Release Notes for Cisco IOS Release 15.4S

First Published: November 21, 2013
Last Updated: March 19, 2018
Release: Cisco IOS Release 15.4(3)S9
Part Number: OL-30834-08

Introduction

These release notes support Cisco IOS Release 15.4S up to and including Cisco IOS Release 15.4(3)S9 and are updated as needed to describe new features, bugs, and related documents. Cisco IOS Release 15.4S 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 15.4S 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.

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

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

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 15.4S 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

Cisco ASR 901 Router

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

http://www.cisco.com/en/US/products/ps12077/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/en/US/partner/products/ps12667/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/en/US/products/ps10956/index.html

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

http://www.cisco.com/en/US/products/ps10965/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

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/en/US/prod/collateral/switches/ps6568/ps10956/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
15.4(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

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

http://www.cisco.com/en/US/products/hw/routers/ps368/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/en/US/products/ps12077/prod_installation_guides_list.html

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

http://www.cisco.com/en/US/products/ps10956/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/en/US/products/ps10956/prod_installation_guides_list.html

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

http://www.cisco.com/en/US/products/ps10965/tsd_products_support_install_and_upgrade.html

For Cisco IOS upgrade ordering instructions, go to the following location:

http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/957_pp.htm

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS 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 15.4S releases.

Limitations and Restrictions in Cisco IOS Release 15.4(3)S

- There are no new limitations and restrictions in Cisco IOS Release 15.4(3)S.

Limitations and Restrictions in Cisco IOS Release 15.4(2)S

- There are no new limitations and restrictions in Cisco IOS Release 15.4(2)S.

Limitations and Restrictions in Cisco IOS Release 15.4(1)S

There are no new limitations and restrictions in Cisco IOS Release 15.4(1)S.

New Features and Important Notes

Features and Important Notes for Cisco IOS Release 15.4(3)S

These release notes describe the following topics:

- New Hardware Features in Cisco IOS Release 15.4(3)S1, page 13
- New Software Features in Cisco IOS Release 15.4(3)S1, page 13
- New Hardware Features in Cisco IOS Release 15.4(3)S, page 13
- New Software Features in Cisco IOS Release 15.4(3)S, page 13
- New Hardware and Software Features supported on Cisco 7600 Series Routers in Cisco IOS Release 15.4(3)S, page 15
- New Hardware and Software Features supported on Cisco ASR 901 Series Routers in Cisco IOS Release 15.4(3)S, page 15
- New Hardware and Software Features supported on Cisco ASR 901 S Series Routers in Cisco IOS Release 15.4(3)S, page 16
- New Hardware and Software Features supported on Cisco ME 3600x and Cisco ME 2600x Series Ethernet Access Switches in Cisco IOS Release 15.4(3)S, page 16
- MIBs, page 16
- Important Notes, page 16

New Hardware Features in Cisco IOS Release 15.4(3)S1

There are no new hardware features in Cisco IOS Release 15.4(3)S1.

New Software Features in Cisco IOS Release 15.4(3)S1

There are no new software features in Cisco IOS Release 15.4(3)S1.

New Hardware Features in Cisco IOS Release 15.4(3)S

There are no new hardware features in Cisco IOS Release 15.4(3)S.

New Software Features in Cisco IOS Release 15.4(3)S

This section describes new and changed features in Cisco IOS Release 15.4(3)S. Some features may be new to Cisco IOS Release 15.4(3)S but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.4(3)S. Links to feature modules are included. If a feature listed does not have a link to a feature module, that feature is documented only in the release notes.

Autonomic Config Download

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

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/auto_net/configuration/15-s/an-auto-net-15-s-book/an-auto-net-infra.html

BFD Support for Multicast(PIM)

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

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipmulti_pim/configuration/15-s/imc-pim-15-s-book/imc_bfdpim.html

BGP - 4-byte AS RD and RT Support (RFC5668)

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/irg-4byte-asn.html

BGP- Subcodes for BGP Cease Notification

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/irg-max-prefix.html

CFM Extension for 1+1 Hot-Standby Support

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

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cether/configuration/15-s/ce-15-s-book/ce-cfm-nsnhsby.html

CFM Low Latency

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

http://www.cisco.com/c/en/us/td/docs/wireless/asr_901/Configuration/Guide/b_asr901-scg/b_asr901-scg_chapter_0101111.html

FHRP - HSRP - Hot Standby Router Protocol V2

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

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/15-s/fhp-15-s-book/HSRP-Version-2.html

HSRP: Global IPv6 Address

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

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/15-s/fhp-15-s-book/HSRP-Global-IPv6-Address.html

IPv6 Routing: OSPFv3 Authentication Support with IPsec

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

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/15-s/iro-15-s-book/ip6-route-ospfv3-auth-ipsec.html

IPv6 Routing: RIP for IPv6 (RIPng)

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

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_rip/configuration/15-s/irr-15-s-book/ip6-rip.html

IPv6 Services: Extended Access Control Lists

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

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_acl/configuration/15-s/sec-data-acl-15-s-book/ip6-acls.html

TWAMP RFC Compliance

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

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipsla/configuration/15-s/sla-15-s-book/sla_twamp.html

VRF Aware BGP Translate-update

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/vrf-aware-bgp-translate-update.html

VRRPv3 Protocol Support

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

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/15-s/fhp-15-s-book/VRRPv3-Protocol-Support.html

New Hardware and Software Features supported on Cisco 7600 Series Routers in Cisco IOS Release 15.4(3)S

For detailed information about hardware and software features supported on Cisco 7600 Series Routers in Cisco IOS Release 15.4(3)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 15.4(3)S

For detailed information about hardware and software features supported on Cisco ASR 901 Series Routers in Cisco IOS Release 15.4(3)S, see the following document:

http://www.cisco.com/c/en/us/td/docs/wireless/asr_901/Release/Notes/asr901_rn_15_4_3_S.html

New Hardware and Software Features supported on Cisco ASR 901 S Series Routers in Cisco IOS Release 15.4(3)S

For detailed information about hardware and software features supported on Cisco ASR 901 S Series Routers in Cisco IOS Release 15.4(3)S, see the following document:

http://www.cisco.com/c/en/us/td/docs/wireless/asr_901s/rn/b_rn_for_asr901s_15_4_3s.html

New Hardware and Software Features supported on Cisco ME 3600x and Cisco ME 2600x Series Ethernet Access Switches in Cisco IOS Release 15.4(3)S

For detailed information about hardware and software features supported on Cisco ME 3600x and Cisco ME 2600x Series Ethernet Switches in Cisco IOS Release 15.4(3)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

http://www.cisco.com/c/en/us/support/switches/me-2600x-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. 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 15.4S:

- 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.
- Bulletins—You can find bulletins at http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/prod_literature.html.

Features and Important Notes for Cisco IOS Release 15.4(2)S

These release notes describe the following topics:

New Hardware Features in Cisco IOS Release 15.4(2)S2

There are no new hardware features in Cisco IOS Release 15.4(2)S2.

New Software Features in Cisco IOS Release 15.4(2)S2

There are no new software features in Cisco IOS Release 15.4(2)S2.

New Hardware Features in Cisco IOS Release 15.4(2)S1

There are no new hardware features in Cisco IOS Release 15.4(2)S1.

New Software Features in Cisco IOS Release 15.4(2)S1

There are no new software features in Cisco IOS Release 15.4(2)S1.

New Hardware Features in Cisco IOS Release 15.4(2)S

This section describes new and changed features in Cisco IOS Release 15.4(2)S. Some features may be new to Cisco IOS Release 15.4(2)S but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.4(2)S. To determine if a feature is new or changed, see the feature information table at the end of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes.

DWDM SFP+ Support on ES+ HD Line Cards for C7600 Platforms.

