



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 Bengaluru 17.4.2, on page 1](#)
- [Resolved Caveats – Cisco IOS XE Bengaluru 17.4.2 - Platform Independent, on page 2](#)
- [Open Caveats – Cisco IOS XE Bengaluru 17.4.2, on page 2](#)
- [Resolved Caveats – Cisco IOS XE Bengaluru 17.4.1, on page 2](#)
- [Open Caveats – Cisco IOS XE Bengaluru 17.4.1, on page 4](#)
- [Cisco Bug Search Tool, on page 4](#)

Resolved Caveats – Cisco IOS XE Bengaluru 17.4.2

Caveat ID Number	Description
CSCvu99207	Router: Incorrect STP forwarding state programming in platform.
CSCvw82303	Support for multicast route leaking in native multicast
CSCvw85511	BDI interface is causing high cpu usage.
CSCvw93411	Interface counters not incrementing after 2yrs, 22+ weeks on ASR920-24SZ-M variant
CSCvx01642	PPPoE tag circuit-id remote-id should not be trusted if the interface is in untrusted mode
CSCvx24923	HS1 2.43 FPGA commit for reload/brom select issue

Caveat ID Number	Description
CSCVx41010	Failed to marshal xcvr_sync message: Bad address
CSCVx55831	Ingress Policy with set qos-group action is creating extra TCAM entry with match on Egress Policy
CSCVx99501	Wrong snmp traps are generated for high voltage threshold violations
CSCVr43362	ASR-920-12SZ-IM, ASR-920-12SZ-A/ASR-920-12SZ-D: Fan speed control measures for overheating router

Resolved Caveats – Cisco IOS XE Bengaluru 17.4.2 - Platform Independent

Caveat ID Number	Description
CSCVv79677	Router crashed after BGP flaps
CSCVx19209	ISIS crash in isis_sr_tilfa_compute_protection
CSCVx26650	On configuring route tag under ISIS, TI-IFA is not forming repair path

Open Caveats – Cisco IOS XE Bengaluru 17.4.2

There are no open caveats for this release.

Resolved Caveats – Cisco IOS XE Bengaluru 17.4.1

Caveat ID Number	Description
CSCVk22965	Bulk License "Out of Compliance" support
CSCVs34482	ISSU is not working on Cisco ASR 900 RSP2 nodes
CSCVt33153	Traceback is seen with the following message: mroute_stats_update
CSCVt69921	RSP2-128: CMAND core during SSO
CSCVt75327	v1731: Traffic is not seen after performing SSO in Imsg_Mix mode
CSCVt76674	ASR920 : Last reload reason should refelect Rommon_upgrade
CSCVt76777	Adj err obj is seen on removing sr-label-preferred
CSCVt92428	RSP2-128: Step by Step ISSU CMD is not working

Caveat ID Number	Description
CSCvt93010	Traffic drop is seen after Kernel log messages are seen while shut or no shut on Phy/BDI interfaces
CSCvu06547	Require varbind entSensorseverity along with trap entSensorThresholdNotification
CSCvu13886	v174: Card protection performs shut or no shut on the CPG STS-1e, SLOS alarm is observed on the peer device
CSCvu29991	Historic performance intervals are not present for STS-1e interfaces in the command and SNMP MIB
CSCvu38550	For VCOP configured with type DS3, applique type should be Subrate T3 instead of Channelized T3/T1
CSCvu45833	ISSU: 1612-173: CEM Ckt is stuck at Setup Failed
CSCvu47732	Cisco ASR-920-12SZ-A and Cisco ASR-920-12SZ-D and Cisco ASR-920-20SZ-M: Bundle 1.40 FPGA and support for macronix SPI flash
CSCvu49097	Ports on ASR920-12SZ-D do not come up when 1G SFPs are used
CSCvu51472	Support for SAToP payload 64 byte and dejitter 2 ms in LOTR IMs
CSCvu59602	17.3.1-with transform-set esp-aes complete traffic drop seen after doing "clear crypto session"
CSCvu66126	OC-192 APS group is stuck with signal Fail condition
CSCvu78801	PPPoE VSA tags get overwritten at each PPPoE IA
CSCvu83291	ASR 920 cylon_mgr memory leak is observed due to QoS policer
CSCvu89908	Crash is observed while doing clear crypto session soak run
CSCvu95940	Egress QoS policy configuration is missing on PoCh member link flap
CSCvu92363	SSD: harddisk is full but received %PLATFORM-1-NOSPACE: bootflash : no space alarm assert
CSCvu97954	MAC flaps are observed when using VPLS over backup pseudowire configuration
CSCvu97978	XE BIT : Cisco ASR 900 RSP2 node is crashed with core generation in 16.12 throttle
CSCvv01146	ASR920: Secure bootflash from removal
CSCvv16454	Traffic failure occurs due to MPLS ECMP load-balancing in one of the labelled path
CSCvv24059	RSP2-128 mgr crash is noticed on Cisco ASR 900 RSP when EMPLSINTD is exhausted
CSCvv31617	e2e circuit does not ping, serial interface is up and line protocol is up
CSCvr43362	ASR-920-12SZ-IM, ASR-920-12SZ-A/ASR-920-12SZ-D: Fan speed control measures for overheating router

Open Caveats – Cisco IOS XE Bengaluru 17.4.1

Caveat ID Number	Description
CSCvv87440	Clock class 6 is advertised immediately on T-GM connection restore
CSCvv72192	When IMA2Z IM, XFP and SFP+ are present and then XFP is removed, LED still shows as green
CSCvw34109	PTP RX failure is observed due to LSMPI buffer exhaustion

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>