



# Release Notes for Cisco IOS Release 15.6S

---

**First Published: November 27, 2015**  
**Last Updated: July 31, 2017**  
**Release: Cisco IOS Release 15.6(1)S4**  
**Part Number: OL-30834-08**

## Introduction

These release notes support Cisco IOS Release 15.6S up to and including Cisco IOS Release 15.6(1)S4 and are updated as needed to describe new features, bugs, and related documents. Cisco IOS Release 15.6S supports platforms within the following Cisco series:

- Cisco 7600 series routers
- Cisco ASR 901 router
- Cisco ASR 901 10G router
- Cisco ASR 901 S router
- Cisco ME 3600X switch
- Cisco ME 3600-24CX switch
- Cisco ME 3800X switch



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**



# System Requirements

This document describes the system requirements for Cisco IOS 15.6S releases and includes the following sections:

- [Feature Support, page 3](#)
- [Memory Recommendations, page 5](#)
- [Supported Hardware, page 5](#)
- [Determining the Software Version, page 6](#)
- [Upgrading to a New Software Release, page 6](#)

## Feature Support

Cisco IOS software is packaged in feature sets that consist of software images that support specific platforms. The feature sets available for a specific platform depend on which Cisco IOS software images are included in a release. Each feature set contains specific Cisco IOS features.



### Caution

Cisco IOS images with strong encryption (including, but not limited to 168-bit [3DES] data encryption feature sets) are subject to U.S. government export controls and have limited distribution. Strong encryption images to be installed outside the United States are likely to require an export license. Customer orders may be denied or subject to delay because of U.S. government regulations. When applicable, the purchaser/user must obtain local import and use authorizations for all encryption strengths. Please contact your sales representative or distributor for more information, or send an e-mail to [export@cisco.com](mailto:export@cisco.com).

Feature-to-image mapping is available through Cisco Feature Navigator. Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or by feature set (software image). You can compare Cisco IOS software releases side-by-side to display both the features unique to each software release and the features that the releases have in common.

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

[www.cisco.com/go/cfn](http://www.cisco.com/go/cfn)

For help with Cisco Feature Navigator, see the help information at the following URL:

[http://www.cisco.com/web/applicat/CFNTOOLS/Help\\_Docs/help/cfn\\_support.html](http://www.cisco.com/web/applicat/CFNTOOLS/Help_Docs/help/cfn_support.html)

## Determining the Software Images (Feature Sets) That Support a Specific Feature

To determine which software images (feature sets) in a Cisco IOS release support a specific feature, go to the [Cisco Feature Navigator home page](#) and perform the following steps.

- Step 1** From the Cisco Feature Navigator home page, click **Research Features**.
- Step 2** Select your software type or leave the field as “All”.

- Step 3** To find a feature, you can search by either Feature or Technology (select the appropriate button). If you select Search by Feature, you can further filter your search by using the Filter By text box.
- Step 4** Choose a feature from the Available Features text box, and click the **Add** button to add the feature to the Selected Features text box.




---

**Note** To learn more about a feature in the list, click the **View Desc** button in the Available Features text box.

---

Repeat this step to add features. A maximum of 20 features can be chosen for a single search.

- Step 5** Click **Continue** when you are finished choosing features.
- Step 6** In the Release/Platform Tree area, select either your release (from the Train-Release list) or your platform (from the Platform list).
- Step 7** The “Search Result” table will list all the software images (feature sets) that support the features that you chose.




---

**Note** You can download your results into an Excel spreadsheet by clicking on the Download Excel button.

---

## Determining the Features Supported in a Specific Software Image (Feature Set)

To determine which features are supported in a specific software image (feature set), go to the [Cisco Feature Navigator home page](#) and perform the following steps.

- Step 1** From the Cisco Feature Navigator home page, click **Research Software**.
- Step 2** Select your software type from the drop-down list and chose the **Release** button in the “Search By” area.
- Step 3** From the Major Release drop-down list, chose the appropriate major release.
- Step 4** From the Release drop-down list, choose the appropriate maintenance release.
- Step 5** From the Platform drop-down list, choose the appropriate hardware platform.
- Step 6** From the Feature Set drop-down list, choose the appropriate feature set. The Image Details area will provide details on the specific image. The Available Features area will list all the features that are supported by the feature set (software image) that you chose.




---

**Note** To learn more about a feature in the list, click the **View Desc** button in the Available Features text box.

---

## Memory Recommendations

To determine memory recommendations for software images (feature sets) in your Cisco IOS release, go to the [Cisco Feature Navigator home page](#) and perform the following steps.

- 
- Step 1** From the Cisco Feature Navigator home page, click **Research Software**.
  - Step 2** Select your software type from the drop-down list and choose the **Release** button in the “Search By” area.
  - Step 3** From the Major Release drop-down list, choose the appropriate major release.
  - Step 4** From the Release drop-down list, choose the appropriate maintenance release.
  - Step 5** From the Platform drop-down list, choose the appropriate hardware platform.
  - Step 6** From the Feature Set drop-down list, choose the appropriate feature set.
  - Step 7** The Image Details area will provide details on the specific image including the DRAM and flash memory recommendations for each image. The Available Features area will list all the features that are supported by the feature set (software image) that you chose.
- 

## Supported Hardware

Cisco IOS Release 15.5S supports the following platforms, including the following models and supervisor engines:

- Cisco 7600 series routers
- Cisco ASR 901 router
- Cisco ASR 901 10G router
- Cisco ME 3600X switch
- Cisco ME 3600X-24CX switch
- Cisco ME 3800X switch

### Cisco 7600 Series Routers

For extensive information about all supported hardware for Cisco 7600 series routers, see the *Guide to Supported Hardware for Cisco 7600 Series Routers with Cisco IOS Release 15S*:

[http://www.cisco.com/en/US/docs/routers/7600/Hardware/15\\_0s/7600\\_hwd.html](http://www.cisco.com/en/US/docs/routers/7600/Hardware/15_0s/7600_hwd.html)

### Cisco ASR 901 Router

For detailed information about the Cisco ASR 901 router, see the documents at the following location:

<http://www.cisco.com/c/en/us/support/routers/asr-901-series-aggregation-services-routers/tsd-products-support-series-home.html>

## Cisco ASR 901 10G Router

For detailed information about the Cisco ASR 901 10G router, see the documents at the following location:

<http://www.cisco.com/c/en/us/support/routers/asr-901-10g-series-aggregation-services-routers/tsd-products-support-series-home.html>

## Cisco ME 3600X Switch and ME 3800X Switch

For detailed information about the Cisco ME 3600X switch, see the documents at the following location:

<http://www.cisco.com/c/en/us/products/switches/me-3600x-series-ethernet-access-switches/index.html>

For detailed information about the Cisco ME 3800X switch, see the documents at the following location:

<http://www.cisco.com/c/en/us/products/switches/me-3800x-series-carrier-ethernet-switch-routers/index.html>

See the *Cisco ME 3800X and ME 3600X Switch Hardware Installation Guide* at

[http://www.cisco.com/en/US/docs/switches/metro/me3600x\\_3800x/hardware/installation/guide/me3800x\\_hig.html](http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/hardware/installation/guide/me3800x_hig.html)

## Cisco ME 3600X-24CX Switch

For detailed information about the Cisco ME 3600X-24CX switch, see the document at the following location:

[http://www.cisco.com/c/en/us/products/collateral/switches/me-3600x-series-ethernet-access-switches/data\\_sheet\\_c78-708663.html](http://www.cisco.com/c/en/us/products/collateral/switches/me-3600x-series-ethernet-access-switches/data_sheet_c78-708663.html)

## Determining the Software Version

To determine the version of Cisco IOS software that is running on your Cisco router, log in to the router and enter the **show version** EXEC command:

```
Router# show version
```

```
Cisco IOS Software, s72033_rp Software (s72033_rp-ADVENTERPRISEK9_WBX_WAN-M), Version 15.6(1)S, EARLY DEPLOYMENT RELEASE SOFTWARE
```

## Upgrading to a New Software Release

For information about choosing a new Cisco IOS software release, see *How to Choose a Cisco IOS Software Release* at the following location:

[http://www.cisco.com/en/US/products/sw/iosswrel/ps1834/products\\_tech\\_note09186a00800fb9d9.shtml](http://www.cisco.com/en/US/products/sw/iosswrel/ps1834/products_tech_note09186a00800fb9d9.shtml)

For information about upgrading the Cisco 7600 series routers, go to the following location:

<http://www.cisco.com/c/en/us/support/routers/7600-series-routers/tsd-products-support-install-and-upgrade.html>

For information about upgrading the Cisco ASR 901 router, go to the following location:

<http://www.cisco.com/c/en/us/support/routers/asr-901-series-aggregation-services-routers/products-installation-guides-list.html>

For information about upgrading the Cisco ME 3600X switch, go to the following location:

<http://www.cisco.com/c/en/us/support/switches/me-3600x-series-ethernet-access-switches/tsd-products-support-install-and-upgrade.html>

For information about upgrading the Cisco ME 3600X-24CX switch, go to the following location:

<http://www.cisco.com/c/en/us/support/switches/me-3600x-series-ethernet-access-switches/products-installation-guides-list.html>

For information about upgrading the Cisco ME 3800X switch, go to the following location:

<http://www.cisco.com/c/en/us/support/switches/me-3800x-series-carrier-ethernet-switch-routers/tsd-products-support-install-and-upgrade.html>

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.





# Limitations and Restrictions

This chapter describes limitations and restrictions in Cisco IOS 15.6S releases.

- [Limitations and Restrictions in Cisco IOS Release 15.6S, page 9](#)

## Limitations and Restrictions in Cisco IOS Release 15.6S

There are no new limitations and restrictions in Cisco IOS Release 15.6(1)S.





## **New Features and Important Notes**



## Features and Important Notes for Cisco IOS Release 15.6(2)S

These release notes describe the following topics:

- [New Hardware Features in Cisco IOS Release 15.6\(2\)S](#), page 13
- [New Software Features in Cisco IOS Release 15.6\(2\)S](#), page 13
- [New Hardware and Software Features supported on Cisco 7600 Series Routers in Cisco IOS Release 15.6\(2\)S](#), page 13
- [New Hardware and Software Features supported on Cisco ASR 901 Series Routers in Cisco IOS Release 15.6\(2\)S](#), page 13
- [New Hardware and Software Features supported on Cisco ASR 901 S Series Routers in Cisco IOS Release 15.6\(2\)S](#), page 13
- [New Hardware and Software Features supported on Cisco ME 3600x Ethernet Access Switches in Cisco IOS Release 15.6\(2\)S](#), page 14
- [MIBs](#), page 14
- [Important Notes](#), page 14

### New Hardware Features in Cisco IOS Release 15.6(2)S

There are no new hardware features in Cisco IOS Release 15.6(2)S.

### New Software Features in Cisco IOS Release 15.6(2)S

There are no new software features in Cisco IOS Release 15.6(2)S.

### New Hardware and Software Features supported on Cisco 7600 Series Routers in Cisco IOS Release 15.6(2)S

For detailed information about hardware and software features supported on Cisco 7600 Series Routers in Cisco IOS Release 15.6(2)S, see the following document:

<http://www.cisco.com/c/en/us/support/routers/7600-series-routers/products-release-notes-list.html>

### New Hardware and Software Features supported on Cisco ASR 901 Series Routers in Cisco IOS Release 15.6(2)S

For detailed information about hardware and software features supported on Cisco ASR 901 Series Routers in Cisco IOS Release 15.6(2)S, see the following document:

<http://www.cisco.com/c/en/us/support/routers/asr-901-series-aggregation-services-routers/products-release-notes-list.html>

### New Hardware and Software Features supported on Cisco ASR 901 S Series Routers in Cisco IOS Release 15.6(2)S

For detailed information about hardware and software features supported on Cisco ASR 901 S Series Routers in Cisco IOS Release 15.6(2)S, see the following document:

<http://www.cisco.com/c/en/us/support/routers/asr-901s-series-aggregation-services-routers/products-release-notes-list.html>

## New Hardware and Software Features supported on Cisco ME 3600x Ethernet Access Switches in Cisco IOS Release 15.6(2)S

For detailed information about hardware and software features supported on Cisco ME 3600x Ethernet Switches in Cisco IOS Release 15.6(2)S, see the following document:

<http://www.cisco.com/c/en/us/support/switches/me-3600x-series-ethernet-access-switches/products-release-notes-list.html>

## MIBs

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use the Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If the Cisco MIB Locator does not support the MIB information that you need, you can obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access the Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank email to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your email address is registered with Cisco.com. If the check is successful, account details with a new random password will be emailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://tools.cisco.com/RPF/register/register.do>

## Important Notes

The following sections contain important notes about Cisco IOS Release 15.6S:

- [Field Notices and Bulletins, page 14](#)

### Field Notices and Bulletins

- Field Notices—Cisco recommends that you view the field notices for this release to see if your software or hardware platforms are affected. You can find field notices at [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).
- Bulletins—You can find bulletins at [http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/prod\\_literature.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/prod_literature.html).