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

http://www.cisco.com/c/en/us/td/docs/routers/7600/Hardware/15_0s/7600_hwd.html

SPA-1xCHSTM1/OC3-V2

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

http://www.cisco.com/c/en/us/td/docs/interfaces_modules/shared_port_adapters/configuration/7600series/sipspasw/76cfstm1.html

SPA-2XT3/E3-V2 and SPA-4XT3/E3-V2

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

http://www.cisco.com/c/en/us/td/docs/interfaces_modules/shared_port_adapters/configuration/7600series/sipspasw/76cfgt3.html

SPA-2XCT3/DS0-V2 and SPA-4XCT3/DS0-V2

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

http://www.cisco.com/c/en/us/td/docs/interfaces_modules/shared_port_adapters/configuration/7600series/sipspasw/76cfgct3.html

New Software Features in Cisco IOS Release 15.4(2)S

This section describes new and changed features in Cisco IOS Release 15.4(2)S. Some features may be new to Cisco IOS Release 15.4(2)S but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.4(2)S. Links to feature modules are included. If a feature listed does not have a link to a feature module, that feature is documented only in the release notes.

Autoroute announce and forwarding adjacencies for OSPFv3 over IPv4 TE tunnels

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

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/15-s/iro-15-s-book/iro-ospf-autoroute.html

Auto-IP for SVI, Port-Channel & VRF

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

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_ipv4/configuration/15-s/ipv4-15-s-book/Auto-IP.html

BGP - Accumulated IGP

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-accumulated-igp.html

BGP PIC Edge for IP/MPLS

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/irg-bgp-mp-pic.html

BGP Signaling - VPLS interAS option B

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

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_l2_vpns/configuration/15-s/mp-l2-vpns-15-s-book/mp-vpls-bgp-sig-inter-as-option-b.html

IGMP Snooping

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

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipmulti_igmp/configuration/15-s/imc-igmp-15-s-book/imc_igmp_snoop.html

ISIS local microloop protection

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

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_isis/configuration/15-s/irs-15-s-book/irs-uloop-local-avoid.html

SLM over PoCH interfaces

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

http://www.cisco.com/c/en/us/td/docs/routers/7600/ios/15S/configuration/guide/7600_15_0s_book/y-1731PM.html

New Hardware and Software Features supported on Cisco ASR 901 Series Routers in Cisco IOS Release 15.4(2)S

For detailed information about hardware and software features supported on Cisco ASR 901 Series Routers in Cisco IOS Release 15.4(2)S, see the following document:

https://www.cisco.com/c/en/us/td/docs/wireless/asr_901/Release/Notes/b-901-rn-15-4-2.html

New Hardware and Software Features supported on Cisco ASR 901 S Series Routers in Cisco IOS Release 15.4(2)S

For detailed information about hardware and software features supported on Cisco ASR 901 S Series Routers in Cisco IOS Release 15.4(2)S, see the following document:

https://www.cisco.com/c/en/us/td/docs/wireless/asr_901s/scg/b_scg_for_asr901s.html

New Hardware and Software Features supported on Cisco ME 3600x and Cisco ME 3800x Series Routers in Cisco IOS Release 15.4(2)S

For detailed information about hardware and software features supported on Cisco ME 3600x and Cisco ME 3800x Series Routers in Cisco IOS Release 15.4(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. 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 15.4S:

- Field Notices and Bulletins, page 20

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.
- Bulletins—You can find bulletins at http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/prod_literature.html.

Features and Important Notes for Cisco IOS Release 15.4(1)S

These release notes describe the following topics:

- New and Changed Information, page 21
- MIBs, page 24
- Important Notes, page 24

New and Changed Information

This section lists the new hardware and software features supported on different platforms in Cisco IOS Release 15.4(1)S and contains the following subsections:

- New Hardware Features in Cisco IOS Release 15.4(1)S2, page 21
- New Software Features in Cisco IOS Release 15.4(1)S2, page 21
- New Hardware Features in Cisco IOS Release 15.4(1)S1, page 21
- New Software Features in Cisco IOS Release 15.4(1)S1, page 21
- New Hardware Features in Cisco IOS Release 15.4(1)S, page 22
- New Software Features in Cisco IOS Release 15.4(1)S, page 22
- New Hardware and Software Features supported on Cisco ASR 901 Series Routers in Cisco IOS Release 15.4(1)S, page 24
- New Hardware and Software Features supported on Cisco ASR 901 S Series Routers in Cisco IOS Release 15.4(1)S, page 24
- New Hardware and Software Features supported on Cisco ME 3600x and Cisco ME 3800x Series Routers in Cisco IOS Release 15.4(1)S, page 24

New Hardware Features in Cisco IOS Release 15.4(1)S2

There are no new hardware features in Cisco IOS Release 15.4(1)S2.

New Software Features in Cisco IOS Release 15.4(1)S2

There are no new software features in Cisco IOS Release 15.4(1)S2.

New Hardware Features in Cisco IOS Release 15.4(1)S1

There are no new hardware features in Cisco IOS Release 15.4(1)S1.

New Software Features in Cisco IOS Release 15.4(1)S1

There are no new software features in Cisco IOS Release 15.4(1)S1.

New Hardware Features in Cisco IOS Release 15.4(1)S

There are no new hardware features in Cisco IOS Release 15.4(1)S.

New Software Features in Cisco IOS Release 15.4(1)S

This section describes new and changed features in Cisco IOS Release 15.4(1)S. Some features may be new to Cisco IOS Release 15.4(1)S but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.4(1)S. Links to feature modules are included. If a feature listed does not have a link to a feature module, that feature is documented only in the release notes.

BGP - EVPN / PBB_EVPN route-reflection

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

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/15-s/bgp-l3vpn-evpn-rr-support.html

BGP - IPv6 NSR

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

http://www.cisco.com/en/US/docs/routers/7600/ios/15S/configuration/guide/7600_15_0s_book.html

BGP - RTC for legacy PE

For detailed information about this feature, see the following document:
http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/15-s/irg-bgp-rtc-for-legacy-pe.html

BGP GSHUT enhancement

The BGP Graceful Shutdown (GSHUT) Enhancement feature enables graceful shutdown of either all neighbors or only virtual routing and forwarding (VRF) neighbors across BGP sessions. The following command has been introduced in this feature: **bgp graceful-shutdown all**.

BGP Monitoring Protocol

The BGP Monitoring Protocol (BMP) feature enables configuration and monitoring of BMP servers, establishing connection with the BMP clients, and monitoring and reporting of all configured BGP neighbors. The following commands were added or modified for this feature:

1. The “bmp-activate” keyword was added to the **neighbor** command.
2. The **bmp** command was added.
3. The **bmp server** command was added to enable bmp-server configuration sub-mode under router configuration mode.

Cisco 8-Port Channelized T1/E1 Shared Port Adapter (SPA-8XCHT1/E1-V2)

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

http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/install_upgrade/7600series/SIP-SSC-SPA-HW-Install.html

IOS VRF Multicast Multi-Topology Support

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

http://www.cisco.com/en/US/docs/ios-xml/ios/mtr/configuration/15-s/vrf-support-mtr.html

IPV6 VACL (Vlan Access Control List)

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

http://www.cisco.com/en/US/docs/routers/7600/ios/15S/configuration/guide/7600_15_0s_book.html

ISIS local microloop protection

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

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_isis/configuration/15-s/irs-uloop-local-avoid.html

LMM support over PoCH on 7600

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

http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap4.html

Multicast MT mode in VRF

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

http://www.cisco.com/en/US/docs/ios-xml/ios/mtr/configuration/15-s/vrf-support-mtr.html

Multi-Topology BGP with VRF enhancement

The Multi-Topology BGP with VRF enhancement feature enables multi- topology BGP routing in VRF. There are no new BGP commands introduced or modified for this feature. If multi-topology BGP is configured, the **address-family (ipv4 | ipv6) multicast** command under a specific “vrf definition” is used for configuration; else all multicast VRF activity is configured using the **address-family (ipv4 | ipv6)** command under “vrf definition”.

OSPFv2 IP FRR Local Microloop Avoidance

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

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/configuration/15-s/iro-ospfv2-ip-frr.html

VPLS over rLFA-FRR on 7600

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

http://www.cisco.com/en/US/docs/routers/7600/ios/15S/configuration/guide/isis_lfa_ipfrr.html

VRF aware BGP translate-update

The VRF aware BGP translate-update feature enables customer devices, that contain an old version of Cisco software that does not support multicast BGP routing, to advertise its routes to multicast VRF-Lite, multicast VPN for VPNv4 and VPNv6 neighbors, as well as through IPv6 over IPv4 tunnel. The “neighbor” command is modified to include the “translate-update” keyword that enables this feature and applies only to the VRF address families.

