

Caveats

This chapter describes open and resolved severity 1 and 2 caveats and select severity 3 caveats:

- The "Open Caveats" sections list open caveats that apply to the current release and may apply to previous releases. A caveat that is open for a prior release and is still unresolved applies to all future releases until it is resolved.
- The "Resolved Caveats" sections list caveats resolved in a specific release, but open in previous releases.

The bug IDs are sorted alphanumerically.

Note The Caveats section includes the bug ID and a short description of the bug. For details on the symptoms, conditions, and workaround for a specific caveat you must use the Bug Search Tool.

- Open Caveats – Cisco IOS XE Dublin 17.12.7, on page 1
- Resolved Caveats – Cisco IOS XE Dublin 17.12.7, on page 2
- Resolved Caveats – Cisco IOS XE Dublin 17.12.6, on page 2
- Open Caveats – Cisco IOS XE Dublin 17.12.6, on page 2
- Resolved Caveats – Cisco IOS XE Dublin 17.12.5, on page 2
- Open Caveats – Cisco IOS XE Dublin 17.12.5, on page 3
- Resolved Caveats – Cisco IOS XE Dublin 17.12.4, on page 3
- Open Caveats – Cisco IOS XE Dublin 17.12.4, on page 3
- Resolved Caveats – Cisco IOS XE Dublin 17.12.3, on page 3
- Open Caveats – Cisco IOS XE Dublin 17.12.3, on page 4
- Resolved Caveats – Cisco IOS XE Dublin 17.12.2a, on page 4
- Open Caveats – Cisco IOS XE Dublin 17.12.2a, on page 4
- Resolved Caveats – Cisco IOS XE Dublin 17.12.1, on page 5
- Open Caveats – Cisco IOS XE Dublin 17.12.1, on page 6
- Cisco Bug Search Tool, on page 6

Open Caveats – Cisco IOS XE Dublin 17.12.7

There are no open caveats in this release.

Resolved Caveats – Cisco IOS XE Dublin 17.12.7

Identifier	Headline
CSCws53320	After upgrading to 17.12.4/5, no Rx values can be received on interface Te0/0/26.
CSCwr15734	Multicast ASM traffic replication issue when RP-PE is located after the LHR.
CSCwt05214	Syslog entry is not available for manual switch.

Resolved Caveats – Cisco IOS XE Dublin 17.12.6

Identifier	Headline
CSCwo58612	REP loop formed with multicast MAC when advertised via VRRP protocol.
CSCwp09722	Smart licensing is not remaining registered status while the upgrading OS.
CSCwp95127	Memory leak due to chunk manager process in router.
CSCwp12666	Router goes down with nested peer-policy templates.

Open Caveats – Cisco IOS XE Dublin 17.12.6

Identifier	Headline
CSCwp64279	CFM MIP auto-creation issue: MIP not displayed in link-traces.

Resolved Caveats – Cisco IOS XE Dublin 17.12.5

Identifier	Headline
CSCwk46171	Enabling T1/E1 TPoP causes latency for control plane packets.
CSCwm91197	Silent reload of 3GMS IM due to PCI transaction failure.
CSCwm00642	RSP reboots while configuring CEM IDs on ACR.
CSCwm86214	LDP session flap causes memory leak for EMPLS3LD which leads to RSP crash.
CSCwk58917	L-bit propogation not enabled for LOF alarm after T1/E1 framing change with framed SAToP.

Open Caveats – Cisco IOS XE Dublin 17.12.5

Identifier	Headline
CSCwk99487	Silent reload happens on router.
CSCwi76112	Message to be displayed for M13 framing when configured with clear-channel.

Resolved Caveats – Cisco IOS XE Dublin 17.12.4

Identifier	Headline
CSCwj71820	L2VPN pseudowire configuration is causing the GNMI state go down

Open Caveats – Cisco IOS XE Dublin 17.12.4

Identifier	Headline
CSCwf32880	QoS performance enhancement for tagged EVC
CSCwi64206	Port LED status glows in green color even after the peer end connection is removed & same vice versa

Resolved Caveats – Cisco IOS XE Dublin 17.12.3

Identifier	Headline
CSCwh88274	Unable to remove service-policy from from standby member link
CSCwi75499	Lost CEM circuit configuration after reboot
CSCwh68394	Unable to remove the service instance under interface
CSCwh85621	The **show platform ha cef ip/ipv6** command is displaying partial output for POCH interface
CSCwi85575	The router drops Wake on LAN (WoL) packet for directly connected interface
CSCwh57819	IP services are down in the device after each reboot
CSCwh84408	The process pubd is not running in NCS4201-02 and RSP2 device
CSCwj01024	ISIS: Counter for the number of redistributed routes does not get decremented

