	C-NIM-2T w/SwitzerCC in unable to boot up in IOS.
CSCwi30529	AAA:Template push fail when aaa authorization is set to local.

Open Bugs in Cisco IOS XE 17.12.3

Identifier	Headline
CSCwi03502	Creating a CLI to push at#enadis=0 followed with at#reboot to FN980 is required when configuring Multi-PDN.
CSCwi29637	Device SFP interface shut down, but opposing device interface is still up.
CSCwi67621	Critical process cpp_ha_top_level_server fault on fp_0_0 (rc=69).
CSCwj21921	Device: L2TP xconnect stops forwarding traffic after a new subinterface is added.
CSCwi46997	NAT command is not readable after the system is reloaded.
CSCwj07584	Device: Shared HSRP vMAC between multiple interfaces causes a data plane problem.
CSCwi16111	After deleting and reconfiguring the IPv6 TCP adjust-MSS setting, it is not functioning correctly.

Identifier	Headline
CSCwj08744	The system unexpectedly restarts when executing the command 'show running-config full | format'.
CSCwi56641	When the peer device restarts, the device, which uses a QSFP fiber connection for 100G/40G, reports a link-flap error.
CSCwi53616	The UCS-E160S module is stuck in the booting state while being used in a device.
CSCwj13681	The device has a limitation of storing only 64 Fully Qualified Domain Name (FQDN) patterns, yet the configuration allows the input of more than 64 FQDNs.

Resolved Bugs in Cisco IOS XE 17.12.2

Identifier	Headline
CSCwh87343	Cisco IOS XE Software Web UI Privilege Escalation Vulnerability. For more information, see Security Advisory: cisco-sa-iosxe-webui-privesc-j22SaA4z.
CSCwf78735	Device uses the NIM-1T/4T card for interconnection, and NAT+ GRE over IPsec cannot be applied.
CSCwh06834	Using special characters in the password while generating TP generates an invalid TP.
CSCwh20734	Crypto PKI-CRL-IO_0 process crash when PKI trustpoint is requested and deleted.
CSCwh41497	DDNS update retransmission timer fails to work with a traceback error.
CSCwf63706	Device HSRP received unexpected active hello packet when the interface is recovered.
CSCwf49390	Device crashes@crypto_map_unlock_map_head.
CSCwh30377	Device data plane crash in Umbrella/OpenDNS processing due to incorrect UDP length.
CSCwh20577	Crashed by track client thread at access invalid memory location.
CSCwf82676	CPU usage mismatch in **show sdwan system status** vs **show process cpu platform**
CSCwf51206	EVPN: BUM traffic is not flooded to bridge domain interface.
CSCwf80191	Flowspec on device does not revoke.
CSCwf99947	Crash when modifying tunnel after running **show crypto** command.
CSCwf67564	Device observes memory leak at process "SSS Manager".
CSCwf60151	Memory leak with pubd.
CSCwh60190	**ip name-server** command not pushed.
CSCwf56463	IOS process crash during VRRP hash table lookup.
CSCwh11858	Device running IOS-XE crashes when removing FQDN ACL.

Identifier	Headline
CSCwf99906	NTP authentication removed after reload using more than 16 bytes.
CSCwf59173	Segmentation fault at IPv6 BGP backup route notification.
CSCwf67351	Cisco IOx application hosting environment privilege escalation vulnerability.
CSCwf68612	WLC unexpected ueload due to segmentation fault in WNCD process.
CSCwh00963	Unable to migrate from ADSL to VDSL without reboot.
CSCwf41084	Extranet multicast code improvements for better handling of data structure.
CSCwh04884	VC down due to control-word negotiation.
CSCwf26494	BDI + NTP configuration puts DMI process in degraded mode.
CSCwh96700	Carrier Grade NAT reaching max host entries and failing to translate due to gatekeeper

