



## 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 17.12.5, on page 1](#)
- [Open Caveats – Cisco IOS XE Dublin 17.12.5, on page 2](#)
- [Resolved Caveats – Cisco IOS XE Dublin 17.12.4, on page 2](#)
- [Open Caveats – Cisco IOS XE Dublin 17.12.4, on page 2](#)
- [Resolved Caveats – Cisco IOS XE Dublin 17.12.3, on page 2](#)
- [Open Caveats – Cisco IOS XE Dublin 17.12.3, on page 2](#)
- [Resolved Caveats – Cisco IOS XE Dublin 17.12.2a, on page 2](#)
- [Open Caveats – Cisco IOS XE Dublin 17.12.2a, on page 3](#)
- [Resolved Caveats – Cisco IOS XE Dublin 17.12.1, on page 3](#)
- [Open Caveats – Cisco IOS XE Dublin 17.12.1, on page 3](#)
- [Cisco Bug Search Tool, on page 3](#)

## Resolved Caveats – Cisco IOS XE Dublin 17.12.5

Identifier	Headline
<a href="#">CSCwm47277</a>	NETCONF storm-control level configuration is not working.

## Open Caveats – Cisco IOS XE Dublin 17.12.5

Identifier	Headline
<a href="#">CSCwn62733</a>	Netconf is not accesible on NCS520.

## Resolved Caveats – Cisco IOS XE Dublin 17.12.4

Identifier	Headline
<a href="#">CSCwj65571</a>	Memory Leak on 'Chunk Manager' process.
<a href="#">CSCwj83811</a>	AAA server marked as Down after multiple no commands.
<a href="#">CSCwj10767</a>	Y.1731 PDUs with higher MD level are forwarded by MEP.

## Open Caveats – Cisco IOS XE Dublin 17.12.4

There are no open caveats for the Cisco IOS XE Dublin 17.12.4 release.

## Resolved Caveats – Cisco IOS XE Dublin 17.12.3

Identifier	Headline
<a href="#">CSCwh66880</a>	Netconf packet punted to CPU when service policy attached to port-channel interface

## Open Caveats – Cisco IOS XE Dublin 17.12.3

Identifier	Headline
<a href="#">CSCwj10767</a>	Y.1731 AIS PDUs with higher MD level are forwarded by UP MEP in UP-&gt;DOWN direction

## Resolved Caveats – Cisco IOS XE Dublin 17.12.2a

Identifier	Headline
<a href="#">CSCwh51947</a>	Unwanted messages pops up on router with BDI interface configuration
<a href="#">CSCwh87343</a>	Cisco IOS XE Software Web UI Privilege Escalation Vulnerability

Identifier	Headline
<a href="#">CSCwf79476</a>	ASR920:when certificate issue "show platform sudi certificate sign nonce xxxx", Flaps L3 interfaces
<a href="#">CSCwh75169</a>	ISIS: Redistribution prefix threshold has been reached seen with lesser prefixes
<a href="#">CSCwf16577</a>	BFD session down alarm not clearing after fault is recovered.

## Open Caveats – Cisco IOS XE Dublin 17.12.2a

Identifier	Headline
<a href="#">CSCuv05226</a>	VRF is not deleted after replacing default configuration.
<a href="#">CSCwh84408</a>	Process pubd is not running on RSP2.
<a href="#">CSCwh68394</a>	Unable to remove the service instance under interface.
<a href="#">CSCwh89032</a>	Remove vulnerability in open port.

## Resolved Caveats – Cisco IOS XE Dublin 17.12.1

Identifier	Headline
<a href="#">CSCwf67274</a>	IPv6 support under global routing table in version 17.11.1.a
<a href="#">CSCwe53050</a>	Misreporting Output Drops as Errors in Interface counters
<a href="#">CSCwe36071</a>	17.12.1 NCS520: Parser failure in CLI "show crypto entropy status"

## Open Caveats – Cisco IOS XE Dublin 17.12.1

Identifier	Headline
<a href="#">CSCwf18420</a>	LLDP does not announce dynamically assigned VLAN
<a href="#">CSCwf68400</a>	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>