## Features and Important Notes for Cisco IOS Release 15.6(1)S

These release notes describe the following topics:

- [New Hardware Features in Cisco IOS Release 15.6\(1\)S, page 15](#)
- [New Software Features in Cisco IOS Release 15.6\(1\)S, page 15](#)
- [New Hardware and Software Features supported on Cisco 7600 Series Routers in Cisco IOS Release 15.6\(1\)S, page 15](#)
- [New Hardware and Software Features supported on Cisco ASR 901 Series Routers in Cisco IOS Release 15.6\(1\)S, page 15](#)
- [New Hardware and Software Features supported on Cisco ASR 901 S Series Routers in Cisco IOS Release 15.6\(1\)S, page 16](#)
- [New Hardware and Software Features supported on Cisco ME 3600x Ethernet Access Switches in Cisco IOS Release 15.6\(1\)S, page 16](#)
- [MIBs, page 16](#)
- [Important Notes, page 16](#)

### New Hardware Features in Cisco IOS Release 15.6(1)S

There are no new hardware features in Cisco IOS Release 15.6(1)S.

### New Software Features in Cisco IOS Release 15.6(1)S

#### IOS-XE IBGP local-as dual-as

For detailed information about this feature, see the following document:

[http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute\\_bgp/configuration/15-s/irg-15-s-book/bgp-supp-local-as-dual-as.html](http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/configuration/15-s/irg-15-s-book/bgp-supp-local-as-dual-as.html)

### New Hardware and Software Features supported on Cisco 7600 Series Routers in Cisco IOS Release 15.6(1)S

For detailed information about hardware and software features supported on Cisco 7600 Series Routers in Cisco IOS Release 15.6(1)S, see the following document:

<http://www.cisco.com/c/en/us/support/routers/7600-series-routers/products-release-notes-list.html>

### New Hardware and Software Features supported on Cisco ASR 901 Series Routers in Cisco IOS Release 15.6(1)S

For detailed information about hardware and software features supported on Cisco ASR 901 Series Routers in Cisco IOS Release 15.6(1)S, see the following document:

<http://www.cisco.com/c/en/us/support/routers/asr-901-series-aggregation-services-routers/products-release-notes-list.html>

## New Hardware and Software Features supported on Cisco ASR 901 S Series Routers in Cisco IOS Release 15.6(1)S

For detailed information about hardware and software features supported on Cisco ASR 901 S Series Routers in Cisco IOS Release 15.6(1)S, see the following document:

<http://www.cisco.com/c/en/us/support/routers/asr-901s-series-aggregation-services-routers/products-release-notes-list.html>

## New Hardware and Software Features supported on Cisco ME 3600x Ethernet Access Switches in Cisco IOS Release 15.6(1)S

For detailed information about hardware and software features supported on Cisco ME 3600x Ethernet Switches in Cisco IOS Release 15.6(1)S, see the following document:

<http://www.cisco.com/c/en/us/support/switches/me-3600x-series-ethernet-access-switches/products-release-notes-list.html>

## MIBs

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use the Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If the Cisco MIB Locator does not support the MIB information that you need, you can obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access the Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank email to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your email address is registered with Cisco.com. If the check is successful, account details with a new random password will be emailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://tools.cisco.com/RPF/register/register.do>

## Important Notes

The following sections contain important notes about Cisco IOS Release 15.6S:

- [Field Notices and Bulletins, page 16](#)

## Field Notices and Bulletins

- **Field Notices**—Cisco recommends that you view the field notices for this release to see if your software or hardware platforms are affected. You can find field notices at [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).
- **Bulletins**—You can find bulletins at [http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/prod\\_literature.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/prod_literature.html).





## Bugs



# Bugs for Cisco IOS Release 15.6(2)S

## Resolved Bugs

Bugs describe unexpected behavior in Cisco IOS software releases. Severity 1 bugs are the most serious bugs; severity 2 bugs are less serious. Severity 3 bugs are moderate bugs, and only select severity 3 bugs are included in this section.

In this section, the following information is provided for each bug:

- Symptoms—A description of what is observed when the bug occurs.
- Conditions—The conditions under which the bug has been known to occur.
- Workaround—Solutions, if available, to counteract the bug.

**Note**

If you have an account on Cisco.com, you can also use the Bug Toolkit to find select bugs of any severity. To reach the Bug Toolkit, log in to [Cisco.com](http://www.cisco.com) and go to [http://www.cisco.com/cgi-bin/Support/Bugtool/launch\\_bugtool.pl](http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl). (If the defect that you have requested cannot be displayed, this 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.)

This section consists of the following subsections:

- [Using the Bug Search Tool](#), page 19
- [Open Bugs—Cisco IOS Release 15.6\(2\)S](#), page 20
- [Resolved Bugs—Cisco IOS Release 15.6\(2\)S](#), page 21

## Using the Bug Search Tool

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

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](#).

**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](#).

To use the Cisco Bug Search Tool:

1. In your browser, navigate to the [Cisco Bug Search Tool](#).

2. If you are redirected to a **Log In** page, enter your registered Cisco.com username and password and then, click **Log In**.
3. To search for a specific bug, enter the bug ID in the **Search For** field and press Enter.
4. To search for bugs related to a specific software release, do the following:
  - a. 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.
  - b. 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. You can mouse over bugs to see more content about a specific bug.

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.
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 Cisco Bug Search Tool.
Support Cases	Whether a support case has been opened or not.

Your search results update when you choose a filter.

All resolved bugs for a release are available in the [Cisco Bug Search Tool](#) through the [fixed bug search](#).

This search uses the following search criteria and filters:

Field Name	Information
Product	Series/Model Cisco IOS and NX-OS Software => Cisco IOS
Release	Example:15.6(1)S
Status	Fixed
Severity	2 or higher

## Open Bugs—Cisco IOS Release 15.6(2)S

This section lists the open bugs for Cisco IOS Release 15.6(1)S1. All the bugs have a link to the Bug Search Tool where you can find details of the specific bug. This section describes only severity 1, severity 2, and select severity 3 bugs.

**Table 1 Cisco IOS Release 15.6(2)S Open Bugs**

Identifier	Description
<a href="#">CSCuy17457</a>	Memory leak with changing single encapsulation to range in TEPF in RSP2
<a href="#">CSCux85117</a>	ASR920: Configured Isakmp policies doesnt populate as expected.
<a href="#">CSCuy55402</a>	CPU HOG and bdomain_inform_port_deletion_from_bd traceback after SSO
<a href="#">CSCuy44515</a>	l2vpn failed to set the PRC code under certain conditions
<a href="#">CSCux33019</a>	Router may crash when loopbacks of its LDP neighbours are flapped
<a href="#">CSCuy16780</a>	onep bypass until flow action is not woking with high traffic rate
<a href="#">CSCuy57683</a>	OSPF TILFA: multiple post converg path exists with TI LFA in some cases.
<a href="#">CSCuy32709</a>	R-LFA Tunnels not established on setting DS required attribute
<a href="#">CSCuy12969</a>	TILFA: False failure in Per-Destination-Q-Space-Check (loop free check)
<a href="#">CSCuy40541</a>	TILFA: tunnels not created when primary-path required tiebreak is in cfg
<a href="#">CSCuy07343</a>	AN : ipv6 global prefixes are seen in the cisco_autonomic vrf table
<a href="#">CSCux62496</a>	VMAN: Not able to copy the files or log to backup HA RSP2 bootflash

## Resolved Bugs—Cisco IOS Release 15.6(2)S

This section lists the resolved bugs for Cisco IOS Release 15.6(2)S. All the bugs have a link to the Bug Search Tool where you can find details of the specific bug. This section describes only severity 1, severity 2, and select severity 3 bugs.

**Table 2 Cisco IOS Release 15.6(2)S Resolved Bugs**

Identifier	Description
<a href="#">CSCux26195</a>	"aaa accounting suppress null-username" not working as expected
<a href="#">CSCuw37292</a>	ASR1k : 3.13.3 crashes due to segfault caused by aaa attributes
<a href="#">CSCuw38000</a>	Password complexity implementation does not match DISA requirements
<a href="#">CSCtj75471</a>	crash at port lookup from stp
<a href="#">CSCuw59193</a>	BRI link fails to come UP after OIR on NT + platform reload on User
<a href="#">CSCuv79776</a>	Router with Pfr feature crashed at cpp_free_exmem
<a href="#">CSCuv61799</a>	ASR1000 power supplies require SW debounce of PWR_OK signal
<a href="#">CSCuu99672</a>	False fan module missing alarm is raised
<a href="#">CSCuv87030</a>	Clock recovery fails on 1gige interfaces of ASR1000-2T+20X1GE
<a href="#">CSCuw47720</a>	ASR1001-X/ISR4k Mgmt port negotiation issue with peer device
<a href="#">CSCuv25529</a>	Remote MEPs 611/613/711/712 not found and unsuccessfull Traceroute
<a href="#">CSCuv84600</a>	Netflow packets are dropped when EPC is enabled
<a href="#">CSCuv83742</a>	ICFD errors in NP5c has to be accounted in show CLIs
<a href="#">CSCuu35042</a>	CSR1000v Slow VRRP Failover to a BDI interface
<a href="#">CSCut62449</a>	Disable HTTP AIC support
<a href="#">CSCuv91545</a>	ESP continuous crash on ASR1013 using 03.13.03.S.154-3.S3-ext.bin

Identifier	Description
<a href="#">CSCux50997</a>	IOS crashes on bootup without any startup configuration
<a href="#">CSCUw66262</a>	ASR1k: Memory Leak in cpp_cp_svr Process
<a href="#">CSCUv76019</a>	process mgr exiting: critical process fault, cpp_cp_svr, fp_0_0, rc=134
<a href="#">CSCUw12883</a>	IPSec dummy packet feature does not work in VRF-aware IPsec
<a href="#">CSCUw21897</a>	Traceback seen with ip cef accounting
<a href="#">CSCUv12943</a>	Add cli support to enable cepThroughputNotif trap
<a href="#">CSCUv52997</a>	/32 static route added without add-route enabled for outside dynamic nat
<a href="#">CSCUw39613</a>	ASR1K fails to perform NAT when flow cache entries are disabled.
<a href="#">CSCUs85112</a>	CGN, QFP: Show cmd display incorrect NAT trans stats for per-host IP add
<a href="#">CSCUw41346</a>	ESP packets discarded during re-key with static NAT on ASR1k
<a href="#">CSCUw95617</a>	QFP crash in NAT ALG after ipv4_nat_destroy_session
<a href="#">CSCUw70220</a>	IOSXE PACTRAC: cpp crash when packet trace enabled for MPLS and SSLVPN
<a href="#">CSCUv74763</a>	ASR 1K - SSH Hangs on "Show Logging Count" When SBC Errors Flood Console
<a href="#">CSCUp91567</a>	ASR1001-X boot-loops with CMCC crash and XGM MAC10 block errors
<a href="#">CSCUv60858</a>	SSL-GW doesn't listen to the new IP after SSL Port and IP addr change
<a href="#">CSCur33588</a>	ipv6 cef not working when using ipv6 neighbor
<a href="#">CSCux32083</a>	AN autoconfigured NTP server must support lower stratum
<a href="#">CSCux59168</a>	AN: autonomic [optional commands] are not available under interface mode
<a href="#">CSCux15053</a>	AN: Config server address not getting removed after withdrawing service
<a href="#">CSCUy42632</a>	AN: DIKE session is not getting READY after shut/no shut
<a href="#">CSCUw65651</a>	AN: Router crashes after defaulting interface with AN EFP
<a href="#">CSCUy08030</a>	AN: sh an int output prints Probing for AN disabled int
<a href="#">CSCux75878</a>	AN: UDI getting truncated in "show autonomic registrar devices accepted"
<a href="#">CSCUv87599</a>	Manually entered IKEv2 crypto profile not NVgen-ed with AN active
<a href="#">CSCUw51767</a>	FlexLSP: Show BFD Neighbors Output not stopping at term length
<a href="#">CSCUw66752</a>	"SSM connection manager" high CPU if VAIs under scale have QoS applied
<a href="#">CSCUu79021</a>	ASR1K: Aggr GEC QoS in Suspend state even after noshut the member link
<a href="#">CSCux70853</a>	ISR - 4400 crash
<a href="#">CSCUv66776</a>	MQC Policy-map counters do not update in T3/E3 SPA
<a href="#">CSCUu37662</a>	Unexpected Reboot during CoA Updates
<a href="#">CSCUu21113</a>	[MK21] : Crash seen on Terminator upon reload with FC4 image
<a href="#">CSCUy12658</a>	Unexpected behavior and errors related to downstream voice flows on cBR8
<a href="#">CSCUv96688</a>	Unexpected call-home msg truncate log
<a href="#">CSCUv99608</a>	uprev dev18 fixes to rel17
<a href="#">CSCUw61375</a>	CME software not updating xmit info and destination call id
<a href="#">CSCux82311</a>	Inconsistency result for mib docsIf3RxChStatusChIfIndex
<a href="#">CSCux57314</a>	Online CM marked CM offline in remote-query and not polled