New Hardware and Software Features supported on Cisco ASR 901 Series Routers in Cisco IOS Release 15.4(1)S

For detailed information about hardware and software features supported on Cisco ASR 901 Series Routers in Cisco IOS Release 15.4(1)S, see the following document:

http://www.cisco.com/en/US/docs/wireless/asr_901/Release/Notes/asr901_rn_15_4_1_S.html

New Hardware and Software Features supported on Cisco ASR 901 S Series Routers in Cisco IOS Release 15.4(1)S

For detailed information about hardware and software features supported on Cisco ASR 901 S Series Routers in Cisco IOS Release 15.4(1)S, see the following document:

http://www.cisco.com/en/US/docs/wireless/asr_901s/rn/b_release_notes_for_asr901s.html

New Hardware and Software Features supported on Cisco ME 3600x and Cisco ME 3800x Series Routers in Cisco IOS Release 15.4(1)S

For detailed information about hardware and software features supported on Cisco ME 3600x and Cisco ME 3800x Series Routers in Cisco IOS Release 15.4(1)S, see the following document:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.4_1_S/release/notes/ol31008.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. 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 15.4S:

- Field Notices and Bulletins, page 25

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.
- Bulletins—You can find bulletins at http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/prod_literature.html.

Bugs

Bugs for Cisco IOS Release 15.4(3)S

Open and 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 and go to 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:

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

- Resolved Bugs—Cisco IOS Release 15.4(3)S5, page 44
- Open Bugs—Cisco IOS Release 15.4(3)S4, page 45
- Resolved Bugs—Cisco IOS Release 15.4(3)S4, page 46
- Open Bugs—Cisco IOS Release 15.4(3)S3, page 48
- Resolved Bugs—Cisco IOS Release 15.4(3)S3, page 49
- Resolved Bugs—Cisco IOS Release 15.4(3)S2, page 51
- Resolved Bugs—Cisco IOS Release 15.4(3)S1, page 53
- Open Bugs—Cisco IOS Release 15.4(3)S, page 53
- Resolved Bugs—Cisco IOS Release 15.4(3)S, page 55

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 Bug Search Tool Help & FAQ
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.

Resolved Bugs—Cisco IOS Release 15.4(3)S9

Table 1 Resolved Bugs—Cisco IOS Release 15.4(3)S9

Caveat ID Number	Description
CSCsv05154	Cisco IOS HTTP server vulnerable to CSRF attacks
CSCui67191	Cisco IOS XE Software Ethernet Virtual Private Network Border Gateway Protocol DOS Vulnerability
CSCun88463	Router reload due to memory corruption with IP SLA
CSCuo87952	Line card FPD upgrade struck, and card FPD status in 'wait' state.
CSCus34406	dmvpn tunnel goes down when removing secondary ip from tunnel source int
CSCus73337	stack stby reloaded by stack-mgr due to active/stdby config out of sync
CSCut45453	icmpv6 reply are blocked
CSCuv80858	byte counters for a port-channel show interface is inaccurate
CSCuw73525	3650 DHCPv6 Guard does not block rogue DHCP server to provide IPv6 addr
CSCux24141	MET mis-programming results in unwanted multicast after switchover
CSCuy14110	CPU Spike seen due to VTEMPLATE BKG OW Process.
CSCuy38144	Protocol Other counted up when executing "show int accounting"
CSCva18762	IGMP packets looping between Active & Standby SP CPU
CSCvb14640	Cisco IOS and Cisco IOS XE Software IPv6 SNMP Message Handling Denial of Service Vulnerability
CSCvc54886	Asr1k(SPA-1XCHSTM1/OC3): Router down after receiving invalid spa ipc-message
CSCvd01613	DSCP value get remarked on the ES+ 10g line cards
CSCvd02153	Router crash due to mpls/ospf config on interface.
CSCvd19860	OSPFv3 AUTH breaks IPv6 traffic intermittently

Caveat ID Number	Description
CSCvd42785	Multicast forwarding when OIF is Null in 7600
CSCve48453	eBGP vrf next-hop setting behaviour is changed by CSCuv07111.
CSCvf12081	Cisco IOS XE Software Verbose Debug Logging Information Disclosure Vulnerability
CSCvf29111	7600 stack low crash
CSCvf74829	CRL download fails due to "failed to create getcacert message"
CSCvf81579	ASR1K: IOSd crash in kmi_initial_check on null map dereference
CSCvg00110	MET table depletion in 7600
CSCvg06443	VPNMAP table depletion in 7600
CSCvg09008	Online Diagnostics detected a Major Error
CSCvg53836	router crashed when MPA with source vlan 1-4094 created
CSCvg84667	Mishandling of udp pkts (that are destined to RP) at 7600 ES+ NP, when BFD is hardware offloaded
CSCvh02536	XE3.16.6B-ES: pmsi_tunnel label value seen as explicit null on downstream PE
CSCvh21686	ES+HD (76-ES+XT-8TG3CXL) LC ports sharing a channel stop forwarding when a port is admin shutdown

Resolved Bugs—Cisco IOS Release 15.4(3)S8

Table 2 Resolved Bugs—Cisco IOS Release 15.4(3)S8

Caveat ID Number	Description
CSCvb61075	ASR920: Dual-rate EEM errors out when hostname has a dot '.' character
CSCvc89965	After reload route policy processing not re-evaluate with route-map using match RPKI
CSCvc58538	BGP crashes when removing advertise-map
CSCuw35828	crash w/BGP show advertised-routes when route-server is on vrf
CSCvd90251	Duplicate BGP prefixes are not dropped
CSCvd09584	eVPN PMSI VNI decoding / encoding as MPLS label
CSCvd16828	High CPU due to periodic route refresh to VPN peers using rtfilter AF
CSCva86436	no export ipv4 unicast map triggered router to crash
CSCva24325	NSF/SSO feature not honouring TCP MSS
CSCvc31517	Router crashes using BGP commands for long cost extended community string
CSCve51657	Slow convergence with scale after a core link flaps
CSCvd43437	Wrong Source IP Selection for eBGP in EVN/VNET environment
CSCve57697	Crash in Bstun SNMP code
CSCvb30567	C7600 ES+ stuck TOD counters for Y.1731 measurements

Caveat ID Number	Description
CSCva34374	ipv6 traffic over bridge-domain carrying on few ports only
CSCve66601	Crash in CISCO-SLB-EXT-MIB code
CSCut87808	Crash While Accessing CallManager XML Config
CSCuz87695	SCCP Phones on CME not forwarding video packets on outbound calls
CSCux18010	Cisco Networking Services Sensitive Information Disclosure Vulnerability
CSCuw77959	1801M - %DATACORRUPTION-1-DATAINCONSISTENCY: copy error
CSCva00899	C841M crashes randomly during execution of the reload EEM script.
CSCvb59372	Double-free of VTY context causes a software-forced crash
CSCux15954	EEM : fatal condition error from operating system
CSCvc98571	EEM applet will not release the Config Session Lock if it ends when CLI is in configuration mode
CSCva42638	Traceback is seen when a EEM script runs
CSCvc44866	3850/3650 - ssh/vty sessions lock up leading to loss of access to device
CSCut77951	Arp entry changes to an encap type of 802.1Q
CSCvc77378	Glare condition exists for mid call DO INVITE when CUBE receives in-dialogue SIP OPTIONS message
CSCva80218	IOS-XE router crashed due to possible memory leak issue due to CCSIP_SPI_CTRL
CSCvb08960	ezvpn client config dissapears from dialer int when pppoe session flaps
CSCve10917	IPSec crash on ASR1k router while processing KMI
CSCvd40880	Modifying crypto ACL leads to a removal of crypto map config
CSCvb94392	Cisco IOS and IOS XE System Software SNMP Subsystem Denial of Service Vulnerability
CSCuz15131	dqueue not empty prior to destruction crashes ipv4fib_les_switch_wrapper
CSCvd97524	Fixed versions for CSCuz15131 crash when traffic with maximum size is on wire
CSCvb25357	NHRP registration requests failed after ipv6 tunnel source change
CSCvb65892	ISDN process crashed unexpectedly
CSCve60376	Crash in ADSL DMT SNMP code
CSCvc15923	L2TP Account accuracy: SSS disconnect ACKs are not received for few sessions
CSCvb41889	NTP leap second inserted every day after leap second occurs
CSCuw97889	Incorrect CLI output after netconf edit-config
CSCuz95908	Memory leak due to path querry with Null outgoing interface
CSCva38391	CVE-2016-1550: NTP security against buffer comparison timing attacks
CSCuz94245	IGP-LDP sync interoperability for OSPF multi area adj
CSCuv69650	OSPF Virtual-link using the lowest cost path
CSCut21950	3560 / RBAC / Unable to exclude enable command.
CSCuv04247	3850 config-sync failure on standby w/ 'no shut' on wlan
CSCuw53025	Cat3850 reports "Error, ECI has run out of event blocks" message