Open Bugs in Cisco IOS XE 17.12.2

Identifier	Headline
CSCwh73350	Router keeps crashing when processing a firewall feature.
CSCwh94906	Segmentation fault crash with Network Mobility Services Protocol (NMSP).
CSCwf67983	The platform USB disable will not work once USB is removed and inserted.
CSCwh22414	Warning and critical CPU utilization thresholds not recomputed when using data-plane-heavy mode.
CSCwh59071	Displays faulty Output for **show int te0/0/0 transceiver** command.
CSCwh16901	HSEC license installation from the workflow does not complete.
CSCwh77221	SNMP unable to poll Cisco SD-WAN tunnel data after a minute.
CSCwh10813	Add verbose log to indicate grant ra-auto un configures grant auto in PKI server.
CSCwh68508	Unexpected reboot after establishing control plane of EVPN MPLS and receiving packets.
CSCwh79161	Device requires Shut/No Shut to populate IP address from modem to host.
CSCwh75800	Router unexpectedly reloads while fetching certificate trustpool for SIP TLS.
CSCwh57544	Silent reload due to LocalSoftADR causes crash without core file.
CSCwi01046	PoE module is not providing enough power to bring the ports after an unexpected reload.
CSCwh50510	Router crash with segmentation fault (11), Process = NHRP when processing NHRP traffic

Identifier	Headline
CSCwd69953	Device driver is not sending NGIO packets to UCSE after the router reload.
CSCwh73320	NAT Pool does not working under prefix 16. Available address = zero.
CSCwh96700	Carrier Grade NAT reaching max host entries and failing to translate due to gatekeeper.
CSCwh45169	Unexpected reboot while dispalying information from cleared SSS session.
CSCwh70449	PMTUD incorrectly converging without attempting to learn a higher MTU.
CSCwf91481	Device crashed unexpectedly after a successful WGB/AP config deployment from OD.
CSCwf00276	Packets with L2TP headers cause device to crash.
CSCwh83228	NHRP phase 3 spoke-spoke cache got purged after 5-6 hours with always on traffic running.
CSCwe54687	After removing the USB from the device, the files copied to it will be deleted.
CSCwh91136	IOS XE:Traffic not encrypted and droped over PSec SVTI tunnel.
CSCwh96415	Unable to disable DMVPN logging.
CSCwh12093	Enable SoS/ROC feature for DSL.
CSCwf86207	Frame relay DTE router crashes due to EXMEM exhaustion.
CSCwh58252	IPv6 SPD min/max defaulting to values 1 and 2.
CSCwh14083	High CPU due to MPLS MIB poll.
CSCwh22981	WNCD process crashes.
CSCwh99513	VPLS IRB not working when traffic came from VPNv4 and next-hop is learned over VPLS.
CSCwh90851	pubd process showing high CPU utilization.
CSCwh83532	1Gig int on device using GLC-SX-MMD are down/down after changing connection.
CSCwh96891	Memory leak with pubd.
CSCwh91085	Convergence improvement after device reboot with mVPN profile 14.
CSCwh58919	NETCONF: DMI enters degraded mode caused by BGP neighbor configured under the SCOPE command.
CSCuu85298	FIB/LFIB inconsistency after BGP flap.
CSCwf83684	IOS XE router may experience "%FMANRP_QOS-4-MPOLCHECKDETAIL:" errors.
CSCwh59926	EEM is running daily instead of weekly or monthly if special strings @weekly or @monthly are used.

Identifier	Headline
CSCwh24280	Mismatch between the resource allocation and "app-resource profile custom" configuration.
CSCwh82668	Incorrect local MPLS label in CEF after BGP flap.
CSCwh95036	Cisco IOS-XE IPv6 based subscription telemetry does not work.
CSCwh99464	Guestshell connectivity not working with NAT overload.
CSCwh30928	SDA - using "spt-threshold infinity" and having LHR+FHR can cause the S,G to be pruned on the RP.
CSCwh01738	Unexpected reload when using rsh/rcmd.
CSCwh04124	Locally generated traffic received on incorrect interface inbound and dropped by ACL.
CSCwh67285	WLC unable to get telemetry data due to pubd unexpected reload and fail.
CSCwh96332	Device crash due to dhcpd_binding_check.
CSCwh56940	Site tag change wncd working/failing EAP-TLS.
CSCwh44418	ARP incomplete in VRF Mgmt-intf - G0/0/0 - Switch -G0.
CSCwh46559	LLDP location information not sent when configured.
CSCuv36790	**clear bgp** command does not consider AFIs when used with update-group option.
CSCwh02698	Device sending incomplete SGT to ISE.
CSCwh05869	Only portion of HSRP config being pushed via CLI ADDON template.
CSCwf53750	"match pktlen-range" does not work with GRE/IPSEC GRE.
CSCwh60107	In the show tech file, "enable secret" does not get hidden.
CSCwh45579	Unexpected reload on device ucode core @l2_dst_output_goto_output_feature_ext_path.
CSCwh95024	ISIS crash in local uloop.
CSCwh41155	Wrong /32 self, complete map-cache entry for fabric hosts on iBN when overlapping summary exists.
CSCwh31485	Member interface config not applied with mis-match in pcakages.conf files.
CSCwh72437	WLC not sending accounting start for user auth after machine auth on 9105AXW RLAN dot1x port.
CSCwi00680	Router unexpectedly reloads while using DHCP for ISG.
CSCwh96823	IOS-XE router not installing classless-static-routes from DHCP option 121.
CSCwh77706	SVL, 10G link on the active chassis will go down after reload.