Identifier	Description
<a href="#">CSCux89392</a>	remote-query polling interval through snmp didn't sync to standby PRE
<a href="#">CSCux18010</a>	Cisco Networking Services Sensitive Information Disclosure Vulnerability
<a href="#">CSCuw37313</a>	IPsec crash at UNIX-EXT-SIGNAL: Aborted(6), Process = NIST rng proc
<a href="#">CSCuv66659</a>	CSR1KV: csr1kv stops Responding to ARP Requests
<a href="#">CSCux90373</a>	CSR1000V: V156_1_S_XE317 core dumps
<a href="#">CSCuv86049</a>	isr4331 and isr4351 platforms crashed during GRE performance testing
<a href="#">CSCuu81130</a>	CSR1000v KVM SR-IOV IPv6 Unsuccessful Ping Traffic
<a href="#">CSCuv44308</a>	Crash Seen during OVA install when using ESXi6.0
<a href="#">CSCuw20432</a>	CSR interfaces shows up DHCP/TFTP for Static IP configuration
<a href="#">CSCuw18669</a>	VACS Activation not working in 3.16
<a href="#">CSCuw58071</a>	CSR XE317: CSR crashes during IPSEC session bring up
<a href="#">CSCuw33169</a>	CSR1000v: L2 133-136 bytes frame drop with ESP-null SHA384 and 512
<a href="#">CSCuw23857</a>	Crash at CWS TUN WL process while running DSA script
<a href="#">CSCuv75489</a>	CWS FPMAN_FP Crash when whitelisting is unconfigured.
<a href="#">CSCuw18990</a>	CWS needs to be route lookup based on the source interface VRF scope
<a href="#">CSCuu43112</a>	CWS OOB needs to be supported with VRF
<a href="#">CSCuv72847</a>	CWS redirect-list should not accept an extended access-list
<a href="#">CSCuw15123</a>	CWS tunnels needs to be deleted if FQDN fails during router reload
<a href="#">CSCuv72596</a>	CWS Whitelisting ACL failed to download on dataplane
<a href="#">CSCuw53464</a>	CWS: ISR crashed while modifying patterns under WL
<a href="#">CSCuw23345</a>	CWS: Parameter-map primary tower configuration issue
<a href="#">CSCuv74034</a>	Router reloads when the cws-tunnel is coming up
<a href="#">CSCux88022</a>	ASR1K : Crash at dhcp_sip_get_config
<a href="#">CSCux02200</a>	ASR1K seg fault crash on DHCP SIP process
<a href="#">CSCut95477</a>	client-identifier disappears from running configuration
<a href="#">CSCux33385</a>	DHCP binding deletes cash after getting unicast DHCP request
<a href="#">CSCus55821</a>	DHCPv6 process crashes when receiving malformed packet
<a href="#">CSCuv39338</a>	ISG: DHCP Server RADIUS Proxy Memory Leak
<a href="#">CSCuw73152</a>	Standby RP Silent reset
<a href="#">CSCuw99105</a>	DNS query is being sent with wrong interface IP instead of configured IP
<a href="#">CSCuw18886</a>	Crash while removing whitelist with 1K entries in DSA DB
<a href="#">CSCuv61150</a>	crash while removing whitelisting with 5k IP's in DSA DB
<a href="#">CSCuw90662</a>	MODEMPASS usage does not show up in show call active voice brief output
<a href="#">CSCuw67294</a>	4351 IOS MTP not relay T.30 messages
<a href="#">CSCux82241</a>	\$\$TS: EIGRP SAF sequence not same for site-prefix and discovered site
<a href="#">CSCux41072</a>	EIGRP sending hello messages with interface in passive mode.
<a href="#">CSCut37529</a>	Several traceback @ intr_stat_snapshot_and_process about ACFE

Identifier	Description
<a href="#">CSCux15835</a>	ISR4331/K9:Router fails to come online with No Service Password Recovery
<a href="#">CSCUw22338</a>	ISR4xxx may report the incorrect power supply type in show inventory.
<a href="#">CSCux91894</a>	ASR9xx iomd memory leak
<a href="#">CSCUw08174</a>	ISR 43XX/44XX Limits Crypto IPsec Window-Size to 512 for No Reason
<a href="#">CSCux20098</a>	erspan cannot support source port-channel,tunnel,multilink and serial.
<a href="#">CSCut79286</a>	ASR1K QoS feature doesn't work fine with RP2/RIs3.x
<a href="#">CSCux15954</a>	EEM : fatal condition error from operating system
<a href="#">CSCUw12720</a>	MallocLite memory leak due to EEM when using "file open" action.
<a href="#">CSCUw43115</a>	CSR1Kv XE 3.13.3S Crashed on clearing ip ospf process
<a href="#">CSCUw82081</a>	LISP CEF: fwd-native routes gleaned for LISP not forwarded natively
<a href="#">CSCUu26303</a>	Router crash triggered by service policy and ipv6 traffic
<a href="#">CSCUw05651</a>	EzPM causes STACKLOW message and a subsequent crash
<a href="#">CSCUv27265</a>	ENH: Enable support for TLSv1.1 & TLSv1.2 for http secure server/client
<a href="#">CSCUu66503</a>	HTTPS: IOS HTTPS client not enforcing subject-name verification
<a href="#">CSCUv36677</a>	IOS allows RC4-MD5 and RC4-SHA1 SSL ciphers to be negotiated by default
<a href="#">CSCut44432</a>	Chunk Manager Leak due to PROTO_COUNTER
<a href="#">CSCux38417</a>	IOS and IOS-XE IKEv2 Fragmentation DoS
<a href="#">CSCux69222</a>	Truncated counters/names in the 'show proc mem platform' output
<a href="#">CSCUu75193</a>	No shut on interface, deletes Rx SC of session on other live interface
<a href="#">CSCux80430</a>	Archive command broken when files removed by tracelogs rotation
<a href="#">CSCUu66331</a>	Battlestar:IPV6 Netflow on sub-bundle interfaces crashes both SUP's
<a href="#">CSCUv93130</a>	Cisco IOS-XE 3S platforms Series Root Shell License Bypass Vulnerability
<a href="#">CSCux14860</a>	ASR1K:Packet Tracing failed with FW,NAT&FW enabled.
<a href="#">CSCUw28179</a>	CWS Whitelist download fails if UTD is enabled on cws-tunnel out intf
<a href="#">CSCUp70353</a>	IOS-XE router reload due to WebUI log file leak
<a href="#">CSCUw49406</a>	"no ip routing protocol purge interface" delete with reload
<a href="#">CSCUu77403</a>	%LINK-4-TOOBIG Messages Seen on ISR 3945 with L2TPv3
<a href="#">CSCUw48118</a>	ASR920 - crash in bcopy called from 'addnew' during reassembly
<a href="#">CSCux46094</a>	Crash while using ip unnumbered with auto install--Zero touch deployment
<a href="#">CSCUw74179</a>	CSR: static route via VTI fails to restore after Interface shut/no shut
<a href="#">CSCux29974</a>	ISR4k:UnconfiguredIpv4Fia drop seen for pkts transit via PPPoE
<a href="#">CSCUv80943</a>	MCP_DEV:Packet drops@Ipv6NoRoute with ipv6gre configs
<a href="#">CSCUv99758</a>	Remove unnecessary packet debugs for UDP tunnels
<a href="#">CSCUw08398</a>	Tunnel Tracebacks observed when changing the PFR loopback address
<a href="#">CSCUq64416</a>	ASR-1004 Call Failures with TCP as Session Protocol towards CVP/CUCM
<a href="#">CSCUv79202</a>	CUBE Crashed while handling Response for Unsupported INFO Request
<a href="#">CSCUw63102</a>	CUBE OPTIONS keepalive profile busyout dial-peer when retry count is 1



Identifier	Description
<a href="#">CSCuw34395</a>	SIP Refer Doesnt Work After CUBE Failover
<a href="#">CSCuv97379</a>	[ST-P] STBY router crashed on disconnecting call on ACTIVE
<a href="#">CSCut83406</a>	IPSLA : PPE exception dump due to num_entries=0 in XR ISSU run phase
<a href="#">CSCux99250</a>	ASR 903 IPv6 Multicast crashes
<a href="#">CSCus06318</a>	SNMP IPv6 address discovery with ipAddressTable
<a href="#">CSCuw73532</a>	ISIS multitopology not working if neighbor is sending IPv4 address
<a href="#">CSCuy02409</a>	BDI not Passing VRRP Multicast Traffic
<a href="#">CSCuy19395</a>	ASR1006 :crashes after running the "redundancy force-switchover" command
<a href="#">CSCux78294</a>	Crash on router when removing L2VPN
<a href="#">CSCuw24741</a>	EVPN: Ether serv inst shut not generating AC event
<a href="#">CSCus72718</a>	L2TPv3 session pending between 2 devices
<a href="#">CSCux58640</a>	LDP NSR: Label Mapping Messages Not Sent on RP SSO and VCs Re-bind
<a href="#">CSCux43298</a>	show interface pseudowire displays invalid peer info
<a href="#">CSCuw67049</a>	Traceback seen when standby is trying to BULK sync
<a href="#">CSCuv57459</a>	ASR1K Kernel crash at pidns_get() - part 2
<a href="#">CSCuv23340</a>	Core file not getting generated after kernel crash in crete platform
<a href="#">CSCuw96085</a>	ASR920 crashes on NID Controller configuration commit of native vlan 1
<a href="#">CSCuv99903</a>	ME3600 drops traffic thro' EVC port when EFPs for BD in 1G and 10G ports
<a href="#">CSCuw17403</a>	xconnect not forwarding traffic with local SPAN on Attachment Circuit
<a href="#">CSCuv46139</a>	DHCP relay does not remove Option82 in Offer forwarded to client
<a href="#">CSCuw10281</a>	Traffic drop on mac movement when mac sec is enabled under EFP
<a href="#">CSCuw23745</a>	ME 3600X / SVI VRF Routing problem with Access-Port
<a href="#">CSCuw79818</a>	Incorrect interface counters for multicast
<a href="#">CSCuw39345</a>	mVPN traffic is sent without dot1q header when SVI is core interface
<a href="#">CSCuw31489</a>	ME3600 ciscoEnvMonSupplyState value is wrong after reload
<a href="#">CSCuw70546</a>	ME3600 :: UDLD runs on internal ports
<a href="#">CSCuw93755</a>	ME3800 crashing due to RPF Fail packets punting to the CPU
<a href="#">CSCuv18439</a>	CPUHOGS in chunk corruption crashinfos distracts troubleshooting
<a href="#">CSCuw10271</a>	Sending IMSI/MSISDN in PBU should be optional
<a href="#">CSCuu37200</a>	SC install fails after link re-route
<a href="#">CSCux38250</a>	ASR-903 crashes when configuring MPLS Explicit Null
<a href="#">CSCux47286</a>	UMMT- ASR903 crashes at fib_chain_remove with periodic toggling of ports
<a href="#">CSCut63712</a>	Router responds to MPLS traceroute with next hop IP 127.0.0.1
<a href="#">CSCuw70667</a>	ASR1K crashes at command "show mpls traffic-engineering tunnel"
<a href="#">CSCuw20292</a>	PFR v3.16 collector CLI has missing port number in PFR config
<a href="#">CSCuw75594</a>	ISR4431: Unable to create vlan using WSMA
<a href="#">CSCuv56532</a>	GS: Display inventory CLI is not showing expected output on DSLAM.

