

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.

- Resolved Caveats - Cisco IOS XE Dublin 17.12.7, on page 2
- Open 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 4
- 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 5
- Resolved Caveats - Cisco IOS XE Dublin 17.12.1, on page 5
- Open Caveats - Cisco IOS XE Dublin 17.12.1, on page 7
- Cisco Bug Search Tool, on page 7

Resolved Caveats - Cisco IOS XE Dublin 17.12.7

Identifier	Headline
CSCws31099	ASR903: BIDI Optics: Observing bandwidth set to 1Gig on 10G interface.
CSCwr11772	The SONET-APS controller level configuration **overhead tunnel aps_all** displays maximum CEM-PW's error.
CSCwr34094	ASR903 OC3 license counter mismatch.
CSCwt05214	Syslog entry is not available for manual switch.

Open Caveats - Cisco IOS XE Dublin 17.12.7

There are no open caveats in this release.

Resolved Caveats - Cisco IOS XE Dublin 17.12.6

Identifier	Headline
CSCwo81175	A900-RSP3C-400-S: uea_mgr fault on fp_0_0 (rc=139) reported with 17.3.3, 16.9.3 and same not seen on 03.18.02.SP.
CSCwp00333	IPv6 and IPv4 reachability fails after removing a member interface from port-channel in ASR 903.
CSCwp12666	ASR 902 router goes down with nested peer-policy templates.

Open Caveats - Cisco IOS XE Dublin 17.12.6

There are no open caveats in this release.

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.

Identifier	Headline
CSCwk58917	L-bit propogation not enabled for LOF alarm after T1/E1 framing change with framed SAToP.
CSCwm04389	Chassis reloaded after RP redundancy force-switchover.
CSCwn24964	Multicast traffic is dropped after interface flap.

Open Caveats - Cisco IOS XE Dublin 17.12.5

Identifier	Headline
CSCwm38823	ECMP is not functioning as expected after one of the link flaps for BGP learnt prefix.
CSCwi76112	Message to be displayed for M13 framing when configured with clear-channel.
CSCwn56729	CRC errors are reported on IMA8Z card (RSP3c) because of the reliability of the link goes down.
CSCwn48959	Unable to configure 8000 EFP's after enabling **efp_feat_ext** template.

Resolved Caveats - Cisco IOS XE Dublin 17.12.4

Identifier	Headline
CSCwj05647	3GMS serial interface protocol goes down with specific modem
CSCwi74892	VLAN tagged pause frames get flooded towards ASR903 (RSP3) and caused port-channel flap.

Open Caveats - Cisco IOS XE Dublin 17.12.4

Identifier	Headline
CSCwj38216	BDI ARP is not learning but peer side BDI MAC is learning through VC
CSCwj72178	ASR903(RSP3) - OSPF not coming on G8032 vlan post reload
CSCwk02087	BFD stuck in INIT state for interface Te 0/0/0 and Te 0/4/3

Resolved Caveats - Cisco IOS XE Dublin 17.12.3

Identifier	Headline
CSCwi51850	ASR903 - RSP3: Traffic drop observed for specific EFP due to VOQ failure.
CSCwh42209	RSS memory increment continuously seen in uea_mgr process upon system event.
CSCwh88274	Unable to remove service-policy from from standby member link.
CSCwi75499	Lost CEM circuit configuration after reboot.
CSCwh84309	With Telcordia profile, Ethernet interfaces sec admin state is not going to AINS state.
CSCwh80239	ASR900 RSP3 - IP SLA Multicast configuration not working

Open Caveats - Cisco IOS XE Dublin 17.12.3

Identifier	Headline
CSCwj05647	3GMS Serial interface protocol down with specific Modem
CSCwi74892	VLAN tagged pause frames were flooded towards ASR903 (RSP3) and caused port-channel flap
CSCwj06370	Serial cease traffic when configuring module other port
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 the mode sonet is configured.
CSCwh30217	With rate of OC-12, threshold sf-ber 3 is added under the **show running config** command.
CSCwf77316	ASR900/RSP3: MPLS incorrect label programmed with scenarios of double implicit-null.
CSCwf85278	mVPN profile 14 is failing with dual home scenarios.
CSCwh62909	ASR903: entitySensorMIB: Clear traps aren't seen when Major and Minor alarms are reported.