Identifier	Headline
CSCwh02592	Device sync fails when device prompt comes along with device banner and TACACS is used.
CSCwh84850	Unexpected reboot in device due to SISF and STP initialization.
CSCwh64903	Crash on device polling SPA sensor data.
CSCwh53432	VLAN name mismatch when authorizing vlan name from radius server and enable vlan fallback.
CSCwh21796	Password getting visible for the mask-secret in show logging.
CSCwh50104	Upgrade failing with config check track-id-name.
CSCwf59929	CTS CORE process crash after configuring role based ACL.
CSCwh81471	IPv6 traffic is passing through when the client is in Webauth Pending state (CWA).
CSCwh93772	Option 121 never requested by IOS-XE client.
CSCwh06087	[IPv6 BGP] multiple sourced paths present for the same prefix.
CSCwh29120	IP SPD queue thresholds are out of range.
CSCwh14953	CBQoS polling for the object cbQosCMPostPolicyBitRate returns incorrect value.
CSCwh89096	Device unexpected reload.
CSCwh99597	After migration MAC/IP only MAC is advertised.
CSCwh75992	"BGP Router" process crash.
CSCwh48058	Memory leak under MallocLite/AAA proxy with NETCONF/RESTCONF.
CSCwh76920	Memory leak in linux_iosd-imag due to SNMP.
CSCwh75112	After a reboot, EAP-FAST/PEAP does not authenticate unless credentials are changed.

Resolved Bugs in Cisco IOS XE 17.12.1a

Identifier	Headline
CSCwe82666	Not all HSL entries get pushed to device if more than 1 HSL entries are configured.
CSCwe31226	Issues/discrepancies around CPU alarms generated and sent to device.
CSCwe98345	FHRP stay in active/active state after physical interface flap.
CSCwe43341	TLS control-connections down, traffic from controller dropped with SDWAN Implicit ACL Drop.
CSCwe18124	MACsec remains marked as secured, but randomly the traffic stops working.
CSCwe18276	Route-map not getting effect when its applied in OMP for BGP routes.

Identifier	Headline
CSCwb74821	Unexpected behavior due to unstable power source.
CSCwe81182	(EPC, packet-trace) for IPsec running COFF (Crypto Offload).
CSCwe63222	Certificate output is not getting changed on renew when Cloud Certificate Authorization is Automated.
CSCwe93905	NAT ALG is changing the Call-ID within SIP message header causing calls to fail.
CSCwe90501	Router upgrade fails due to **advertise aggregate** with VRF.
CSCwe85195	AAR: BoW feature ignoring color preference from Tiered Transport preference configuration.
CSCwe14885	VPN is established although the peer is using a revoked certificate for authentication.
CSCwe88689	ROMMON for auto-upgrade.
CSCwd53710	Crash seen when umbrella/zscaler template pushed to device when name_lookup takes > 30 sec.
CSCwe66318	NAT entries expire on Standby Router.
CSCwd84599	Dataplane memory utilization issue - 97% QFP DRAM memory utilization.
CSCwd59722	Unexpected reboot due to IOSXE-WATCHDOG: Process = Crypto IKMP.
CSCwe70374	Platform punt-policer is not configurable.
CSCwe73408	For some error condition platform_properties may double free.
CSCwd42523	Same label is assigned to different VRFs.
CSCwe85301	Crypto PKI-CRL-IO_0 process crash when PKI trustpoint is being deleted.
CSCwe12194	Auto-Update Cycle incorrectly deletes certificates.
CSCwe57239	All usb internal communcation is closed when using **platform usb disable** command.
CSCvz82148	%CRYPTO_SL_TP_LEVELS-6-VAR_NEW_VALUE message is observed in each write config with same crypto value.
CSCwe85421	Device BFD Session Down with interface flap.
CSCwe95606	Double GR_Additional log enablement defect.
CSCwe31471	Segmentation fault in PB rx when per-tunnel qos config withdraw.
CSCwe89404	No way audio when using secure Hardware conference with secure endpoints.
CSCwd39257	IOS-XE cpp crash when entering **no ip nat create flow-entries**.
CSCwe70642	AAR overlay actions are applied to DIA traffic.