Identifier	Description
<a href="#">CSCUu75888</a>	AN: Traceback while removing tunnels after "no autonomic" with NTP
<a href="#">CSCUu80205</a>	Error Msgs on Satellite console when doing shut/no shut of host ICL port
<a href="#">CSCUx20613</a>	Bus error crash at oer_saa_mc_get_probe_stats_cbk
<a href="#">CSCUv22992</a>	PFR router crashes due to watchdog when displaying config
<a href="#">CSCUw65212</a>	Process watchdog crash on 2900 seen with oer_mc_cfg_command
<a href="#">CSCUw47521</a>	Make changes to GRUB in MCP to boot CGE7 images
<a href="#">CSCUw24373</a>	Called-station-id and NAS-ID via account profile satus query
<a href="#">CSCUu64952</a>	double access-request with same username with vpdn authen-before-forward
<a href="#">CSCUx51271</a>	Need to add the attributes 32 and 30 under all status-query related
<a href="#">CSCUu20167</a>	Radius-Proxy Session-Restart fails after ISG idle-timout
<a href="#">CSCUw53543</a>	Stale entries for unauthenticated user in ISG dont clear .
<a href="#">CSCUw91822</a>	vISG not sending COA Response
<a href="#">CSCUw61282</a>	ANCP process crash while sending scale port up messages
<a href="#">CSCUx93045</a>	ISG requests RADIUS although profile is configured locally - ppp changes
<a href="#">CSCUw49798</a>	ASR1K: cpp_cp_svr core@cpp_qm_cm_n_delete_queue
<a href="#">CSCUu92634</a>	ASR1K:FP100: cpp_svr core file seen with uws_wan_xe311 profile
<a href="#">CSCUw94014</a>	cpp_cp crashes with BB profile #6 48k PTA
<a href="#">CSCUw81487</a>	Kahuna RP crash when bringing up PTA sessions with QoS
<a href="#">CSCUw73223</a>	Polaris : cpp_cp_svr crash when the interface goes down
<a href="#">CSCUx10321</a>	ASR1000 CLI hangs on executing the "show platform hardware qfp xxx"
<a href="#">CSCUv56407</a>	ASR1001-X crashed with "ip account mac output" config on interface
<a href="#">CSCUv36911</a>	ASR1K active CGN ESP200 may crash when the CGN standby reloaded
<a href="#">CSCUv90904</a>	ASR1K B2B CGN NAT lost sync in standby IP NAT allocated addresses
<a href="#">CSCUv02537</a>	ASR1K ESP200 reload in a B2B CGN NAT scenario with PAP+BPA
<a href="#">CSCUw79438</a>	NAT64: MAP-T 1300-bytes packet drop at high traffic rate
<a href="#">CSCUu90605</a>	CPP crash in cpp_qm_event_proc_parent_update
<a href="#">CSCUw40400</a>	Router crashed at cpp_free_exmem
<a href="#">CSCtx83808</a>	PPP: Traceback when changing police to shaper on LNS
<a href="#">CSCUv19528</a>	CPU Spikes 99% for 32k scale with common acl and per user ace download
<a href="#">CSCUw26070</a>	%SYS-4-CHUNKSIBLINGSEXCEED:No. of siblings in chunk gone above threshold
<a href="#">CSCUv70649</a>	P2MPTE FRR: Traffic not flowing after moving to backup Tunnel
<a href="#">CSCUx05439</a>	RSVP host sender not chkptd when doing path change (baseline issue)
<a href="#">CSCUv30117</a>	ISR4000 routers lose SRST COR list config after reload
<a href="#">CSCUu74719</a>	ISR 4331 - SRST - Router crash with PSTN conferencing (LocalSoft)
<a href="#">CSCUx61417</a>	Memory leak in IPPM Server due multiple timer registrations
<a href="#">CSCsw96293</a>	Reload in SNMP Proxy Forwarder after IOS upgrade
<a href="#">CSCUu78845</a>	IOS 15.5 SSH auth does not progress to next method

Identifier	Description
<a href="#">CSCuv62376</a>	aaa_coa_request_set_error_reply AAA related Crash
<a href="#">CSCuv56698</a>	ASR1k standby-hot RP crash at SSS Bad root chunk pointer
<a href="#">CSCuv94697</a>	checkpointing of CSUN message
<a href="#">CSCux38847</a>	CSUN sent with M bit set
<a href="#">CSCux36567</a>	DT CPOC bugs
<a href="#">CSCuw53706</a>	LAC does not carry the correct circuit-id in ICRQ message to the LNS
<a href="#">CSCuw82928</a>	Peruser ACL definition needs to be displaced in show CLI same as common
<a href="#">CSCux77926</a>	RFC 5515 : Interim record is triggered when the same ANCP port
<a href="#">CSCux81900</a>	RFC 5515:ICRQ having Blank circuit-id and incorrectly formatted AVP's
<a href="#">CSCux01316</a>	RP crashes when show command for common acl is executed
<a href="#">CSCuw47130</a>	STCAPP commands gets removed after reloading 43XX/44XX routers
<a href="#">CSCuv96640</a>	Traceback seen when BPDU received on BPDU guard enabled NIM-ES2 port
<a href="#">CSCuv31270</a>	Issues with E1 unframed mode when we use back to back ISR4451s
<a href="#">CSCux03041</a>	LDP NSR: Session Flaps on Standby RP Due to MD5 Authentication Failure
<a href="#">CSCuv28196</a>	TCP MSS option in SYN may be ignored
<a href="#">CSCuw21000</a>	Netconf:Unable to install OVA from USB0, neither throw an error message
<a href="#">CSCsq06282</a>	Need ability to specify source address for HTTP messages from VXML GW
<a href="#">CSCuv80214</a>	Router crash on removing dial peer
<a href="#">CSCuw60540</a>	Invalid Input: Trailing space accepted on voice-card x/y command
<a href="#">CSCux07364</a>	QoS settings on Cisco ISR-4K VG for TDM to IP
<a href="#">CSCus84696</a>	Voice gateway not sending ISDN USER_INFO for SIP Info to update number
<a href="#">CSCux29793</a>	2 extra Interim Accounting messages sent after SRL service activation
<a href="#">CSCuv63373</a>	DNS value received from 4G EHWIC not populated correctly in IOS



# Bugs for Cisco IOS Release 15.6(1)S

## Resolved Bugs

Bugs describe unexpected behavior in Cisco IOS software releases. Severity 1 bugs are the most serious bugs; severity 2 bugs are less serious. Severity 3 bugs are moderate bugs, and only select severity 3 bugs are included in this section.

In this section, the following information is provided for each bug:

- Symptoms—A description of what is observed when the bug occurs.
- Conditions—The conditions under which the bug has been known to occur.
- Workaround—Solutions, if available, to counteract the bug.

**Note**

If you have an account on Cisco.com, you can also use the Bug Toolkit to find select bugs of any severity. To reach the Bug Toolkit, log in to [Cisco.com](http://www.cisco.com) and go to [http://www.cisco.com/cgi-bin/Support/Bugtool/launch\\_bugtool.pl](http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl). (If the defect that you have requested cannot be displayed, this 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.)

This section consists of the following subsections:

- [Using the Bug Search Tool, page 29](#)
- [Resolved Bugs—Cisco IOS Release 15.6\(1\)S4, page 31](#)
- [Resolved Bugs—Cisco IOS Release 15.6\(1\)S3, page 32](#)
- [Open Bugs—Cisco IOS Release 15.6\(1\)S2, page 34](#)
- [Resolved Bugs—Cisco IOS Release 15.6\(1\)S2, page 36](#)
- [Open Bugs—Cisco IOS Release 15.6\(1\)S1, page 42](#)
- [Resolved Bugs—Cisco IOS Release 15.6\(1\)S1, page 43](#)
- [Resolved Bugs—Cisco IOS Release 15.6\(1\)S, page 44](#)

## Using the Bug Search Tool

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

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](#).

**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](#).

To use the Cisco Bug Search Tool:

1. In your browser, navigate to the [Cisco Bug Search Tool](#).
2. If you are redirected to a **Log In** page, enter your registered Cisco.com username and password and then, click **Log In**.
3. To search for a specific bug, enter the bug ID in the **Search For** field and press Enter.
4. To search for bugs related to a specific software release, do the following:
  - a. 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.
  - b. 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. You can mouse over bugs to see more content about a specific bug.

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.
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 Cisco Bug Search Tool.
Support Cases	Whether a support case has been opened or not.

Your search results update when you choose a filter.

All resolved bugs for a release are available in the [Cisco Bug Search Tool](#) through the [fixed bug search](#).

This search uses the following search criteria and filters:

Field Name	Information
Product	Series/Model Cisco IOS and NX-OS Software => Cisco IOS
Release	Example: 15.6(1)S
Status	Fixed
Severity	2 or higher

## Resolved Bugs—Cisco IOS Release 15.6(1)S4

This section lists the resolved bugs for Cisco IOS Release 15.6(1)S4. All the bugs have a link to the Bug Search Tool where you can find details of the specific bug. This section describes only severity 1, severity 2, and select severity 3 bugs.

**Table 1** Cisco IOS Release 15.6(1)S4 Resolved Bugs

Caveat ID Number	Description
<a href="#">CSCve54313</a>	Crash in ALPS SNMP code
<a href="#">CSCvc42729</a>	Autonomic Networking Infrastructure Adjacency Discovery DoS Vulnerability
<a href="#">CSCvc42717</a>	Autonomic Networking Infrastructure Registrar Device Reload
<a href="#">CSCvc89965</a>	After reload route policy processing not re-evaluate with route-map using match RPKI
<a href="#">CSCCuw35828</a>	crash w/BGP show advertised-routes when route-server is on vrf
<a href="#">CSCvd09584</a>	eVPN PMSI VNI decoding / encoding as MPLS label
<a href="#">CSCvc31517</a>	Router crashes using BGP commands for long cost extended community string
<a href="#">CSCve57697</a>	Crash in Bstun SNMP code
<a href="#">CSCCuw77959</a>	1801M - %DATACORRUPTION-1-DATAINCONSISTENCY: copy error
<a href="#">CSCvc16650</a>	IOS secure conferencing leads to SRTP bandwidth and tunnels usage to exceed the license limits
<a href="#">CSCCup70353</a>	Cisco IOS XE Software Web User Interface Denial of Service Vulnerability
<a href="#">CSCCuz30491</a>	High CPU Utilization with RIP Timers
<a href="#">CSCvb70426</a>	GETVPN: crash due to unexpected exception to CPU during Reg/Rekey policies from KS
<a href="#">CSCve10917</a>	IPSec crash on ASR1k router while processing KMI
<a href="#">CSCvd40880</a>	Modifying crypto ACL leads to a removal of crypto map config
<a href="#">CSCvc27005</a>	Stateless IPSec HA doesn't work when HSRP packets are being recirculated on VASI link
<a href="#">CSCvc59750</a>	IKEv2 Aggregate-auth Timing Issue
<a href="#">CSCvc99738</a>	IKEv2 tunnel fails to come up b/w Cisco routers post upgrading one router to 15.5(3)S5, 15.5(3)M5
<a href="#">CSCvc12306</a>	Limit ike-init queue to improve performance in scaled scenarios
<a href="#">CSCvd47757</a>	csr1000v is not able to poll CISCO-IPSEC-FLOW-MONITOR-MIB
<a href="#">CSCve62464</a>	Locally generated traffic may be dropped in a GETVPN over DMVPN setup
<a href="#">CSCvb25357</a>	NHRP registration requests failed after ipv6 tunnel source change
<a href="#">CSCvb66239</a>	Willr noL3 tunnel MTU is not signalled properly for locally-originated packets
<a href="#">CSCvb41889</a>	NTP leap second inserted every day after leap second occurs
<a href="#">CSCCuy32325</a>	DMVPN: NHRP route-watch does not delete NHO route after route change
<a href="#">CSCvb92697</a>	High CPU due to NHRP when NHRP cache entry for remote spoke's tunnel address is deleted

Caveat ID Number	Description
<a href="#">CSCvc12485</a>	ASR1006 crash in ospfv2_print_db_simple on cmd "sh ip ospf retransmission-list"
<a href="#">CSCvb84388</a>	Auth and CRL download fails with "There is another request in progress"
<a href="#">CSCuz22162</a>	Digital certificates does not sync to standby
<a href="#">CSCuv44053</a>	PKI Rollover: rollover cert is being added as active id cert
<a href="#">CSCvb73018</a>	PKI: Cannot import RSA SubCA signed by ECDSA
<a href="#">CSCuw42556</a>	retry does not work in one scenario after renewal fail
<a href="#">CSCvc22184</a>	BQS Interrupt QSM_CSR32_QSM_LOGIC_ERR_LEAF_INT__INT_INCORRECT_POP_STATU S_ERR1
<a href="#">CSCvb44207</a>	CTS/SGT across GRE p2p tunnel broken when doing inline tagging
<a href="#">CSCvb92562</a>	Evaluation of all for Openssl 1.0.1 September 2016
<a href="#">CSCve66658</a>	Crash in TN3270E-RT-MIB code
<a href="#">CSCve21448</a>	multiple ISR4K VGW's crashed with Segmentation fault(11), Process = DSMP

## Resolved Bugs—Cisco IOS Release 15.6(1)S3

This section lists the resolved bugs for Cisco IOS Release 15.6(1)S3. All the bugs have a link to the Bug Search Tool where you can find details of the specific bug. This section describes only severity 1, severity 2, and select severity 3 bugs.

