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.

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

Open Caveats – Cisco IOS XE Fuji 16.7.2

Caveat ID Number	Description
CSCve00923	SR_OSPF: High conv observed with LDP labeled in primary path and unlabeled/imp null backup path.

Caveat ID Number	Description
CSCvi41441	ASR920 monitor session configuration without destination interface blocks ISIS on source interface.

Resolved Caveats – Cisco IOS XE Fuji 16.7.2

Caveat ID Number	Description
CSCvh55399	T1 service latency is asymmetric in a simple linear topology.
CSCvf46252	ASR920 crash in cylon_mgr when MPLS TE interface shut down.
CSCvf80724	ASR920 VPLS A-S PW: Complete traffic drop (imp and disp) over VPLS Act PW.
CSCvf99074	ASR-920-10SZ-PD: Ping loss on built-in Te 0/0/10 or 0/0/11 port and CRC or MAC errors at peer end.
CSCvg21893	Unexpected traffic sent out from ASR920 access port from REP ring.
CSCvg70173	ASR920: Not able to configure xconnect untagged service instance with EVPN under the same interface.
CSCvg79798	ZTP reset as last reload reason in IOS when ZTP button pressed greater than 8 seconds.
CSCvh03346	Fan speed display in IOS not matching the actual written value and read value.
CSCvh41777	Removal of the policy from the service instance under a tengig interface causes traffic loss
CSCvi06424	Traffic fails after moving or relearning mac-address from EFP to Xconnect interface.
CSCvg36200	IPv4 deny ACL applied in the BDI is blocking L2 switched traffic under certain conditions.
CSCvg53877	Egress QOS fails when speed is changed at interface through nego auto, speed CLI command.
CSCvg85163	ZTP not triggered with gratuitous ARP.
CSCvg21899	Traffic forwarding not happening for VLANs added through **encap dot1q add** command in TEFP.
CSCvg86559	ASR920: Cylon_Mgr resources leaked on multiple occurrences of primary core BFD session flaps
CSCvh03346	Fan speed display in IOS not matching the actual written value and read value.
CSCvh22799	ASR-920-12SZ-IM: Ports 4 to7 no traffic flow on TDM IM removal and inserting Gigabit Ethernet IM.
CSCvh86486	ASR-920-12SZ-IM: CIsco ASR 920 routers issue with sfp-h10gb-cu1m cabling.

Caveat ID Number	Description
CSCvi44683	ASR920 REP: Not able to achieve less than 50 ms convergence.
CSCvc27630	Tx packets or Tx bytes generated is always lesser than configured rate-steps.

Open Caveats – Cisco IOS XE Fuji 16.7.1

Caveat ID Number	Description
CSCvf97552	dualrate_eem_policy does not succeed during port mode change which causes BDI Ping failure
CSCvg08224	G8265.1: PTP flaps between Holdover and Locked with 64/64 packet rate and HOTSTANDBY
CSCvg21899	Traffic forwarding not happening for VLANs added via **encap dot1q add** command in TEFP
CSCvg26930	Ten Gig interface going into admin down state after one gig shut down
CSCvg42314	ASR920: Random BFD Flap seen on ASR920

Resolved Caveats – Cisco IOS XE Fuji 16.7.1

Caveat ID Number	Description
CSCvd75495	Wrong marking for locally generated packet of BFD,LDP, and BGP
CSCvf10783	Cisco IOS XE Software for Cisco ASR 920 Series Routers Arbitrary File Overwrite Vulnerability
CSCvf68605	DHCP Snooping Database restore/renew failing on all ASR903/ASR920 variants