Caveat ID Number	Description
CSCus23013	show cmd under "parser view include-exclude" cause standby router to reload
CSCuz22162	Digital certificates does not sync to standby
CSCva66819	Non-Vlan1 did not get initiated with pnp startup-vlan conf after reload
CSCuw60955	non-vlan1 doesn't seem to initiate in Beni-MR3
CSCux52544	PnP Fails to Initiate with Non-VLAN1 Feature Configured
CSCuw15272	PNP: non-vlan 1 zero-touch upgrade does not work
CSCut25533	PnPA: non-vlan CLI should only apply to newly bootup devices
CSCvc80135	Crash when removing and re-adding bandwidth remaining percent while class-default has fair-queue
CSCvd23034	Multiple Parent Events Per Node lead to a crash
CSCvc56422	XE316:NIM serial interface flaps after soft OIR with traffic
CSCuy08656	SNMP Traps leading a leak in CHUNK functions
CSCve60402	Crash in Voice DNIS SNMP code
CSCve21448	multiple ISR4K VGW's crashed with Segmentation fault(11), Process = DSMP
CSCvb97638	CCSIP_SPI_CONTROL memory usage leads to crash - SIP subscribe messages
CSCvc99971	Cisco Router 2921 sending cisco-rtp payload 121 for RFC2833 (rtp-nte) instead of 101.
CSCvc86595	HTTP 304 response causes mc error and bad magic

Open Bugs—Cisco IOS Release 15.4(3)S8

Table 3 Open Bugs—Cisco IOS Release 15.4(3)S8

Caveat ID Number	Description
CSCux26195	"aaa accounting suppress null-username" not working as expected
CSCvd69608	Asr1k crashes at PPP process on pushing 4 or more per-user static ipv6 routes
CSCve54313	Crash in ALPS SNMP code
CSCuw97842	Standby RP crash at be_ancp_get_dsl_line_attrs
CSCva00765	crash after no ipv4 multicast multitopology command
CSCvf10260	7600 - ACL not programmed upon configuration changes - all incoming packets processed by CPU
CSCts36318	7600: Native Vlan not removed from trunk port
CSCvd86374	ES20 module crash after FRR object is freed then accessed
CSCvc68496	Discrepancy in number of ACEs in active and Standby after CoA
CSCun31438	Abnormal Call Disconnection due under load due to DP errors
CSCux41072	EIGRP sending hello messages with interface in passive mode.

Caveat ID Number	Description
CSCvb86484	wrong EIGRP redistribution statement in startup config breaks BGP settings atfer router reload
CSCuv74256	IOS: HMAC key miscalculated with DH Group 21 and IPSec PFS enabled
CSCve13491	Router might crash due watchdog when creating a new swidb at if_index_allocate_index
CSCva55916	CUBE crash in resolve_sig_ip_address_to_bind NULL ccb
CSCuv08835	IPSEC key engine process leaks /w dynamic crypto map in scaled scenario
CSCuv14856	WATCHDOG timeout crash during IPSEC phase 2
CSCuv51788	GM Router failed to register after reload.
CSCup84620	"show crypto isakmp stats" should print dropped IKE messages
CSCup90021	IKEv1 periodic DPDs sent per IPsec SA, not per IKE
CSCvc21452	ASR903:ISIS routes are set with Max Metric due to IGP LDP Sync
CSCvc82325	Crash after the MPLS LDP neighbor flap in the NSR scenario
CSCvf21718	ASR1K crash when running 'show ip nhrp vrf ... detail'
CSCvc65670	NTP leap second addition/deletion for consecutive leap months not working properly
CSCuz62898	Crash in BGP due to regular expressions
CSCvf24928	QFP exmem memory leak in cpp_fm_sce_result_chunk
CSCuv02537	ASR1K ESP200 reload in a B2B CGN NAT scenario with PAP+BPA
CSCux93752	SRST Double Ringback heard on blind transfer to PSTN
CSCuv74171	crash on command "show snmp view"
CSCve46273	%TRANSCEIVER-3-RPC_FAILED: Application error (rc = 3)
CSCux86075	Unexpected crash during SSH operation
CSCvb72458	Router repeatedly crashing with "%UTIL-3-TREE: Data structure error"
CSCuu71299	MPLS LDP flap with %TCP-6-BADAUTH: No MD5 digest
CSCve66658	Crash in TN3270E-RT-MIB code
CSCva08142	IOSd crash on LISP enable router
CSCva00551	Cisco Router may crash on SIP MA Process Due to sstrncpy()
CSCuz72665	DATACORRUPTION-1-DATAINCONSISTENCY error when copying from PAI header

Resolved Bugs—Cisco IOS Release 15.4(3)S7

Table 4 Resolved Bugs—Cisco IOS Release 15.4(3)S7

Caveat ID Number	Description
CSCva47253	AAA crash on multiple username deletions - Part 2
CSCvb64818	ASR1k/ISG : 3.13.6 : Crash due to bad id in id_to_ptr when sending Accounting to non-existing group
CSCvc42499	Function radius_message_authenticator_decode
CSCuy76789	16.2 Throttle: UDP Packets are getting dropped with nat64+ZBFW configs
CSCuw66787	Clear ip nat translation vrf X impacts vrf Y
CSCvb95069	FTP Passive mode: NAT door limit being exceeded
CSCvb62767	NATed packets are dropped by ALG_PROCESS_TOKEN_FAIL due to NAT door limit being exceeded
CSCuz93698	PPTP Traffic issue with Carrier Grade NAT on IOS-XE
CSCva86436	no export ipv4 unicast map triggered router to crash
CSCva24325	NSF/SSO feature not honouring TCP MSS
CSCva25965	Router may crash after multiple show ip bgp sum/neighbor
CSCuv69297	Catalyst 3850: SSH/VTY session hangs on show run or other show commands
CSCvc33619	Major error status seen on card WS-X6748-GE-TX
CSCva61877	IPv6 neighbor discovery packet processing behavior
CSCvb69386	Controller SPA-1CHSTM1 OC3V2 goes into wedge state after excess controller flaps
CSCva94139	IPv6 neighbor discovery packet processing behavior with SIP-400
CSCva91655	FIB recursive loop crash
CSCuz81292	IPv6 neighbor discovery packet processing behavior
CSCuh23818	HTTPS Secure server script crashed iosd and reloads with traceback
CSCuv97379	[ST-P] STBY router crashed on disconnecting call on ACTIVE
CSCuy30957	For IPv6:Activate Under GDOI Fail-Close Disappears on Reboot
CSCva62029	Crash observed on GM when rekey message received from Key server
CSCvb94852	IKEV2 Default Proposal Reset After Reload
CSCva61415	Unable to initiate IKE sessions due to mismatch in CAC counters
CSCvb29204	BenignCertain on IOS and IOS-XE
CSCva44179	IKEv1 DPD delete logic causes stale phase 2
CSCuz42299	Crash when configuring CWS
CSCut45177	CWS HTTPs traffic fails to load on ISR configured with NVI
CSCva18067	CPU HOG and Crash by MFIB_rate
CSCuz28618	sup2t: sup crashed after MFIB errors
CSCva43443	DNA/SA,Upon Quad SUP SSO,Mcast decap traffic black holing for ~50 sec
CSCva59927	UCI,On QuadS6T Second SSO,PIM joins are not encapsulating over VRF LISP
CSCva99279	RSP3:Labels not getting assigned in spite of having free label space
CSCva97469	VA stuck in protocol down state after failing to establish IPSec session

