Caveats

Bug Search Tool

The system grades known problems (bugs) per severity level. These release notes contain descriptions of the following bug levels:

- All severity level 1 or 2 bugs

- Significant severity level 3 bugs

- All customer-found bugs

You can search for open and resolved caveats of any severity for any release using the Cisco Bug Search tool, an online tool available for customers to query defects according to their own needs.

To access the Cisco Bug Search tool, you need the following items:

- Internet connection

- Web browser

- Cisco.com user ID and password

Follow these steps to use Cisco Bug Search tool:

1. Access the Cisco Bug Search tool: https://tools.cisco.com/bugsearch/.

2. Log in with your Cisco.com user ID and password.

3. If you are looking for information about a specific problem, enter the bug ID number in the **Search for:** field and click **Go**.

Tip Click **Help** on the Bug Search page for information about how to search for bugs, create saved searches, and create bug groups.

Resolved Caveats

You can find the latest resolved caveat information for Cisco Prime License Manager by using the Bug Search tool, an online tool available for customers to query defects according to their own needs.

Tip You need an account with Cisco.com to use the Bug Search tool to find open and resolved caveats of any severity for any release.

See https://tools.cisco.com/bugsearch/.

Table 1: Resolved Caveats for Cisco Prime License Manager

Identifier	Headline
CSCvp37218	CUCM: Address April 2019 Oracle JDK Critical Patch Vulnerabilities (OpenJDK Upgrade to 1.7.0.221)
CSCvq01924	Multiple Vulnerabilities in tomcat (Tomcat Upgrade to 7.0.94)
CSCvn42153	CiscoSSL update to 6.1.479 / 6.2.323
CSCvo90929	Multiple Vulnerabilities in libssh2
CSCvo46223	Python X509 Certificate NULL Pointer Dereference Denial of Service V ...

Open Caveats

There are no known issues in this release.