Identifier	Headline
CSCwa96399	Configuring **entity-information** xpath filter causes syslogs to print, does not return data.
CSCwe79007	Device unexpected reload when doing ips test with UTD IPS engine.
CSCwe31281	Autotunnel Ipsec tracker: Tracker does not come up at all on vedge.
CSCwd93401	AppNav-XE: Policy-map edit on cluster with multiple service context fails to program TCAM.
CSCwf65696	Non-fabric- Load the minimal bootstrap configs again if device rebooted without saving the configs.
CSCwd76648	Port-channel DPI Load-Balancing not utilizing all the member-links.
CSCwe39011	GARP on port up/up status from router is not received by remote peer device.
CSCwb39206	Enable VFR CLI.
CSCwe85022	Telstra Cert: FN980 modem (P-5GS6-GL) is showing 4 additional NR bands support - 1, 3, 7, and 28.

Open Bugs in Cisco IOS XE 17.12.1a

Identifier	Headline
CSCwf70854	Changes to speed on the interface via CLI/GUI dont go through unless first done via shell access.
CSCwh67812	Unable to configure crypto map on a physical interface due to which crypto map-based VPN's cannot be formed.
CSCwf72079	Router unexpectedly reloads due to 'LocalSoft'.
CSCwh06834	Using special characters in the password while generating TP generates an invalid TP.
CSCwh06870	APN password in plain text when Cellular controller profile is configured.
CSCwf87292	Punt keep alive failure crash on controller managed device apparently due to data packets.
CSCwf83850	With Pure IPV6, minimal bootstrap unable to onboard Non-Fabric - ipv6 config missing in wan int G1.
CSCwf94294	Misprograming during vpn-list change under data policy.
CSCwa57254	Router Silent Reload due to CpuCatastrophicError.
CSCwf55145	SFP transceiver DOM not working after some time, however interface forwards the traffic as expected.
CSCwf94052	BFD going down for newly onboarded device.

Identifier	Headline
CSCwh01095	Rapid memory leak on ngiolite process.
CSCwf61720	No licenses in use after upgrading from Traditional to Smart licensing IOS-XE versions.
CSCwf80927	Speed tests to internet from device triggered will fail sometimes.
CSCwf84522	Unexpected reboot due QFP UCode due to IPSec functions.
CSCwh00320	**Show run** and other show commands not in sync after removing GigabitEthernet3.
CSCwf44703	NAT64 prefix is not originated into OMP.
CSCwf99947	Crash when modifying tunnel after running **show crypto** commands.
CSCwf77252	SIP calls not working on device with ZBFW enabled.
CSCwf96416	Could not access any device show commands at all.
CSCwf67564	RP3 observes Memory Leak at process SSS Manager.
CSCwf34171	**Configure replace** command fails due to the license udi PID XXX SN:XXXX line on IOS-XE devices.
CSCwh01425	ITU channel configuration seems not working on router.
CSCwh00963	Unable to migrate from ADSL to VDSL without reboot on device.
CSCwf69062	SDRA-SSLVPN : The SSLVPN session closes with re-authentication error after some interval of time.
CSCwf79264	Traffic forwarded to wrong VPN hence traffic gets wrong zonepair matched and gets dropped.
CSCwf71557	IPv4 connectivity over PPP not restored after reload.
CSCwf45486	OMP to BGP Redistribution Leads to Incorrect AS_Path Installation on Chosen Next-Hop.
CSCwh01313	Unexpected reboot due qfp Ucode due to IPsec functions.
CSCwf95527	BFD Entries Removed.
CSCwe26895	Router has Local Soft ADR crash, writes flat core, and reloads.
CSCwh01318	Multiple Crashes observed on device platform due to Memory Exhaustion.
CSCwf71116	Static route keep advertising via OMP even though there is no route.
CSCwf60120	Static NAT entry gets deleted from running config; but remains in startup config.
CSCwh00332	B2B NAT: when configration ip nat inside/outside on VASI intereface,ack/seq number abnormal.
CSCwf49390	Device crashes with crypto map unlock map head.

Identifier	Headline
CSCwf78735	Device uses the NIM-1T/4T card for interconnection, and NAT with GRE over IPsec cannot be applied.
CSCwf84960	C-NIM-2T: LED L remains green after port shutdown.

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 results 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.

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.

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.