Caveat ID Number	Description
CSCux99025	Evaluation of Cisco IOS and IOS-XEl for NTP January 2016
CSCux46898	NTP associations vulnerability
CSCvb19326	NTP leap second failure to insert after leap second occurs
CSCvb00272	OSPFv3 IPSEC socket session is not coming up after reboot
CSCvb66420	PFR Sync Issues between MC and Border router ,active probes are missing on border router randomly
CSCvb96706	Client auth and enroll to subca fails
CSCuy13701	IOS PKI: Crash while editing a VRF aware TP with enrollment profile
CSCuv44053	PKI Rollover: rollover cert is being added as active id cert
CSCvb73018	PKI: Cannot import RSA SubCA signed by ECDSA
CSCva15013	AAA/RADIUS memory leak on IOS-XE
CSCuz87179	Crash observed while bringing up PTA sessions in SSS Manager
CSCva67564	No V-Cookie in accounting stop due to idle timeout or manual clearing
CSCuz57124	Tracebacks *MSG 00001 TRUNCATED* on standby, after PTA Sess brought up
CSCvb24139	H225 Sanity Check Failure
CSCuz82533	Router crashed when the virtual access interface comes up
CSCuo75126	Ucode crash seen with Firewall configs in B2BHA setup
CSCva65990	'sh police int' hidden command causes RP to crash
CSCuz76821	tableid_ha: Memleak @ eobc_pool_getbuffer
CSCva37519	stale flowmgr entry during ipv6 tacacs transaction leads to crash
CSCuy38157	Router crash during handling L2 and L3 subscribers at the same time
CSCuv41355	Unable to telnet -- No wild listener: port 23
CSCuh09324	udp entries not deleted from flowmgr table
CSCuz03079	ISR-4K Processing Error: H323 Setup parameter "mediaWaitForConnect TRUE"
CSCva22751	Router crashing due to a watchdog in the ISDN process
CSCvb24266	ISR 4K Crashes When Running "Debug Voice Translation"
CSCva00015	STBY SBC router crashing multiple times
CSCvc19209	SIP session between VXML GW and the Nuance server remains active after callback (CCB) is scheduled
CSCvb90483	VXML GW hardening changes for ICBC memory corruption issue

Open Bugs—Cisco IOS Release 15.4(3)S7

Table 5 Open Bugs—Cisco IOS Release 15.4(3)S7

Caveat ID Number	Description
CSCux26195	"aaa accounting suppress null-username" not working as expected
CSCuu36200	Radius auth fails if ip radius source-interface vrf default in startup
CSCvb05362	RP crashed - UNIX-EXT-SIGNAL: Segmentation fault(11), Process = ANCP HA
CSCuz21435	IOS-XE: 'ACE event' process watchdog crash.
CSCus85112	CGN, QFP: Show cmd display incorrect NAT trans stats for per-host IP add
CSCup57389	Traffic drops while testing VRF Lite coexistance with SP NAT for LNS
CSCuw97842	Standby RP crash at be_ancp_get_dsl_line_attrs
CSCul15273	AN Link local Tunels not deleted after no autonomic is issued
CSCuo97277	iosd crashed at bfd_chkpt_create_and_send_msg
CSCvc12039	ASR903/RSP1B&RSP3C 3sec to 10sec loss on RSP switchover when SSO enabled
CSCut40990	BGP:send-community inheritance when explicit configuration match default
CSCva00765	crash after no ipv4 multicast multitopology command
CSCus04010	dmvpn hub router crashes when clearing bgp peers
CSCus19601	IPV6 RR not changing Next-hop for a IPV6 prefix
CSCuq27095	Memory leak in BGP table if terminate at show bgp af summary auto more
CSCup33405	Prefixes from GR peer not removed from BGP table when peer goes down
CSCvb22903	RP3 fails to clear SA in the large scale IPSec SCM configuration
CSCup01258	sh ipv6 dhcp pool command display wrong output after router reload
CSCva13768	ISR 4K|PPPoE Interface|Not Forwarding all IP fragments
CSCun31438	Abnormal Call Disconnection due under load due to DP errors
CSCux41072	EIGRP sending hello messages with interface in passive mode.
CSCvb86484	wrong EIGRP redistribution statement in startup config breaks BGP settings atfer router reload
CSCur72967	43xx/44xx "show platform software cerm-information" not accounting pkts
CSCuv74256	IOS: HMAC key miscalculated with DH Group 21 and IPSec PFS enabled
CSCtw50974	ASR/ISR4K DTMF 2833 to 2833 Not Working with MTP CoLocated and OOB+2833
CSCut79286	ASR1K QoS feature doesn't work fine with RP2/Rls3.x
CSCup26658	Unexpected Process Restart after "no spanning tree", "default interface"
CSCuw43115	CSR1Kv XE 3.13.3S Crashed on clearing ip ospf process
CSCva55916	CUBE crash in resolve_sig_ip_address_to_bind NULL ccb
CSCuq17104	CUBE disconnecting a call after call transfer due to Hold timer
CSCuu12283	CUBE failed to create DP session on STBY for Webex flow
CSCuw39465	During a transfer CUBE doesnt update the media to the Recording server
CSCuq24354	GETVPN KS rekeys without pol changes may cause IOS XE GMs to re-register
CSCuv08835	IPSEC key engine process leaks /w dynamic crypto map in scaled scenario

Caveat ID Number	Description
CSCux16726	ipv6 OSPFv3 crypto session doesnt come UP after reload
CSCuj53943	Multicast packets are dropped after "clear crypto gdoi ks members"
CSCvc78492	Unable to pass traffic if spoke to spoke fails to build in phase 2
CSCuv51788	GM Router failed to register after reload.
CSCuu41857	Incorrect GDOI registration backoff timer calculation after crash/reload
CSCup84620	"show crypto isakmp stats" should print dropped IKE messages
CSCup90021	IKEv1 periodic DPDs sent per IPsec SA, not per IKE
CSCun72450	IPv6 GETVPN traffic dropped after un-configure then re-configure VRF
CSCvb65892	ISDN process crashed unexpectedly
CSCul24766	Core files are corrupt - crc error
CSCuy03680	V3Lite IGMP packets sent instead of V3 when UDP based feature is present
CSCur10311	MAG does not accept PBA without GRE key during de-registration
CSCvc21452	ASR903:ISIS routes are set with Max Metric due to IGP LDP Sync
CSCuv00547	CRASH SEEN AFTER FLAPPING MPLS INTERFACES
CSCuq95663	CENT: small increase in IPC still exists in longevity
CSCuz22260	ISR G2: unexpected byte lost with PfRV3 and NBAR based QoS integration
CSCvb92697	High CPU due to NHRP when NHRP cache entry for remote spoke's tunnel address is deleted
CSCux80450	%REGISTRY-3-STUB_CHK_OVERWRITE: error seen during boot up
CSCvc65670	NTP leap second inserted every day after leap second occurs
CSCvb48912	SNMP crashes getting ntpAssociationEntry with low/fragmented memory condition
CSCuz62898	Crash in BGP due to regular expressions
CSCuv69650	OSPF Virtual-link using the lowest cost path
CSCum19502	Inconsistent behavior between telnet and ssh in low memory conditions
CSCus23013	show cmd under "parser view include-exclude" cause standby router to reload
CSCva72564	Customer POC- Autoinstall obtained IP overrides USB bootstrap config
CSCuw24373	Called-station-id and NAS-ID via account profile satus query
CSCun96847	IOS-XE : Zone mismatch vulnerability in Zone Based Firewall
CSCux52451	VRF Domain half open counter increments when aggressive aging occurs
CSCuv02537	ASR1K ESP200 reload in a B2B CGN NAT scenario with PAP+BPA
CSCvb77570	ASR1K: Crash after upgrade to 3.16.3 at transmit_pkt_marmot_spa_d
CSCuw95297	ESP200 crash with 550K translations with cablevision config
CSCux68096	ucode crash abort called from ipv4_nat_create_inside_addrport_bind
CSCva95830	HQF not cleaned after invalid policy applied to vlan-manual GEC subintf
CSCtx83808	PPP: Traceback when changing police to shaper on LNS
CSCum03909	mvpnv6 mldp router crash on _be_ipv6_pdb_remove_ipdb_private
CSCux93752	SRST Double Ringback heard on blind transfer to PSTN

Caveat ID Number	Description
CSCup04090	asr920 throws error messages on snmp polling of a couple of MIBs
CSCuv74171	crash on command "show snmp view"
CSCux86075	Unexpected crash during SSH operation
CSCvb72458	Router repeatedly crashing with "%UTIL-3-TREE: Data structure error"
CSCuy74990	BGP not forming neighborship on ASR1k with dual RP
CSCuu71299	MPLS LDP flap with %TCP-6-BADAUTH: No MD5 digest
CSCva08142	IOSd crash on LISP enable router
CSCvc81332	ASR Cube crashed @ AFW_M_Connection_EventPreProcess
CSCvb97638	CCSIP_SPI_CONTROL memory usage leads to crash
CSCva00551	Cisco Router may crash on SIP MA Process Due to sstrncpy()
CSCuz72665	DATACORRUPTION-1-DATAINCONSISTENCY error when copying from PAI header
CSCux16650	SHA-2 support on ISR G2

Resolved Bugs—Cisco IOS Release 15.4(3)S6a

This is a special release in Cisco IOS software that addresses Cisco Product Security Incident Response Team (PSIRT) caveats.