Identifier	Headline
CSCwh06519	Fan failure alarm doesn’t display the correct module name or description.
CSCwh28391	The show running config and write memory trigger the **ERR:Interfacenotfound** error messages.
CSCwh87343	Cisco IOS XE Software Web UI Privilege Escalation Vulnerability.
CSCwh04884	ASR903:17.6.3: VC Down due to control-word negotiation.
CSCwf79476	When certificate issues the **show platform sudi certificate sign nonce xxxx"**, flaps L3 interfaces.
CSCwh75169	ISIS: Redistribution prefix threshold has been reached and seen with lesser prefixes.
CSCwf16577	BFD session down alarm not clearing after fault is recovered.

Open Caveats - Cisco IOS XE Dublin 17.12.2a

Identifier	Headline
CSCwh80239	ASR900 RSP3 IP SLA multicast configuration not working.
CSCwf92194	Stale MAC address entries under the show mac address table.
CSCwh15292	Traffic fails with SPF: GLC-GE-DR-LX on router IM configured with 100 mbps speed.
CSCwh42209	RSS memory increment continuously seen in uea_mgr process upon system event.
CSCwh06611	Y1564 ext packets generated by probe is of size 69 B instead of 64 B when running SAT ext IR 7619 mbps.
CSCwh85621	ASR 903 - Layer 2 CEF interface is unavailable.
CSCuv05226	VRF is not deleted after replacing default config.
CSCwh66210	Netconf RPC failed to apply if increase mpls MTU limit to 9644 bytes.
CSCwh84408	Process pubd is not running in RSP2 device.
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
CSCwd85267	FR Port mode in **show interface** CLI does not display FR PW statistics.

Identifier	Headline
CSCwd87661	Fan running at high speed and creating noise (Fan PID A903-FAN-H) - SW version 17.03.04.
CSCwf18367	RSP3: uea_mgr RIFID leak/comsumption for Muticast routes.
CSCwe58324	Node Reload observed after routing change in core.
CSCwd66728	ASR903-RSP-3C - uea_mgr crash seen with uea_brcm_update_hw_stats.
CSCvy81362	Controllers are down due to LP-LOP alarm After CE reboots.
CSCwe19162	ASR903:RSP3: After SSO: False Alarm on CNAAP.
CSCwf14167	RSP3: uea_mgr memory leak on ARP probes.
CSCwd25376	Loopback local on 3GMS IM causing BIP B2 counters increment under show controller cli.
CSCwd86980	High traffic drop is observed on RPFO
CSCwf67803	DS3_ADMIN_DOWN gets cleared after IM OIR and displaying LINK_DOWN alarm in 3GMS.
CSCwf54249	With CPG, STS1e configuration is giving %ERROR: Standby doesn't support this command.
CSCwe34672	High CPU on ptp_uea process.
CSCwf37941	ACL config under serial interface makes dut crash during unconfig.
CSCwf40403	T3: DCR: cem id not displayed correctly under **sh recovered-clock**.
CSCwf42164	No snmp trap link-status get re-added after IM reload.
CSCwe38959	The rs232 ASYNC PW service with full scale seeing packet and byte drops intermittently.
CSCwd88680	High Convergence after Port channel member Failure.
CSCwf49426	PAIS alarm get reported after IM OIR.
CSCwf54221	With T3 ctrl shut, if mode T3 is unconfigured, forced Tx/Rx alarm in arrive is set to AIS.
CSCwe10460	Power sensor threshold warning alarms in EPNM.
CSCwe13024	ASR900-RSP2: All readings for Power supply unit reflect as zero though the unit is functional.
CSCwd67723	In IMA32D/IMA8D card, sometimes change in E1 controller config(after ctrlr flap) results in IM reboot.
CSCwe98227	The **show version** does not display details of T1/E1 interfaces for 8D and 32D IMs.

Identifier	Headline
CSCwe55191	IS-IS 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	ASR903/RSP2 UDP pseudowire stuck while activating.
CSCwe36122	IS-IS down when performing TI-LFA calculation.
CSCwe27155	Traffic drops with BDI shut (IP_FRR configs).

Open Caveats - Cisco IOS XE Dublin 17.12.1

Identifier	Headline
CSCwf77276	ASR903: memory leak seen on chunk module when BDI routed network traffic flow along with mac move.
CSCwf77316	MPLS L3VPN PE not able to connect remote CE.
CSCwf15278	Pending objects for "fman_fp_image: bd-efp-bind: bd X" during BDI interface creation.
CSCwf69937	The port channel does not come up on adding recommended configs until the router is reloaded.
CSCwf71463	During traffic flow, when speed lowered on ASYNC port, SYNC port CEM traffic gets impacted.
CSCwf18420	LLDP does not announce dynamically assigned VLAN.
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