Open Caveats – Cisco IOS XE Dublin 17.12.3

Identifier	Headline
CSCwh17987	NCS4201-02: traffic drop seen when BW on the Gig interface is changed to 100 Mb with MTU beyond 5000
CSCwj05647	3GMS Serial interface protocol down with specific Modem
CSCwh66210	Netconf RPC failed to apply if increase mpls MTU limit to 9644 bytes
CSCwj06370	Serial cease traffic when configuring module other port
CSCwi64206	Port LED status glows in green color even after the peer end connection is removed and same vice versa
CSCwh59032	CPE SIT: Data structure error pointing to rsvp-db during TE FRR
CSCwh75614	Increased CPU after upgrading router to 17.6.3 from 16.9.4 when 1000 SLM/DMM sessions are configured

Resolved Caveats – Cisco IOS XE Dublin 17.12.2a

Identifier	Headline
CSCwf81523	OCX: traceback seen IOSXE_RP_SPA-3-IOMD_CONFIG_FAIL: when mode sonet is configured.
CSCwh30217	NCS4200-3GMS: With rate of OC-12, the threshold sf-ber 3 is added under the `show running-config` command.
CSCwh87343	Cisco IOS XE Software Web UI Privilege Escalation Vulnerability.
CSCwh04884	VC Down due to control-word negotiation
CSCwf79476	When certificate issue `show platform sudi certificate sign nonce xxxx`, Flaps L3 interfaces
CSCwh75169	ISIS: Redistribution prefix threshold is reached with lesser prefixes.
CSCwf16577	BFD session down alarm does not clear after fault recovery.

Open Caveats – Cisco IOS XE Dublin 17.12.2a

Identifier	Headline
CSCwh75614	IP SLA Multicast configuration Not Working

Identifier	Headline
CSCwh82358	Service Instance IDs of integers 4001-5000 is not supported.
CSCuv05226	VRF is not deleted after replacing default configuration.
CSCwh66210	Netconf RPC failed to apply if MPLS MTU limit is increased to 9644 bytes.
CSCwh68394	Unable to remove the service instance under interface.
CSCwh89032	Remove vulnerability in open port.

Resolved Caveats – Cisco IOS XE Dublin 17.12.1

Identifier	Headline
CSCwd78618	IMASER14A/S does not boot.
CSCwe98227	The "show version" does not display details of T1/E1 interfaces for 8D and 32D IMs.
CSCwd90840	Mcast data traffic is getting dropped over vpls.
CSCwe38904	Frame loss seen for 64 bytes packet size for rate step 2333333/all kbps.
CSCwf42164	No snmp trap link-status get re-added after IM reload.
CSCwf49426	PAIS alarm get reported after IM OIR.
CSCwf48343	Display issue when Label pointing in LB object in BGP-PIC edge case.
CSCwd85267	FR Port mode - show interface CLI does not display FR PW statistics.
CSCwd25376	Loopback local on 3GMS IM causing BIP B2 counters increment under show controller CLI.
CSCwe54549	SFP not detected due to checksum error.
CSCwe10460	Power sensor threshold warning alarms in EPNM.
CSCwe58324	Node reload observed after routing change in core.
CSCvy81362	Controllers are down due to LP-LOP alarm After CE reboots.
CSCwf67803	DS3_ADMIN_DOWN gets cleared after IM OIR and displaying LINK_DOWN alarm in 3GMS.
CSCwd46121	Time stamp issue on Transparent clock for 1G PORTS.
CSCwe38959	rs232 ASYNC PW service with full scale seeing packet and byte drops intermittently.
CSCwe13024	RSP2: All readings for Power supply unit reflect as zero though the unit is functional.

Identifier	Headline
CSCwd67723	In IMA32D/IMA8D card, sometimes change in E1 controller config(after ctrlr flap)results in IM reboot.
CSCwe27336	Cylon error logs during reload.
CSCwe19162	After SSO: False Alarm on CNAAP.
CSCwe55191	ISIS neighbors flap during switchover when authentication is enabled.
CSCwe95820	VRF Static Route Redistribution into EIGRP fails.
CSCwe53345	External R1 10M is not selected after double SSO with GNSS.
CSCwd66936	RSP2 UDP pseudowire stuck in activating.
CSCwe36122	ISIS crash when performing TI-LFA calculation.
CSCwe27155	Seen traffic drop with BDI shut (IP_FRR configs).

Open Caveats – Cisco IOS XE Dublin 17.12.1

Identifier	Headline
CSCwf23533	PTP-G8275.1 Profile - High Offset Seen on BC th data traffic.
CSCwf71463	With traffic ON, when speed lowered on ASYNC port, SYNC port CEM traffic gets impacted.
CSCwf65076	The isis hello-interval minimal configuration causes ASIC lock.
CSCwf18420	LLDP does not announce dynamically assigned VLAN.
CSCwf68400	RSP3:<group>0</group> additional value gets added during fetch, applying the same config fails.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST), the online successor to Bug Toolkit, is designed to improve effectiveness in network risk management and device troubleshooting. You can search for bugs based on product, release, and keyword, and aggregates key data such as bug details, product, and version. For more details on the tool, see the help page located at http://www.cisco.com/web/applicat/cbsshelp/help.html