**Table 2** Cisco IOS Release 15.6(1)S3 Resolved Bugs

Caveat ID Number	Description
<a href="#">CSCva92726</a>	AN: AN memory holding grows during longevity test
<a href="#">CSCva29933</a>	AN: ASR901 hangs after AN aborts setup dialogue
<a href="#">CSCuz76841</a>	AN: ISR-G3 crashes after disabling autonomic
<a href="#">CSCva49849</a>	AN: Nbr/ACP flap continuously when a rouge device tried to join
<a href="#">CSCuz88340</a>	AN: ULA is configured on ANI & same ANI used for multiple neighbors
<a href="#">CSCva87987</a>	ASR 902 crash on __be_bfd_fib_nh_change_cb
<a href="#">CSCuz58682</a>	Incorrect VPN withdraw with overlapping RT on multiple RT Filter
<a href="#">CSCva86436</a>	no export ipv4 unicast map triggered router to crash
<a href="#">CSCva24325</a>	NSF/SSO feature not honouring TCP MSS
<a href="#">CSCuz21061</a>	router crashes after %BGP-6-BIGCHUNK + SNMP query.
<a href="#">CSCuz81585</a>	CEF adjacency breaks with intervrf traffic in ASR920
<a href="#">CSCuy64522</a>	dhcp process crashed on ISSU when the relay configured on BDI over TEFP
<a href="#">CSCva16353</a>	Fnf related tracebacks and fnf config issues during ISSU process
<a href="#">CSCva15828</a>	AN: Router crash during ACP flap pointing to ikev2
<a href="#">CSCva95795</a>	(RC)ISR 4451 PfR Due to FP Route-Map (Modification of CSCva79279 fix)



<b>Caveat ID Number</b>	<b>Description</b>
<a href="#">CSCuz12967</a>	Crash after show ip protocols vrf with RIP enabled
<a href="#">CSCuz41999</a>	Optimizing the EoGRE endpoint creation/deletion
<a href="#">CSCuz47777</a>	DTMF issue on ISR G3/ASR during the prompt using TCL Script
<a href="#">CSCuy33804</a>	Traceback seen @resolve_sig_ip_address_to_bind during SRTP calls
<a href="#">CSCvb29204</a>	BenignCertain on IOS and IOS-XE
<a href="#">CSCuy14032</a>	IPv6 loopback address not being advertised in isis
<a href="#">CSCuz25240</a>	ISIS not installing back to RIB neighbors loopback when interface flaps
<a href="#">CSCva15526</a>	PW down after clear mpls ldp neighbor followed by RSP SSO
<a href="#">CSCva18067</a>	CPU HOG and Crash by MFIB_rate
<a href="#">CSCuz28618</a>	sup2t: sup crashed after MFIB errors
<a href="#">CSCva43443</a>	DNA/SA, Upon Quad SUP SSO, Mcast decap traffic black holing for ~50 sec
<a href="#">CSCuy45804</a>	MCAST: PIM issue tracking RP source address
<a href="#">CSCva59927</a>	UCI, On QuadS6T Second SSO, PIM joins are not encapsulating over VRF LISP
<a href="#">CSCuz01454</a>	DMVPN: Implicit NHRP Entry Persists if Crypto Fails to Build
<a href="#">CSCva40110</a>	QoS Policy flap with every registration when NAT is involved
<a href="#">CSCva35619</a>	Cisco IOS Software Crafted NTP Packets Denial of Service Vulnerability
<a href="#">CSCvb00978</a>	OSPF SR SID Conflict: when OSPF is shut, conflict resolution not handled
<a href="#">CSCuz49651</a>	AN: PKI crash during bootstrap and certificate renewal
<a href="#">CSCva17234</a>	roll over to new certificate triggers "Crypto CA" to crash
<a href="#">CSCuz62115</a>	Router crash due to PKI process
<a href="#">CSCva72564</a>	Nike-PoC: Autoinstall obtained IP overrides USB bootstrap config
<a href="#">CSCva15013</a>	AAA/RADIUS memory leak on IOS-XE
<a href="#">CSCuz87179</a>	Crash observed while bringing up PTA sessions in SSS Manager
<a href="#">CSCur10056</a>	Memory leak in SSS Manager
<a href="#">CSCuz57124</a>	Tracebacks *MSG 00001 TRUNCATED* on standby, after PTA Sess brought up
<a href="#">CSCuz77746</a>	16.3 throttle: serial interface goes down after enabling ppp
<a href="#">CSCuo76385</a>	Router crashes at ic_dp_classify when Serial link flaps
<a href="#">CSCuw50415</a>	Crash seen @ hwidb_iftype_unlist while doing unconifg of channel-group
<a href="#">CSCuz76821</a>	tableid_ha: Memleak @ eobc_pool_getbuffer
<a href="#">CSCva29311</a>	AN: RPL crash during ACP flap & in scale setup
<a href="#">CSCva46459</a>	SSH session hangs if its not closed properly
<a href="#">CSCux86075</a>	Unexpected crash during SSH operation
<a href="#">CSCuz52528</a>	Evaluation of all for OpenSSL May 2016
<a href="#">CSCuy14110</a>	CPU Hike seen in XE 316 due to VTEMPLATE BKG OW Process
<a href="#">CSCuy38157</a>	Router crash during handling L2 and L3 subscribers at the same time
<a href="#">CSCuz62915</a>	ISR4451 crash under load due to Segmentation fault(11), Process = DSMP
<a href="#">CSCva22751</a>	Router crashing due to a watchdog in the ISDN process

Caveat ID Number	Description
<a href="#">CSCva00551</a>	Cisco Router may crash on SIP MA Process Due to strstrncpy()
<a href="#">CSCuz72665</a>	DATA CORRUPTION-1-DATA INCONSISTENCY error when copying from PAI header
<a href="#">CSCvb24266</a>	ISR 4K Crashes When Running "Debug Voice Translation"

## Open Bugs—Cisco IOS Release 15.6(1)S2

This section lists the open bugs for Cisco IOS Release 15.6(1)S2. All the bugs have a link to the Bug Search Tool where you can find details of the specific bug. This section describes only severity 1, severity 2, and select severity 3 bugs.

**Table 3** Cisco IOS Release 15.6(1)S2 Open Bugs

Identifier	Description
<a href="#">CSCux26195</a>	"aaa accounting suppress null-username" not working as expected
<a href="#">CSCuz44459</a>	Account-stop sent without input output fields
<a href="#">CSCuz77105</a>	ISG: multiple corruption in different code
<a href="#">CSCuz22430</a>	Router reload unexpectedly when received anomaly from TACACS+ server
<a href="#">CSCuz52901</a>	ASR crash while removing crypto key from DMVPN tunnel
<a href="#">CSCuz27907</a>	IOS-XE: Issues with GETVPN and mGRE packet classification
<a href="#">CSCuw94493</a>	Octeon core hang causing F1/F0 offline
<a href="#">CSCuw97842</a>	Standby RP crash at be_ancp_get_dsl_line_attr
<a href="#">CSCuy24258</a>	Bulk sync failure with "bgp ha-mode sso prefer"
<a href="#">CSCuy64509</a>	CUCME enabled on 4321 supports 42 users only
<a href="#">CSCux79855</a>	TPS Server failure in crypto_engine_pk_decrypt breaking https post sso.
<a href="#">CSCuy01341</a>	Crash on processing packet on cws-tunnel in
<a href="#">CSCur72967</a>	43xx/44xx "show platform software cerm-information" not accounting pkts
<a href="#">CSCuz52857</a>	ISR 4K - Crash Due to Stuck Thread in Crypto IPC processing
<a href="#">CSCuz62911</a>	ISR4K Stop Decrypting due to CERM Error - IN_PKT_CERM_DROP
<a href="#">CSCuw48857</a>	UP23n : USD platforms crashes for "sh plat hard crypto-device util" cli
<a href="#">CSCuz50434</a>	ISSU:XE314<->XE316 : IOSd Core@cfm_ha_issu_db_to_msg_pre_mpd_b_transport
<a href="#">CSCut57456</a>	copy run http command crash
<a href="#">CSCuy96461</a>	IOS-XE EPC does not work on port-channel subinterfaces
<a href="#">CSCuy50298</a>	Empty object-group permitting all traffic 4331
<a href="#">CSCuv86229</a>	Interrupt stack overrun and crash due to recursive tunnel lookup, Part 2
<a href="#">CSCux25412</a>	Crash with SIP subscribe notify enabled
<a href="#">CSCuz45207</a>	Cube crash at skinny_codec_supported
<a href="#">CSCuu12283</a>	CUBE failed to create DP session on STBY for Webex flow

Identifier	Description
<a href="#">CSCuz47777</a>	DTMF issue on ISR G3/ASR during the prompt using TCL Script
<a href="#">CSCux05980</a>	IOS-XE router has "[dsp] (ERR): TABLE DB LOOKUP: Invalid ID 0." error
<a href="#">CSCuz71250</a>	Router crashes when parsing ack for mid call
<a href="#">CSCuz69975</a>	Under load crash is seen in CVP REFER_PASSTHRU scenario
<a href="#">CSCuy72671</a>	Traffic drops on ASR1K with RRI gateway option.
<a href="#">CSCuz39721</a>	ASR1K/RP2/SW 15.4(3)S4 crash
<a href="#">CSCux50799</a>	Virtual-PPP source interface is removed adter reload
<a href="#">CSCuy32696</a>	Traceback after cmd 'redistribute lisp'
<a href="#">CSCuu57942</a>	MLDP:Met is inncorectly programmed on root node failure-traffic loss
<a href="#">CSCux10171</a>	[3.17] KinPin Crashed when configuring custom HTTP
<a href="#">CSCuy74032</a>	No value is returned for an SNMP Query from Hierarchical DMVPN HUB
<a href="#">CSCux65145</a>	ASR1K-REST API-ACL: Portnumbers in access-lists are returned incorrectly
<a href="#">CSCuz61339</a>	BGP task crashed with common regular expression in run-configure
<a href="#">CSCuz62898</a>	Crash in BGP due to regular expressions
<a href="#">CSCuz74592</a>	OSPFv3H-2500/6/4 crashed with watchdog due to INValid Key- INVALIDSADATA
<a href="#">CSCum19502</a>	Inconsistent behavior between telnet and ssh in low memory conditions
<a href="#">CSCuz49651</a>	AN: PKI crash during bootstrap and certificate renewal
<a href="#">CSCuy72304</a>	expired or corrupted certificate caused router to crash
<a href="#">CSCuz62115</a>	Router crash due to PKI process
<a href="#">CSCuw79412</a>	%SYS-6-STACKLOW: Stack for process PPP SIP running low, 0/6000
<a href="#">CSCuy08412</a>	ASR1K fman_fp_image crash with ACL changes
<a href="#">CSCuy41164</a>	ISR 4351 crashed while IWAN app was pushing configs
<a href="#">CSCuz10855</a>	ASR1002x crash in crypto_pstate_dequeueue
<a href="#">CSCuz01052</a>	ISR4K: PPE crash from hal_abort with ice_tx_open_slots_thd_matched
<a href="#">CSCux47830</a>	ASRNAT: Pool leak in PAP mode leading to %NAT-6-ADDR_ALLOC_FAILURE
<a href="#">CSCuw95297</a>	ESP200 crash with 550K translations with cablevision config
<a href="#">CSCuw97834</a>	Mismatch in Drop and post policy counters pertaining to CLI and SNMP
<a href="#">CSCuw50415</a>	Crash seen @ hwidb_iftype_unlist while doing unconfig of channel-group
<a href="#">CSCuz72951</a>	Conditional default originate broken for IPv6 BGP
<a href="#">CSCux86075</a>	Unexpected crash during SSH operation
<a href="#">CSCuy38157</a>	Router crash during handling L2 and L3 subscribers at the same time
<a href="#">CSCuy74990</a>	BGP not forming neighborhood on ASR1k with dual RP
<a href="#">CSCue25168</a>	TPM reserves UDP/4500 for no apparent reason
<a href="#">CSCuz23329</a>	Many inactive sccp sessions in show sccp connections
<a href="#">CSCuy85653</a>	One way audio via ISR 4K after call is resumed from IP phone after SNR
<a href="#">CSCuz52693</a>	ISR 4K Memory Holding in CCSIP_SPI_CONTROL
<a href="#">CSCux20199</a>	Re-Invite with (main m line) dead audio stream (port 0) cause FPI hung.