Table 6 Resolved Bugs—Cisco IOS Release 15.4(3)S6a

Caveat ID Number	Description
CSCvb29204	BenignCertain on IOS and IOS-XE
CSCuv87976	CLI Knob for handling Leap second Add/delee ignore/ handle
CSCux46898	NTP associations vulnerability
CSCvb19326	NTP leap second addition is not working during leap second event

Open Bugs—Cisco IOS Release 15.4(3)S6

Table 7 Open Bugs—Cisco IOS Release 15.4(3)S6

Caveat ID Number	Description
CSCva15013	AAA/RADIUS memory leak on IOS-XE
CSCva00765	crash after no ipv4 multicast multitopology command
CSCva82501	FNF crash during multiple config

Caveat ID Number	Description
CSCva55916	CUBE crash in resolve_sig_ip_address_to_bind NULL ccb
CSCuu12283	CUBE failed to create DP session on STBY for Webex flow
CSCva71545	Under load crash seen@CCSIP_UDP_SOCKET process in XE3.16 image
CSCva62029	Crash observed on GM when rekey message received from Key server
CSCuy03680	V3Lite IGMP packets sent instead of V3 when UDP based feature is present
CSCuy13701	IOS PKI: Crash while editing a VRF aware TP with enrollment profile
CSCuo75126	Ucode crash seen with Firewall configs in B2BHA setup
CSCuy74990	BGP not forming neighborship on ASR1k with dual RP
CSCva08142	IOSd crash on LISP enable router
CSCva00551	ISR 4K Crash on SIP MA Process Due to sstrncpy()
CSCva00015	STBY SBC router crashing multiple times

Resolved Bugs—Cisco IOS Release 15.4(3)S6

Table 8 Resolved Bugs—Cisco IOS Release 15.4(3)S6

Caveat ID Number	Description
CSCuz48415	"aaa authentication suppress null-username" not working as expected
CSCuw86386	AAA crash when removing TACACS servers
CSCuy21675	Crash@username_command with service pwd-encryption & common-criteria cfg
CSCux69225	Mac filtering option "None" sends blank password
CSCuy01051	MPLS VPN over mGRE Routing issue after reload
CSCuz82218	TACACS Enable authentication fails with null pre shared key
CSCuy03054	ASR1K IOSd may crash in BGP Accepter process due to segmentation fault
CSCux55351	ASR1K router crashed due to running BGP with AIGP
CSCux70093	BGP RR does not advertise vpnv6 prefixes even all RT filters are learnt
CSCuy20481	Crash due to stale pointer after removing vrf command export AF map
CSCux76332	Deleting a statement in export map, removes other statement
CSCux96029	GR Non-restarting peer does not advertise VPN routes default RT filter
CSCuy03504	Incorrect prefix count upon clearing bgp peering
CSCuz58682	Incorrect VPN withdraw with overlapping RT on multiple RT Filter
CSCuz21061	router crashes after %BGP-6-BIGCHUNK + SNMP query.
CSCux62094	Routes are not exported from vrf to global due to incorrect export limit

Caveat ID Number	Description
CSCuw66752	"SSM connection manager" high CPU if VAIs under scale have QOS applied
CSCuy79944	call-home crash because calling XOS API in interrupt level
CSCuw06084	DTMF not getting recognized on ISR G3 when using TCL Script
CSCux60876	Memory corruption due to DHCP
CSCux49494	'allow connections' or 'telephony-service' config is required on ISR4k
CSCuz56699	ISR 4k Paging over SIP / FXS phones have no audio
CSCuy38707	After RSP switchover, BFD hangs for up to 10 minutes before converging
CSCuw48118	ASR920 - crash in bcopy called from 'addnew' during reassembly
CSCux29974	ISR4k:UnconfiguredIpv4Fia drop seen for pkts transit via PPPoE
CSCuz12967	Crash after show ip protocols vrf with RIP enabled
CSCuy48358	Crash during SIP subscribe notify ACK
CSCuz47777	DTMF issue on ISR G3/ASR during the prompt using TCL Script
CSCuy40672	One way audio in a DODO call after transfer with REFER disabled
CSCuz71250	Router crashes when parsing ack for mid call
CSCuz69975	Under load crash is seen in CVP REFER_PASSTHRU scenario
CSCuw23947	For IPv4: Activate Under GDOI Fail-Close Disappears on Reboot
CSCuy43118	XE316: HubBR might be crashed@tunnel_protection_validate_shared_profile
CSCuu44128	GETVPN on ASR with vasi interface fail to install the Rekey
CSCuz14788	New reg invoke PKI function breaks the GETVPN CRL Checking feature
CSCuv31981	ISR Router Crashes When Trying to Delete a Freed SA
CSCuz99865	IPSec MIB queries results in memory leak and shows wrong SNMP value.
CSCuz25240	ISIS not installing back to RIB neighbors loopback when interface flaps
CSCux29806	ISIS routes are not not installed in the routing table from isisdatabase
CSCuz35203	SSM connection manager crash during VFI pseudowire bind
CSCuq32410	"Seg fault @ mLDP Process"&Crash@nile_mc_handle_prefix_L3_and_not_L2
CSCuy02409	BDI not Passing VRRP Multicast Traffic
CSCuz39721	ASR1K/RP2/SW 15.4(3)S4 crash
CSCux78294	Crash on router when removing L2VPN
CSCus72718	L2TPv3 session pending between 2 devices
CSCux58640	LDP NSR: Label Mapping Messages Not Sent on RP SSO and VCs Re-bind
CSCuw65792	CWS not associating CN with nested groups when "," (comma) is used
CSCuw65059	mfib on the line card stuck in Connecting state
CSCuv02246	With access interface flap, traffic doesnt switch back to data mdt.
CSCuv37022	Extranet MVPN traffic is getting dropped & not switched to data MDT
CSCuy87734	ASR1K RP crashes LCON Main process when heavily loaded
CSCva17339	LDP session stuck in established with no TCP connection
CSCuy71712	FlexVPN: Spoke spawns a virtual access to connect to the hub

