



## Information about Caveats

---

Caveats describe unexpected behavior. Severity 1 caveats are the most serious caveats. Severity 2 caveats are less serious. Severity 3 caveats are moderate caveats. This chapter includes severity 1, severity 2, and selected severity 3 caveats.



**Note**

---

For information about the caveats pertaining to releases earlier than Release 3.6S, see [Cisco IOS XE 3S Release Notes](#).

---

We recommend that you view the field notices for the current release to determine whether your software or hardware platforms are affected. You can access the field notices from the following location:

[http://www.cisco.com/en/US/support/tsd\\_products\\_field\\_notice\\_summary.html](http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html)



**Note**

---

If you have an account on cisco.com, you can also use the Bug Search Tool to find select caveats of any severity. To reach the Bug Search Tool, log in to cisco.com and go to <https://tools.cisco.com/bugsearch/product?name=Cisco+ASR+1013+Router#search> (If the defect that you have requested is not displayed, it may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.) For details on how to use the Cisco Bug Search Tool, see “Using the Cisco Bug Search Tool” section on page 173.

---

The *Dictionary of Internetworking Terms and Acronyms* contains definitions of acronyms that are not defined in this document:

[http://docwiki.cisco.com/wiki/Category:Internetworking\\_Terms\\_and\\_Acronyms\\_\(ITA\)](http://docwiki.cisco.com/wiki/Category:Internetworking_Terms_and_Acronyms_(ITA))

## Using the Cisco Bug Search Tool

For more information about how to use the [Cisco Bug Search Tool](#), including how to set email alerts for bugs and to save bugs and searches, see [Bug Search Tool Help & FAQ](#).



**Before You Begin****Note**

You must have a Cisco.com account to log in and access the [Cisco Bug Search Tool](#). If you do not have one, you can register for an account.

- Step 1** In your browser, navigate to the [Cisco Bug Search Tool](#).
- Step 2** If you are redirected to a Log In page, enter your registered Cisco.com username and password and then, click Log In.
- Step 3** To search for a specific bug, enter the bug ID in the Search For field and press Enter.
- Step 4** To search for bugs related to a specific software release, do the following:
- In the Product field, choose Series/Model from the drop-down list and then enter the product name in the text field. If you begin to type the product name, the [Cisco Bug Search Tool](#) provides you with a drop-down list of the top ten matches. If you do not see this product listed, continue typing to narrow the search results.
  - In the Releases field, enter the release for which you want to see bugs.
- The [Cisco Bug Search Tool](#) displays a preview of the results of your search below your search criteria.
- Step 5** To see more content about a specific bug, you can do the following:
- Mouse over a bug in the preview to display a pop-up with more information about that bug.
  - Click on the hyperlinked bug headline to open a page with the detailed bug information.
- Step 6** To restrict the results of a search, choose from one or more of the following filters:

| Filter        | Description  |
|---------------|--|
| Modified Date | A predefined date range, such as last week or last six months.   |
| Status        | A specific type of bug, such as open or fixed.   |
| Severity      | The bug severity level as defined by Cisco. For definitions of the bug severity levels, see <a href="#">Bug Search Tool Help &amp; FAQ</a> . |
| Rating        | The rating assigned to the bug by users of the <a href="#">Cisco Bug Search Tool</a> .   |
| Support Cases | Whether a support case has been opened or not.   |

Your search results update when you choose a filter.

## Open and Resolved Bugs

The open and resolved bugs for this release are accessible through the [Cisco Bug Search Tool](#). This web-based tool provides you with access to the Cisco bug tracking system, which maintains information about bugs and vulnerabilities in this product and other Cisco hardware and software products. Within the [Cisco Bug Search Tool](#), each bug is given a unique identifier (ID) with a pattern of CSCxxNNNNN, where x is any letter (a-z) and N is any number (0-9). The bug IDs are frequently referenced in Cisco documentation, such as Security Advisories, Field Notices and other Cisco support documents. Technical Assistance Center (TAC) engineers or other Cisco staff can also provide you with the ID for a specific bug. The [Cisco Bug Search Tool](#) enables you to filter the bugs so that you only see those in which you are interested.

In addition to being able to search for a specific bug ID, or for all bugs in a product and release, you can filter the open and/or resolved bugs by one or more of the following criteria:

- Last modified date
- Status, such as fixed (resolved) or open
- Severity
- Support cases

You can save searches that you perform frequently. You can also bookmark the URL for a search and email the URL for those search results.