Identifier	Description
<a href="#">CSCuz17364</a>	DTMF Type ahead buffer on GW with Nuance not working
<a href="#">CSCux16650</a>	SHA-2 support on ISR G2

## Resolved Bugs—Cisco IOS Release 15.6(1)S2

This section lists the resolved bugs for Cisco IOS Release 15.6(1)S2. All the bugs have a link to the Bug Search Tool where you can find details of the specific bug. This section describes only severity 1, severity 2, and select severity 3 bugs.

**Table 4** Cisco IOS Release 15.6(1)S2 Resolved Bugs

Identifier	Description
<a href="#">CSCuy21675</a>	Crash@username_command with service pwd-encryption & common-criteria cfg
<a href="#">CSCuy46133</a>	IOS-XE unable to parse automate-tester cmd after save, gone after reload
<a href="#">CSCux69225</a>	Mac filtering option "None" sends blank password
<a href="#">CSCuy01051</a>	MPLS VPN over mGRE Routing issue after reload
<a href="#">CSCuz04324</a>	radius-server vsa send authentication lost after reload
<a href="#">CSCuy92938</a>	Traceback is seen on cpp_cp during the router bootstrap
<a href="#">CSCuy77986</a>	Traceback seen on configuring sgt-caching
<a href="#">CSCuz21435</a>	IOS-XE: 'ACE event' process watchdog crash.
<a href="#">CSCux91300</a>	Polaris 16.2: Traceback@be_ace_send_ikea with gre configs
<a href="#">CSCuy86812</a>	Router crash when share tunnel protection with MGRE and GRE tunnels.
<a href="#">CSCuw95900</a>	Throughput license breaks Dynamic NAT
<a href="#">CSCux86297</a>	show tech-support take long time due to "show crypto ssl stats"
<a href="#">CSCux32083</a>	AN autoconfigured NTP server must support lower stratum
<a href="#">CSCuy04454</a>	AN: "autonomic connect" interface is not in AN VRF after int reconf.
<a href="#">CSCuy02477</a>	AN: AN creating channel in autonomic connect interface
<a href="#">CSCuu12394</a>	AN: Config download is not triggered when reloaded without saving conifg
<a href="#">CSCux15053</a>	AN: Config server address not getting removed after withdrawing service
<a href="#">CSCuy87056</a>	AN: Device receives & keeps multiple certificates
<a href="#">CSCuy41049</a>	AN: Multiple CD channels getting created on same int for same neighbor
<a href="#">CSCuw81472</a>	AN: Need to increase max NTP association for scale setups
<a href="#">CSCuy86757</a>	AN: NTP not syncing in recent images
<a href="#">CSCux21920</a>	AN: Registrar does not retry bootstrap once it fails during re-bootstrap
<a href="#">CSCuy08030</a>	AN: sh an int output prints Probing for AN disabled int
<a href="#">CSCuw47904</a>	Registrar should validate configured domain-id while unshutting.
<a href="#">CSCuy03054</a>	ASR1K IOSd may crash in BGP Acceptor process due to segmentation fault
<a href="#">CSCuw92735</a>	BGP multicast signalling is not working properly, Error: c-route type 7
<a href="#">CSCuz05346</a>	BGP needs to recognize 4-byte private ASN
<a href="#">CSCuy20481</a>	Crash due to stale pointer after removing vrf command export AF map
<a href="#">CSCux76332</a>	Deleting a statement in export map, removes other statement
<a href="#">CSCux91976</a>	gateway route with AIGP metric only works for host route without supernet
<a href="#">CSCuy03504</a>	Incorrect prefix count upon clearing bgp peering
<a href="#">CSCux62094</a>	Routes are not exported from vrf to global due to incorrect export limit
<a href="#">CSCuw99632</a>	SUP crash @process bgp router when configure ng-mvpn
<a href="#">CSCuy40894</a>	VPN routes may miss withdraws with RTC post route to peer disturbance
<a href="#">CSCuy12658</a>	Unexpected behavior and errors related to downstream voice flows on cBR8
<a href="#">CSCuy90036</a>	Hostname not allowed beginning with numbers

Identifier	Description
<a href="#">CSCUy53662</a>	SIP CME is not updating busy-trigger-per-button value
<a href="#">CSCUx75400</a>	TDOS and silent-discard are impacting SIP SRST Phone Registration
<a href="#">CSCUw02624</a>	IOS:Cannot periodically establish SSL connection
<a href="#">CSCUx47123</a>	Polaris: In FIPS mode, router should crash if it can not get HW entropy
<a href="#">CSCUw58071</a>	CSR XE317: CSR crashes during IPSEC session bring up
<a href="#">CSCUy01341</a>	Crash on processing packet on cws-tunnel in
<a href="#">CSCUw43560</a>	crash while running uid script.
<a href="#">CSCUx77377</a>	Traceback on Idle system with one lite session on continuous churn
<a href="#">CSCUv91777</a>	VPN suboptions are never removed.
<a href="#">CSCUz49548</a>	MLPPP over dialer broken for all platforms
<a href="#">CSCUy46981</a>	"no ip domain lookup" always in "sh run all"
<a href="#">CSCUw21120</a>	Crash on router due to authentication
<a href="#">CSCUv46710</a>	Segmentation Fault in Auth Manager
<a href="#">CSCUy96753</a>	Sup7E crashes when executing "no authentication port-control auto"
<a href="#">CSCUy04058</a>	ISR-4K IOS CFB resources get into hung state (inactive)
<a href="#">CSCUw90662</a>	MODEMPASS usage does not show up in show call active voice brief output
<a href="#">CSCUz62786</a>	ISR4K sccp based transcoding hanging dsp-session_leg on data-plane
<a href="#">CSCUv50743</a>	MAC stuck on 'PRE Event Handling' - needs reload for recover
<a href="#">CSCUx82241</a>	\$\$TS: EIGRP SAF sequence not same for site-prefix and discovered site
<a href="#">CSCUx92391</a>	\$\$TS: SAF service 5 is not seen on 3945e branch after HUB MC reload
<a href="#">CSCUx41072</a>	EIGRP sending hello messages with interface in passive mode.
<a href="#">CSCUv85472</a>	SR 635576687 6500 EIGRP VRF MD5 AUTHENTICATION ERROR AFTER RELOAD
<a href="#">CSCUv74256</a>	IOS: HMAC key miscalculated with DH Group 21 and IPsec PFS enabled
<a href="#">CSCUw42626</a>	ISR4451(overlord): Packet drop with AH Algorithm SHA384 and 512
<a href="#">CSCUw48857</a>	UP23n : USD platforms crashes for "sh plat hard crypto-device util" cli
<a href="#">CSCUv40225</a>	G8032 ring stuck on protection State
<a href="#">CSCUz50434</a>	ISSU:XE314<->XE316 : IOSd Core@cfm_ha_issu_db_to_msg_pre_mpd_b_transport
<a href="#">CSCUx99594</a>	EEM Policies May Not Be Able To Send Email
<a href="#">CSCUx68976</a>	Crash in fib_fib_get_fib_tableid
<a href="#">CSCUx06777</a>	Device crash with RPF configured.
<a href="#">CSCUx91174</a>	FNF: add show tech fnf
<a href="#">CSCUy38707</a>	After RSP switchover, BFD hangs for up to 10 minutes before converging
<a href="#">CSCUz07185</a>	CDR field 71 (remote-media-address string) is 0.0.0.0
<a href="#">CSCUy21885</a>	Changing "no monitor event-trace voip ccsip limit" to default limit
<a href="#">CSCUy92547</a>	Crash at pp_delete_socket
<a href="#">CSCUy48358</a>	Crash during SIP subscribe notify ACK

Identifier	Description
<a href="#">CSCuy96064</a>	Crash seen under load in CVP REFER_MIDCALL BLOCK scenario
<a href="#">CSCux25412</a>	Crash with SIP subscribe notify enabled
<a href="#">CSCux01773</a>	CUBE Anti-Tromboning C-Line Transition not properly handled.
<a href="#">CSCux73693</a>	Cube doesn't handle notify 200 ok if it is received after the bye
<a href="#">CSCuy33237</a>	CUBE not triggering reinvoke during call resume
<a href="#">CSCuz14872</a>	IOS Fails to correctly populate RTCP SSRC Field
<a href="#">CSCuy19807</a>	IOS-XE CUBE Hold/Resume Fails when negotiating video
<a href="#">CSCuz14861</a>	IOS-XE Fails to correctly populate RTCP SSRC Field
<a href="#">CSCux05980</a>	IOS-XE router has "[dsp] (ERR): TABLE DB LOOKUP: Invalid ID 0." error
<a href="#">CSCuw70011</a>	NanoCUBE stale registration entries with options keepalive
<a href="#">CSCuz25416</a>	ROC update for CUBE session refresh dspware and IOS code commit
<a href="#">CSCuy19738</a>	sh dspfarm profile <id> shows active dsp resource even after call disconnect
<a href="#">CSCuw17287</a>	[PI28 HARD]CUBE is sending wrong codec in 200OK resp ED UPDATE consume
<a href="#">CSCux10166</a>	After flapping mid router interface more than 1 child SAs are removed
<a href="#">CSCuy30957</a>	For IPv6:Activate Under GDOI Fail-Close Disappears on Reboot
<a href="#">CSCuw79748</a>	Cannot ping own tunnel interface
<a href="#">CSCuy43118</a>	XE316: HubBR might be crashed@tunnel_protection_validate_shared_profile
<a href="#">CSCtw74492</a>	flexvpn: user authorization should work with local AAA
<a href="#">CSCuw48400</a>	GetVPN GM unable to register or rekey fails - sig-hash > default SHA-1
<a href="#">CSCuy01778</a>	GETVPN KS reload after split and merge
<a href="#">CSCuz14788</a>	New reg invoke PKI function breaks the GETVPN CRL Checking feature
<a href="#">CSCux83732</a>	Pseudotime not being synchronized between GETVPN Key Servers
<a href="#">CSCux25628</a>	Diffie Hellman computation fails due to leak in crypto engine
<a href="#">CSCuy41990</a>	ikev2 2nd time rekey fails when rekey request packet is fragmented
<a href="#">CSCuz17348</a>	IKEv2 lifetime resets to default after reboot
<a href="#">CSCuw76420</a>	IKEv2 rsa-sig failed with certificate lifetime beyond 2035
<a href="#">CSCux66591</a>	vrf specific name-server / host entries gets deleted on flexvpn client
<a href="#">CSCuv31981</a>	ISR Router Crashes When Trying to Delete a Freed SA
<a href="#">CSCuy83787</a>	ISIS authentication problem even 'send-only' is configured
<a href="#">CSCuz25240</a>	ISIS not installing back to RIB neighbors loopback when interface flaps
<a href="#">CSCux29806</a>	ISIS routes are not not installed in the routing table from isisdatabase
<a href="#">CSCuy37025</a>	ISIS: Show ip route shows deleted route as still being advertised, even though it not advertised.
<a href="#">CSCuy81301</a>	mpls forwarding table holds info even after config replace with base cfg
<a href="#">CSCuy90947</a>	ASR1K : GTP PDP context stuck in deleting state
<a href="#">CSCuz35203</a>	SSM connection manager crash during VFI pseudowire bind
<a href="#">CSCuy02409</a>	BDI not Passing VRRP Multicast Traffic
<a href="#">CSCuy60338</a>	l2tp crashes during failover preceded by a kernel panic