Caveat ID Number	Description
CSCuy04757	Crash@ospfv3_router_process_mgd_timers on shut/no shut of sub-intf
CSCuy32709	R-LFA Tunnels not established on setting DS required attribute
CSCux19034	XE3.16 crashes when conf "distribute-list" under router ospf and sh run
CSCuo61229	ASR1002 Crashed after "show pfr master active running"
CSCux20613	Bus error crash at oer_saa_mc_get_probe_stats_cbk
CSCuw57225	PFRv2 not work well for 10% inbound load-balance
CSCuy22067	PfRv2 stream keep remaining in DEFAULT state
CSCuy85870	Wrong TD next-hop for overlapping prefixes
CSCur10056	Memory leak in SSS Manager
CSCuw79412	%SYS-6-STACKLOW: Stack for process PPP SIP running low, 0/6000
CSCuo76385	Router crashes at ic_dp_classify when Serial link flaps
CSCuz99848	Memory exhaustion traceback due to large and complex configuration
CSCva28875	NAT ALG fails on Multipart SIP Header
CSCuw50415	Crash seen @ hwidb_iftype_unlist while doing unconifg of channel-group
CSCuw55717	Memleak @ pak_pool_cache_item_get : Scaled TFEX
CSCuy55849	RTR installs the ISIS(or OSPF) route with Higher Metric in the RIB
CSCuz76295	MPLS-TE FRR packet drops during re optimization.
CSCuy38709	Memory leak with watcher_create_common.
CSCux82377	ASR 1K ISG Router Crashes When Polling "csubSessionEntry" MIB
CSCuy69440	ISG Critical Exception and crashing with SSS-Manager holding memory
CSCuz62915	ISR4451 crash under load due to Segmentation fault(11), Process = DSMP
CSCuy65330	RSVP Reservation Failure Causes Call Drop on Voice to Video Calls
CSCus45019	Media loop detection failure
CSCuj50209	Memory leak @ voip_rtp_recv_fs_input
CSCuy14532	rtp/rtcp media activity timer doesn't trigger when only 1 rtp leg drops
CSCux54794	Configuration under the E&M voice-ports are missing after the reload
CSCuy16501	Static noise introduced on FXO after IOS upgrade
CSCva30483	IOS-XE 4321 Router crash with BRI interface going down
CSCuz52693	ISR 4K Memory Holding in CCSIP_SPI_CONTROL
CSCus03761	Stack overflow crash @ ip_epm_proxy_slow_check.
CSCuy83854	deb voip application vxml with 1 cvp call caused buffer overflow
CSCuz17364	DTMF Type ahead buffer on GW with Nuance not working
CSCuu25704	Memory corruption in the IO pool when a t38 fax gateway receives t37 fax

Open Bugs—Cisco IOS Release 15.4(3)S5

Table 9 Open Bugs—Cisco IOS Release 15.4(3)S5

Identifier	Description
CSCux44606	Name ACL for Multicast Boundary Stops Working Upon Reload
CSCux33568	ESP crash while reconfiguring FR interface to MFR bundle
CSCux07224	ASR1K crash with OTV due to L2BD FIB entry change
CSCux59115	ASR1002-X Crash with dpidb_tableid_params_initialize
CSCux93176	ASR1k:stby RP stuck while bootup
CSCur48133	ATM 3xOC3 SPA failed to program with IFCFG_CMD_TIMEOUT error

Resolved Bugs—Cisco IOS Release 15.4(3)S5

Table 10 Resolved Bugs—Cisco IOS Release 15.4(3)S5

Identifier	Description
CSCuw89522	ASR IOSD crash because of AVC feature
CSCuw13407	PfRV3: transport bytes expected counters overflow and not expected
CSCuv79776	Router with Pfr feature crashed at cpp_free_exmem
CSCuw30599	ISR4331-B: traceback occured when enabling Ethernet Data Plane Loopback
CSCuv84600	Netflow packets are dropped when EPC is enabled
CSCux29703	ASR1000-2T+20X1GE fails to boot on router reload with SPA-3-NULL_BAY_PTR
CSCuu48458	ASR1k/15.4(3)S QinQ frames are dropped under "TCAM Failure Drops"
CSCux55692	TCAM Errors in NL11k TCAM of Fixed Ethernet Linecards
CSCuw98135	ZBFW HA not replicating sessions when matching based upon L4 proto/port
CSCuw21897	Traceback seen with ip cef accounting
CSCux57066	ASR1K : Lawful Intercept not working as expected for IPv6 traffic
CSCux02656	ASR1K: Crash related to collecting NetFlow data for IPv6 flows
CSCuw36887	Crash with with Flexible Netflow enabled
CSCuw78755	IOS-XE need not require appxk9 license to support per-tunnel DMVPN QoS
CSCup91567	ASR1001-X boot-loops with CMCC crash and XGM MAC10 block errors
CSCux01133	interface counter stuck on build-in interfaces in ASR1001X
CSCux43951	Packet drops on built-in 1Gig ports of ASR1001-X
CSCuv26762	ASR1001X HMAN generating error msg when reading /proc/cpuinfo
CSCux42411	ASR1001-X Frame Relay with Fortitude NIM fails due to LMI packet padding
CSCuv93130	Cisco IOS-XE 3S platforms Series Root Shell License Bypass Vulnerability
CSCup70353	IOS-XE router reload due to WebUI log file leak
CSCuw49798	ASR1K: cpp_cp_svr core@cpp_qm_cmn_delete_queue

Identifier	Description
CSCuw94014	cpp_cp crashes with BB profile #6 48k PTA
CSCut49714	GEC:QoS: pkt buff util high after apply/remove flat policy w/ fair-queue
CSCuw81487	Kahuna RP crash when bringing up PTA sessions with QoS
CSCuw73223	Polaris : cpp_cp_svr crash when the interface goes down
CSCux10321	ASR1000 CLI hangs on executing the "show platform hardware qfp xxx"
CSCud50181	SBC srtp ucode crash doing srtp-rtp interworking
CSCuu45832	STUN packets not handled properly by CPP SBC module in ASR CUBE
CSCuw71226	Call stuck in a deactivating state (CUBE-SP)
CSCut78545	delegate registration failed after password change

Open Bugs—Cisco IOS Release 15.4(3)S4

Table 11 Open Bugs—Cisco IOS Release 15.4(3)S4

Identifier	Description
CSCuv07111	IOS and IOS-XE devices changing the next-hop on BGP route with own IP
CSCup33405	Prefixes are not removed from BGP table with BDI interface shut
CSCut79286	ASR1K QoS feature doesn't work fine with RP2/Rls3.x
CSCuw09483	Unexpected reload w/"privilege exec level '0-15' show macdb" configured
CSCuu12283	CUBE failed to create DP session on STBY for Webex flow
CSCuu26224	CUBE with SRTP fallback will crash when call hit on incoming dial-peer 0
CSCuv61208	ASR1k EasyVPN server looses RRI for clients behind PAT
CSCuw02157	DMVPN Hub: IOS crash at crypto_ipsec_show_map_info
CSCuq24354	GETVPN KS rekeys without pol changes may cause IOS XE GMs to re-register
CSCuw09323	GETVPN: ASR GM stops decrypting until old SA expires after KS ACL change
CSCuw08567	Ident SM exists without Dynamic Crypto Map leading to rekey failures
CSCuj55363	lispgetVpn traffic is dropped when getvpn profile is applied in wan intf
CSCuj53943	Multicast packets are dropped after "clear crypto gdoi ks members"
CSCus85701	AQoS peer mismatch with NAT
CSCuv66070	Crash on executing "show nhrp group-map" command
CSCuv86821	Router crashed due to Crypto IKMP
CSCuv21051	XE310:Traceback@crypto_isakmp_profile_free after unconfiguration
CSCuv94186	SNMPWALK crash at ipsmIPSec_policyOfTunnel
CSCuv79429	IPSEC: static reverse-route is removed after retransmissions in IKMP
CSCun72450	IPv6 GETVPN traffic dropped after un-configure then re-configure VRF
CSCuv59898	Kernel Watchdog crash at ktime_get
CSCus62778	Stale Data MDT entry

Identifier	Description
CSCuq95663	CENT: small increase in IPC still exists in longevity
CSCuv74171	crash on command "show snmp view"
CSCup31575	HTTPS : Back to Back POST request fails
CSCus06158	ISR4x/ISR3x: Mask IOS-XE SSLVPN syntax from configuration
CSCuw14345	High CPU due to "IP Connected Rou" process and Low Memory .

