

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 17.11.1a, on page 1
- Open Caveats – Cisco IOS XE Dublin 17.11.1, on page 1
- Cisco Bug Search Tool, on page 2

Resolved Caveats – Cisco IOS XE Dublin 17.11.1a

Identifier	Headline
CSCwc56918	NCS520: IPv6 host functionality config fails after upgrade to latest image
CSCwe07340	Static route not programmed in CEF when more than six static routes use the same next hop ip address
CSCwb68238	CSPN SSH requirement

Open Caveats – Cisco IOS XE Dublin 17.11.1

Identifier	Headline
CSCwe53050	Misreporting Output Drops as Errors in Interface counters

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