Identifier	Description
<a href="#">CSCux78294</a>	Crash on router when removing L2VPN
<a href="#">CSCux58640</a>	LDP NSR: Label Mapping Messages Not Sent on RP SSO and VCs Re-bind
<a href="#">CSCuz33024</a>	standby RSP failed to syncup if mix of manual and auto-discovered PW
<a href="#">CSCuz34243</a>	the AC segment remains unprovisioned when 'no shut' is done
<a href="#">CSCux73439</a>	ASR - hpet2 increasing min_delta_ns to 33750 nsec
<a href="#">CSCuz18772</a>	ASR1004:RP1 : Clock reset to 1 January, 1970 after reload
<a href="#">CSCux05579</a>	IPCentral: Systemtap 1.4
<a href="#">CSCuy65618</a>	LISP may put incorrect UDP checksum into control messages
<a href="#">CSCuy03680</a>	V3Lite IGMP packets sent instead of V3 when UDP based feature is present
<a href="#">CSCuy51474</a>	In-band signaling: mLDP database inconsistency causes RPF failures
<a href="#">CSCux21746</a>	NTT: CPU hog post SSO for 30K/50K scale
<a href="#">CSCux23839</a>	MAG flaps bindings and tunnel for every mobile network update
<a href="#">CSCux34430</a>	Traffic not flowing through for MAG MNP's with PBR
<a href="#">CSCuy87734</a>	ASR1K RP crashes LCON Main process when heavily loaded
<a href="#">CSCuw37452</a>	ASR1K: Traceback seen @ unconfiguring LDP configurations
<a href="#">CSCuy81441</a>	Router may crash due to LDP bindings
<a href="#">CSCuz04378</a>	ICMP Time exceed dropped due to uRPF on the MPLS PE (per-ce label)
<a href="#">CSCuy05549</a>	MPLS: ping mpls failed with no FEC mapping
<a href="#">CSCuz13646</a>	Crash seen on ISR c2951
<a href="#">CSCuy51013</a>	ESP crash on upgrade from XE3.11 to XE3.16.1a
<a href="#">CSCuy71712</a>	FlexVPN: Spoke spawns a virtual access to connect to the hub
<a href="#">CSCuw92679</a>	IOS-XE crash at nhrp_iprib_lost_route when running "debug nhrp routing"
<a href="#">CSCut61985</a>	MPLSoDMVPN; Ping to spoke int. fails if dest. mask is /32
<a href="#">CSCux80450</a>	%REGISTRY-3-STUB_CHK_OVERWRITE: error seen during boot up
<a href="#">CSCuu75888</a>	AN: Traceback while removing tunnels after "no autonomic" with NTP
<a href="#">CSCuy20654</a>	ASR1k reply to NTP broadcast
<a href="#">CSCux99025</a>	Evaluation of Cisco IOS and IOS-XE for NTP January 2016
<a href="#">CSCuz24233</a>	NTP process is getting stopped & not able to create server relationship
<a href="#">CSCux47463</a>	RestAPI: rate-limit is trigger due to one request with wrong user/paswd
<a href="#">CSCuz42995</a>	CSCus79699 broke top allocators in crashinfo
<a href="#">CSCuy68037</a>	Crash due to IOS watchdog when deleting persistent logging files
<a href="#">CSCuy44377</a>	Syslog: Source-Interface address change doesn't take effect in IPv6
<a href="#">CSCuy04757</a>	Crash@ospfv3_router_process_mgd_timers on shut/no shut of sub-intf
<a href="#">CSCuy32709</a>	R-LFA Tunnels not established on setting DS required attribute
<a href="#">CSCux19034</a>	XE3.16 crashes when conf "distribute-list" under router ospf and sh run
<a href="#">CSCux82630</a>	show version: system restart time changes by a second periodically
<a href="#">CSCuu25580</a>	VTY0-4 settings are modified if switch is accessed via WebUI



Identifier	Description
<a href="#">CSCuo61229</a>	ASR1002 Crashed after "show pfr master active running"
<a href="#">CSCCuy85870</a>	Wrong TD next-hop for overlapping prefixes
<a href="#">CSCCuu98319</a>	AN: Disabling AN is not removing crypto pki trust point created by AN
<a href="#">CSCCuy33129</a>	G2 routers not able to download Trustpool due to nvram space
<a href="#">CSCCuy13701</a>	IOS PKI: Crash while editing a VRF aware TP with enrollment profile
<a href="#">CSCCuy77179</a>	Calling-station-id missing in web logon access-request
<a href="#">CSCCuz41395</a>	CoA Ack for service-logon does not have session ip addr
<a href="#">CSCCuy26377</a>	Memory leak observed after upgrade to XE 3.13.4
<a href="#">CSCCuy40721</a>	Not updated parameters when session is renewed in unauth state
<a href="#">CSCCuy08412</a>	ASR1K fman_fp_image crash with ACL changes
<a href="#">CSCCuz10855</a>	ASR1002x crash in crypto_pstate_dequeue
<a href="#">CSCCux68096</a>	ucode crash abort called from ipv4_nat_create_inside_addrport_bind
<a href="#">CSCCuw35544</a>	CGE7,SysBuff exhaust due to conf/unconf qlimit causing fairq qlimit go wild
<a href="#">CSCCuy16530</a>	Crash after member link re-added to port-channel and clear counters CMD
<a href="#">CSCCux89723</a>	Error when service-policy at sub-interface/pvc/service-group is applied
<a href="#">CSCCuw50415</a>	Crash seen @ hwidb_iftype_unlist while doing unconfifg of channel-group
<a href="#">CSCCuw55717</a>	Memleak @ pak_pool_cache_item_get : Scaled TFEX
<a href="#">CSCCuy55849</a>	RTR installs the ISIS(or OSPF) route with Higher Metric in the RIB
<a href="#">CSCCuy07343</a>	AN : ipv6 global prefixes are seen in the cisco_autonomic vrf table
<a href="#">CSCCuw81424</a>	AN: Router crashes in scale hub & spoke setup
<a href="#">CSCCuy39110</a>	ESRST voice gateway crash when SCCP phone goes off-hook
<a href="#">CSCCuy86782</a>	AN: SSH to AN ULA though ACP fails, if access list is configure on VTY
<a href="#">CSCCuw57124</a>	Cat3750 stack switch memory leak in MallocLite and Dead memory
<a href="#">CSCCuy87667</a>	Crash due to Block overrun by AAA banner
<a href="#">CSCCuw09694</a>	Device crash when "ip host" used by an SSH sourced from CLI is removed
<a href="#">CSCCuy45630</a>	IOS SSH client incorrectly interprets version string and terminates sess
<a href="#">CSCCuy38709</a>	Memory leak with watcher_create_common.
<a href="#">CSCCuy54623</a>	Evaluation of all for OpenSSL March 2016
<a href="#">CSCCux82377</a>	ASR 1K ISG Router Crashes When Polling "csubSessionEntry" MIB
<a href="#">CSCCux90880</a>	ASR1004 memory leak due to SSS Manager
<a href="#">CSCCuy69440</a>	ISG Critical Exception and crashing with SSS-Manager holding memory
<a href="#">CSCCuy14138</a>	RFC 5515 : CSUN is triggered when IPBSA service is applied
<a href="#">CSCCux81900</a>	RFC 5515:ICRQ having Blank circuit-id and incorrectly formatted AVP's
<a href="#">CSCCuy94842</a>	Crash on router when using stcapp
<a href="#">CSCCuz03079</a>	ISR-4K Processing Error: H323 Setup parameter "mediaWaitForConnect TRUE"
<a href="#">CSCCuy87720</a>	Commit libQsig for both 64bit and 32bit
<a href="#">CSCCuz23329</a>	Many inactive sccp sessions in show sccp connections

Identifier	Description
<a href="#">CSCuy85653</a>	One way audio via ISR 4K after call is resumed from IP phone after SNR
<a href="#">CSCuy79096</a>	show call active voice brief crashed router with FLEX DSPRM MAIN
<a href="#">CSCuy65330</a>	RSVP Reservation Failure Causes Call Drop on Voice to Video Calls
<a href="#">CSCuy43633</a>	Voice Gateways - SCCP Early Offer fails with IPv6 enabled.
<a href="#">CSCuz58660</a>	FXO port stuck with "Connection plar opx immediate " under CUCM
<a href="#">CSCuz42755</a>	FXS Ports on VG320 registered on CUCM via MGCP stop working after reset
<a href="#">CSCuz20065</a>	needs to discard voip packet for lmr half duplex case in isr4k
<a href="#">CSCuy80902</a>	VG320 - voice-port power alarms and loud noise when call is answered
<a href="#">CSCuy15638</a>	Voice ports are stuck in EM_PARK state in e&m-melcas-delay
<a href="#">CSCuv87098</a>	Connected number not populated in RPID correctly
<a href="#">CSCuy68921</a>	Crash seen when forwarding of SIP MWI as qsig MWI on ISR4k and ISRG2
<a href="#">CSCuz22409</a>	SIP UPDATE/Re-INVITE not passed to one of the recording legs by CUBE
<a href="#">CSCus03761</a>	Stack overflow crash @ ip_epm_proxy_slow_check.
<a href="#">CSCuz60446</a>	TDM to SIP - Gateway views outgoing SDP content-length size inaccurately
<a href="#">CSCum05146</a>	NAT SIP ALG removes certain media attributes
<a href="#">CSCuz17364</a>	DTMF Type ahead buffer on GW with Nuance not working

## Open Bugs—Cisco IOS Release 15.6(1)S1

This section lists the open bugs for Cisco IOS Release 15.6(1)S1. All the bugs have a link to the Bug Search Tool where you can find details of the specific bug. This section describes only severity 1, severity 2, and select severity 3 bugs.

**Table 5** Cisco IOS Release 15.6(1)S1 Open Bugs

Identifier	Description
<a href="#">CSCuw81424</a>	AN: Router crashes in scale hub & spoke setup
<a href="#">CSCuy03054</a>	ASR1K IOSd may crash in BGP Acceptor process due to segmentation fault
<a href="#">CSCuy01341</a>	Crash on processing packet on cws-tunnel in
<a href="#">CSCuw75695</a>	Router crash due to Process = SSS Manager
<a href="#">CSCux96341</a>	3945 crash on flapping tunnels with traffic
<a href="#">CSCuy08412</a>	ASR1K fman_fp_image crash with ACL changes
<a href="#">CSCuy20489</a>	ASR experiences ucode crashes on 15.6(1)S due to sipvicious
<a href="#">CSCuy16530</a>	Crash after member link re-added to port-channel and clear counters CMD
<a href="#">CSCuy39110</a>	ESRST voice gateway crash when SCCP phone goes off-hook
<a href="#">CSCuy38157</a>	Router crash during handling L2 and L3 subscribers at the same time

## Resolved Bugs—Cisco IOS Release 15.6(1)S1

This section lists the resolved bugs for Cisco IOS Release 15.6(1)S1. All the bugs have a link to the Bug Search Tool where you can find details of the specific bug. This section describes only severity 1, severity 2, and select severity 3 bugs.

**Table 6** Cisco IOS Release 15.6(1)S1 Resolved Bugs

Identifier	Description
<a href="#">CSCuw38000</a>	Password complexity implementation does not match DISA requirements
<a href="#">CSCux44780</a>	ASR1K/ISR4K crashes after removing tunnel interface
<a href="#">CSCuw66787</a>	Clear ip nat translation vrf X impacts vrf Y
<a href="#">CSCuw79036</a>	AN: Device id/address is not getting populated properly beyond 127
<a href="#">CSCux80195</a>	AN: Manual tunnel creation fails after few ACP flap
<a href="#">CSCux75878</a>	AN: UDI getting truncated in "show autonomic registrar devices accepted"
<a href="#">CSCux70853</a>	ISR - 4400 crash
<a href="#">CSCux88022</a>	ASR1K : Crash at dhcp_sip_get_config
<a href="#">CSCux33385</a>	DHCP binding deletes cash after getting unicast DHCP request
<a href="#">CSCuw99105</a>	DNS query is being sent with wrong interface IP instead of configured IP
<a href="#">CSCuy04058</a>	ISR-4K IOS CFB resources get into hung state (inactive)
<a href="#">CSCux70821</a>	HSRP crashed after changed serial int encaps from frame-relay to DHCP
<a href="#">CSCux11291</a>	OTV adjacency does not come-up with VRF
<a href="#">CSCuw48118</a>	ASR920 - crash in bcopy called from 'addnew' during reassembly
<a href="#">CSCuw74179</a>	CSR: static route via VTI fails to restore after Interface shut/no shut
<a href="#">CSCux29974</a>	ISR4k:UnconfiguredIpv4Fia drop seen for pkts transit via PPPoE
<a href="#">CSCuw90105</a>	Found multiple sessions in MF multiple recording server scenario
<a href="#">CSCux09048</a>	flow restrict on backup crypto map causes traffic to fail
<a href="#">CSCux99250</a>	ASR 903 IPv6 Multicast crashes
<a href="#">CSCuy19395</a>	ASR1006 :crashes after running the "redundancy force-switchover" command
<a href="#">CSCus72718</a>	L2TPv3 session pending between 2 devices
<a href="#">CSCux05779</a>	LISP possible segmentation fault with DDT enabled
<a href="#">CSCuu75176</a>	Multiple AN values for Rx SA observed in show macsec status
<a href="#">CSCux38250</a>	ASR-903 crashes when configuring MPLS Explicit Null
<a href="#">CSCuu30930</a>	ENH IOS PKI: Client should accept content-type x-x509-next-ca-cert
<a href="#">CSCuw24373</a>	Called-station-id and NAS-ID via account profile satus query
<a href="#">CSCuu20167</a>	Radius-Proxy Session-Restart fails after ISG idle-timout
<a href="#">CSCuw91822</a>	vISG not sending COA Response
<a href="#">CSCuw61282</a>	ANCP process crash while sending scale port up messages
<a href="#">CSCuw70580</a>	csr 1000v reboot when configuring firewall
<a href="#">CSCux52451</a>	VRF Domain half open counter increments when aggressive aging occurs

Identifier	Description
<a href="#">CSCux35719</a>	ASR1K QFP crash with SSLVPN
<a href="#">CSCuv19528</a>	CPU Spikes 99% for 32k scale with common acl and per user ace download
<a href="#">CSCuu74719</a>	ISR 4331 - SRST - Router crash with PSTN conferencing (LocalSoft)
<a href="#">CSCuw51653</a>	SIP SRST router in eSRST mode reject phone registration due to + DN
<a href="#">CSCux03041</a>	LDP NSR: Session Flaps on Standby RP Due to MD5 Authentication Failure
<a href="#">CSCux07364</a>	QoS settings on Cisco ISR-4K VG for TDM to IP
<a href="#">CSCuy16501</a>	After IOS upgrade users hear static during external calls
<a href="#">CSCux88265</a>	DSP errors seen and audio fails for MGCP-FXO to IP Phone call
<a href="#">CSCux22874</a>	On demand PCM captures needs to be available on ISR4k routers
<a href="#">CSCux29793</a>	2 extra Interim Accounting messages sent after SRL service activation

## Resolved Bugs—Cisco IOS Release 15.6(1)S

This section lists the resolved bugs for Cisco IOS Release 15.6(1)S. All the bugs have a link to the Bug Search Tool where you can find details of the specific bug. This section describes only severity 1, severity 2, and select severity 3 bugs.

**Table 7** Cisco IOS Release 15.6(1)S Resolved Bugs

Identifier	Description
<a href="#">CSCuw59839</a>	ASR903-200G: Associated sensors are not populated for 200G RSP.
<a href="#">CSCuv30861</a>	ATM auto-vc VCs unable to activate, stuck in deleted state
<a href="#">CSCul15273</a>	AN Link local Tunels not deleted after no autonomic is issued
<a href="#">CSCuv87599</a>	Manually entered IKEv2 crypto profile not NVgen-ed with AN active
<a href="#">CSCut74192</a>	bfd session not coming up after interface in vrf shut and no shut
<a href="#">CSCuv66776</a>	MQC Policy-map counters do not update in T3/E3 SPA
<a href="#">CSCuw37313</a>	IPsec crash at UNIX-EXT-SIGNAL: Aborted(6), Process = NIST rng proc
<a href="#">CSCuu41817</a>	3850 cts assigning multicast traffic to sgt default (65535)
<a href="#">CSCuw23857</a>	Crash at CWS TUN WL process while running DSA script
<a href="#">CSCuv72590</a>	CWS-Tunnel adjacency not formed even though tunnel is UP
<a href="#">CSCuw23345</a>	CWS: Parameter-map primary tower configuration issue
<a href="#">CSCut40756</a>	ISR Crashing when upgrading image
<a href="#">CSCuo91040</a>	ENH: Add "ip dhcp support tunnel unicast" command to IOS-XE
<a href="#">CSCuv39338</a>	ISG: DHCP Server RADIUS Proxy Memory Leak
<a href="#">CSCuw18886</a>	Crash while removing whitelist with 1K entries in DSA DB
<a href="#">CSCuv61150</a>	crash while removing whitelisting with 5k IP's in DSA DB
<a href="#">CSCut37527</a>	MDC: mc origin not found rejecting the channel addition on branch master
<a href="#">CSCut98730</a>	EIGRP authentication fail with key config-key password encryptionenabled
<a href="#">CSCuq78983</a>	RIPv2 key-chain CLI disappears when doing config replace

Identifier	Description
<a href="#">CSCut79286</a>	ASR1K QoS feature doesn't work fine with RP2/RIs3.x
<a href="#">CSCut12738</a>	[ASR1K HSRP] Physical Link Failure Causes HSRP to Fail
<a href="#">CSCuu87276</a>	Link-protection group config is removed from interface after IM_OIR
<a href="#">CSCuv45996</a>	DM on EVC BD Up mep, reload inactive SLA session showing wrong values.
<a href="#">CSCuw12720</a>	MallocLite memory leak due to EEM when using "file open" action.
<a href="#">CSCus26844</a>	Interrupt stack overrun and crash caused by MPLS recursive tunnel lookup
<a href="#">CSCuu03778</a>	ISSU:XE313<->XE314 Traceback@fib_subtree_context_lc_unpack_xdr after RV
<a href="#">CSCuu26303</a>	Router crash triggered by service policy and ipv6 traffic
<a href="#">CSCuw05651</a>	EzPM causes STACKLOW message and a subsequent crash
<a href="#">CSCut80144</a>	Beni MR1: Debug(network-rf ) enabled by default on Mingla
<a href="#">CSCut44432</a>	Chunk Manager Leak due to PROTO_COUNTER
<a href="#">CSCuu26939</a>	ISR4k: MAC address for STCAPP FXS ports will show as 0000000000
<a href="#">CSCuv19154</a>	After upgrade of IOS-XE software, appnav functionality maybe impacted.
<a href="#">CSCuv83793</a>	AppNav-XE drop packets when traffic from WAAS has wrong ID
<a href="#">CSCuu82763</a>	Evaluation of ciscossl in bins for OpenSSL June 2015 vulnerabilities
<a href="#">CSCur72779</a>	XE314 : B2B NAT : Stale NAT translations observed on Active rtr
<a href="#">CSCuv39756</a>	EFP crash with vxlan mcast core and unicast traffic 1400 size
<a href="#">CSCuv14905</a>	vxlan source port calculated based on src and dest IP/port of payload
<a href="#">CSCuu80048</a>	interface IP address change cause leaked routes in exported vrfs
<a href="#">CSCue68124</a>	PBR not work with null0 default route
<a href="#">CSCuv80943</a>	MCP_DEV:Packet drops@Ipv6NoRoute with ipv6gre configs
<a href="#">CSCuw19340</a>	Mixed Mode: Tunnel changes for mixed mode support for VTI.
<a href="#">CSCuu29037</a>	MPLS VPN OVER MGRE fails if physical interface used instead of loopback.
<a href="#">CSCuv99758</a>	Remove unnecessary packet debugs for UDP tunnels
<a href="#">CSCut24140</a>	Old active not coming up after first sso also seeing a traceback.
<a href="#">CSCuu28199</a>	[Amur-MR3]IOSD crash reported@spi_iosd_ipc_process_inbound_mts_msg
<a href="#">CSCuv08835</a>	IPSEC key engine process leaks /w dynamic crypto map in scaled scenario
<a href="#">CSCun57148</a>	High CPU in FNF Cache Ager P
<a href="#">CSCut98036</a>	ISR 4K Crash during Keychain Config w/ "Pass enc AES" Enabled
<a href="#">CSCuv26780</a>	Memory leak when qos pre-classify is configured with Crypto
<a href="#">CSCut23024</a>	ipv6 bgp neighborhood does not come up
<a href="#">CSCuv11419</a>	ISR G3 is rejecting the incoming ISDN call setup (SEGMENT) message.
<a href="#">CSCuv07441</a>	ASR1k OTV FHRP packets are blocked even with 'no fhrp filter' CLI
<a href="#">CSCuv39712</a>	asr1k After config/UNCONFIG MPLS, can NOT config OTV. MPLS still there.
<a href="#">CSCuv56754</a>	EoMPLS xconnect remains "RECOVERING" after RP SSO on egress
<a href="#">CSCuv29418</a>	Router is continuously switching between active and standby EoMPLS PW
<a href="#">CSCuu50269</a>	RSP2: MSPW sessions down on S-PE after SSO

Identifier	Description
<a href="#">CSCuu92194</a>	RSP3:HSPW PW-Group Switchover results in traffic blackhole with no scale
<a href="#">CSCut24465</a>	Static VFI went down after PTF reset
<a href="#">CSCuv34896</a>	VPLS autodiscovery PW failed to comeup when BGP recovers from failure
<a href="#">CSCuu36041</a>	VPLS BGP AD resigalling time takes ~20-40s for multi-homing scenario
<a href="#">CSCuu88964</a>	ASR1K Kernel crash at pidns_get()
<a href="#">CSCuv57459</a>	ASR1K Kernel crash at pidns_get() - part 2
<a href="#">CSCuv23340</a>	Core file not getting generated after kernel crash in crete platform
<a href="#">CSCuu90695</a>	DM/SM boundary (S,G) are not repopulated: Multicast Missing Registration
<a href="#">CSCuu30091</a>	MCP_DEV:Packet drops@Ipv4NoAdj with V6MVPN configs
<a href="#">CSCuv18439</a>	CPUHOGS in chunk corruption crashinfos distracts troubleshooting
<a href="#">CSCuu37200</a>	SC install fails after link re-route
<a href="#">CSCuv61750</a>	ASR903 MCP_DEV: Mismatch in VC label programming, EoMPLS scenario
<a href="#">CSCuv65370</a>	Avoid any action on Leap SEcond indicator flag for non-leap second months
<a href="#">CSCut64845</a>	Crashdump does not work on PPC Platform
<a href="#">CSCuv22992</a>	PFR router crashes due to watchdog when displaying config
<a href="#">CSCuu97977</a>	Pfrv2 load-balance not working with passive mode.
<a href="#">CSCuv30857</a>	Crash observed in SSS Manager - 16K PM testing
<a href="#">CSCuv31586</a>	Crash on stby RP while Oversubscription
<a href="#">CSCuu28688</a>	Oversubscription not working with "shaper average percent" config
<a href="#">CSCut22660</a>	Session in attempting state on standby when method list is default
<a href="#">CSCur88124</a>	default throttling require other defaults in some cases
<a href="#">CSCut68925</a>	Crash seen in QOS when policy-map without child or turbo svc is used
<a href="#">CSCuv21984</a>	Fair-queue queue-limit force adjust after change queue-limit.
<a href="#">CSCuu68862</a>	SUP crash @ Process = SNMP ENGINE
<a href="#">CSCuv74171</a>	crash on command "show snmp view"
<a href="#">CSCuu06215</a>	AAA sends garbage value to SSH and causes RP crash
<a href="#">CSCuu78845</a>	IOS 15.5 SSH auth does not progress to next method
<a href="#">CSCuv56698</a>	ASR1k standby-hot RP crash at SSS Bad root chunk pointer
<a href="#">CSCut65242</a>	ISG passing traffic while configured default drop should be used
<a href="#">CSCuu75354</a>	ISG: Dedicated session provisioning failure post lite session conversion
<a href="#">CSCut87425</a>	CPU hog in "EEM TCL Proc" after TCL script termination with long runtime
<a href="#">CSCuv51901</a>	ASR1K BGP send UPDATE don't observe the TCP OPTION

## Related Documentation

The following sections describe the documentation available for Cisco IOS Release 15.5S. These documents include hardware and software installation guides, Cisco IOS configuration and command reference publications, system error messages, and feature modules.

Documentation is available online on Cisco.com.

Use these release notes with the resources described in the following sections:

- [Platform-Specific Documents, page 47](#)
- [Cisco Feature Navigator, page 47](#)
- [Cisco IOS Software Documentation Set, page 48](#)
- [Notices, page 48](#)
- [Obtaining Documentation and Submitting a Service Request, page 50](#)

## Platform-Specific Documents

Cisco 7600 Series Routers

[http://www.cisco.com/en/US/products/hw/routers/ps368/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/hw/routers/ps368/tsd_products_support_series_home.html)

Cisco ASR 901 Router

<http://www.cisco.com/en/US/products/ps12077/index.html>

Cisco ME 3600X Switch

<http://www.cisco.com/en/US/products/ps10956/index.html>

Cisco ME 3600X-24CX Switch

[http://www.cisco.com/en/US/prod/collateral/switches/ps6568/ps10956/data\\_sheet\\_c78-708663.html](http://www.cisco.com/en/US/prod/collateral/switches/ps6568/ps10956/data_sheet_c78-708663.html)

Cisco ME 3800X Switch

<http://www.cisco.com/en/US/products/ps10965/index.html>

## Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS and Catalyst OS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

Cisco Feature Navigator is updated regularly and when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/cfn>

## Cisco IOS Software Documentation Set

The Cisco IOS Release 15.6S documentation set consists of configuration guides, command references, and other supporting documents and resources. For the most current documentation, go to the following URL:

[http://www.cisco.com/en/US/products/ps13594/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps13594/tsd_products_support_series_home.html)

## Notices

The following notices pertain to this software license.

### OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

### License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).

#### **OpenSSL License:**

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:  
“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)”.



THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

**Original SSLeay License:**

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

“This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”.

The word ‘cryptographic’ can be left out if the routines from the library being used are not cryptography-related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”.

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY

THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

---

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Copyright © 2015 Cisco Systems, Inc. All rights reserved.

---