Resolved Bugs—Cisco IOS Release 15.4(3)S4

Table 12 Resolved Bugs—Cisco IOS Release 15.4(3)S4

Identifier	Description
CSCus21322	Adding NAS_IPV6_ADDRESS in the Sanet
CSCut27272	CPUHOG and crash due to Auth Manager process
CSCur59242	Crash due to tplus_client_stop_timer
CSCuu59324	router crashes @aaa_memerase
CSCus82903	BGP - %IPV6_ADDRESS-3-NULLIDB: Uninitialized interface pointer
CSCuu85298	FIB/LFIB inconcistency after BGP flap
CSCuv66776	MQC Policy-map counters do not update in T3/E3 SPA
CSCur68351	%COMMON_FIB-4-FIBIDBMISMATCH when configuring sub-int for port-channel
CSCur35098	cmfib line card crash
CSCut42214	High memory & CPU utilization on mfib-const-lc Pr process
CSCuv39005	Supervisor crash after configuring NetFlow on a BGP PIC enabled router
CSCuv15500	TCAM utilization increasing up to 100%
CSCuu50392	aaa attr list leak at dsensor_process_pkt_update_cache
CSCuv39338	ISG: DHCP Server RADIUS Proxy Memory Leak
CSCut10251	Some commands are not in running-config after AUTOINSTALL finishes
CSCus25205	Traceback@eigrp_process_dying during unconfiguration
CSCut12738	[ASR1K HSRP] Physical Link Failure Causes HSRP to Fail
CSCuu68439	Crash after no route-target import command
CSCut28445	CSCur47160 broke load balancing
CSCuu26303	Router crash triggered by service policy and ipv6 traffic
CSCus65125	Router crash with NAT @ ipnat_for_us_feature
CSCut80144	Beni MR1: Debug enabled by default on Mingla
CSCuv19154	After upgrade of IOS-XE software, appnav functionality maybe impacted.
CSCuv83793	AppNav-XE drop packets when traffic from WAAS has wrong ID
CSCuu82763	Evaluation of ciscossl in binos for OpenSSL June 2015 vulnerabilities
CSCur32628	7600 mis-programming causing intermittent packet loss

Identifier	Description
CSCuu80048	interface IP address change cause leaked routes in exported vrfs
CSCuv43978	IPv6 GRE over 6PE does not work properly
CSCuv80943	MCP_DEV:Packet drops@Ipv6NoRoute with ipv6gre configs
CSCut24140	Old active not coming up after first sso also seeing a traceback.
CSCuu28199	[Amur-MR3]IOSD crash reported@spi_iosd_ipc_process_inbound_mts_msg
CSCuu29667	ASR1K crash when snmp setting cipSecTunnelEntry
CSCus92857	Crypto Stateless redundancy causing "IPSEC install failed" after preempt
CSCuu54392	Different Tunnel Protection with shared profile cannot be used
CSCut87217	GETVPN - ASR1K GM deny policy fails when the policy is updated by the KS
CSCur29582	IPSEC-VPN: removal of "crypto-map" kills BFD session forever
CSCus79972	Crash on 'tunnel protection ipsec profile profile-name'
CSCut14502	Address pool leak upon Anyconnect reconnect and subsequent disconnect
CSCuu93699	Crash on IKEv2 cluster hub when anyconnect client tries reconnect
CSCut32445	Crash - IPSec/ISAKMP Timer driven crash.
CSCus30128	RRI dynamic L2L after client change ip address Ipsec rekey lost routes
CSCuv26780	Memory leak when qos pre-classify is configured with Crypto
CSCuj13127	SSTE: DNS IPv6 traffic fails with IKEv2 and ZBFW configured
CSCut88270	Duplicate hsrp vmac entries after OTV AEDs fail over
CSCut30167	ISIS may crash when reaching LSPFULL condition with IPv6 routes
CSCuu77927	OTV stuck in inactive status when failover due to missing isis vlan tlv
CSCup51000	CEMoUDP: PW interface still being unprovisioned, retry later
CSCuv56754	EoMPLS xconnect remains "RECOVERING" after RP SSO on egress
CSCuv29418	Router is continuously switching between active and standby EoMPLS PW
CSCuu50269	RSP2: MSPW sessions down on S-PE after SSO
CSCuu92194	RSP3:HSPW PW-Group Switchover results in traffic blackhole with no scale
CSCuv34896	VPLS autodiscovery PW failed to comeup when BGP recovers from failure
CSCuu36041	VPLS BGP AD resignalling time takes ~20-40s for multi-homing scenario
CSCuq70725	LDAP Address Error at ldap_clear_transaction_all
CSCuu88964	ASR1K Kernel crash at pidns_get()
CSCtz61014	f Linux kernel NTP leap second handling could cause deadlock
CSCuu12600	SR is not working fine in mk2fc2-sup720 device
CSCuu90695	DM/SM boundary (S,G) are not repopulated: Multicast Missing Registration
CSCur70478	Software crash at ldpx_mem_reallocz_grow due to insufficient memory
CSCuv61750	ASR903 MCP_DEV: Mismatch in VC label programming, EoMPLS scenario
CSCuu76169	PfRV3: Collocated hub MC/BR keep on publish site-prefix with enter-pfx
CSCuv83586	PI25: channel flapping with NBAR based QoS Policy for NTT
CSCut85551	Crash with DMVPN NHS using FQDN

Identifier	Description
CSCut77619	APRIL 2015 NTPd Vulnerabilities
CSCuv65370	Avoid any action on Leap SEcond indictor flag for non-leap second months
CSCup81878	Line by Line Sync fails while deleting dynamic NTP peer
CSCus34757	bgp rpki: crash if bgp default received
CSCus68229	Memory leak in OSPFv3R
CSCut63500	dot1q encapsulation causes vam2+ to crash
CSCut96721	Crash on pfr master router at oer_mc_apc_changed_prefix
CSCuu08872	Crash on pfr master router at pfr_exp_send_tc_config_internal
CSCus13902	Failure seen in OER Border router functionality
CSCuv22992	PFR router crashes due to watchdog when displaying config
CSCuu98524	PFR/OER related IOS crash
CSCuu97977	Pfrv2 load-balance not working with passive mode.
CSCuu18348	IOS PKI HA fails to initialize on standby router after reload or upgrade
CSCuu81737	Router crashes when using crypto
CSCut22660	Session in attempting state on standby when method list is default
CSCur88124	default throttling require other defaults in some cases
CSCut67877	IOS crashes when changing tunnel destination on a Tunnel with QoS
CSCuu46604	Router crashes when a failed primary link comes back up
CSCuq75576	Input queue wedged on outside interface of standby nat-ha router
CSCuo93893	RG-Infra: Add a hook for RG Domain for Reloading peer event:
CSCuu82607	Evaluation of all for OpenSSL June 2015
CSCut46130	MARCH 2015 OpenSSL Vulnerabilities
CSCus06143	CSR1k SSLVPN: Mask unsupported virtual-template type VPN from config
CSCut65242	ISG passing traffic while configured default drop should be used
CSCuu75354	ISG: Dedicated session provisioning failure post lite session conversion
CSCut87425	CPU hog in "EEM TCL Proc" after TCL script termination with long runtime
CSCuv51901	ASR1K BGP send UPDATE don't observe the TCP OPTION
CSCul10482	TFEX: Image auto download fails due to "ip tftp source-interface" config
CSCus46844	802.1x 3650 Radius Response not picked up by AAA code

Open Bugs—Cisco IOS Release 15.4(3)S3

Table 13 Open Bugs—Cisco IOS Release 15.4(3)S3

Identifier	Description
CSCut04815	LDAP authentication is not working on 5760 or 3850
CSCuu36031	Kernel crash is related to a GPF related to memory corruption.

Identifier	Description
CSCut12738	[ASR1K HSRP] Physical Link Failure Causes HSRP to Fail
CSCur32628	7600 mis-programming causing intermittent packet loss
CSCuu32159	CUBE issue with webex HA
CSCuu00050	CUBE with SRTP fallback is dropping SRTP RTP/SAVP from the 200 OK SDP
CSCur35618	[XE 3.15] FP Crashed for SRTP Video Call + DSP
CSCuu29667	ASR1K crash when snmp setting cipSecTunnelEntry
CSCut14502	Address pool leak upon Anyconnect reconnect and subsequent disconnect
CSCut30167	ISIS may crash when reaching LSPFULL condition with IPv6 routes
CSCue32350	kron crash after deconfiguring the occurance
CSCus62778	Stale Data MDT entry
CSCur70478	Software crash at ldpx_mem_reallocz_grow due to insufficient memory
CSCuq95663	CENT: small increase in IPC still exists in longevity
CSCut67137	Memory fragmentation on ASR903 due to OSPF
CSCuu24757	ASR1k QFP leak with cpp_sp_svr at module FM CACE
CSCuo51601	ISR4400 - Traffic incorrectly forwarded through class class-default
CSCus06143	CSR1k SSLVPN: Mask unsupported virtual-template type VPN from config
CSCup04062	IOS SSLVPN - Anyconnect Data traffic failure with TLS transport
CSCur10056	Memory leak in SSS Manager
CSCus77343	DSMP crash while doing OIR or module reload when active call exists
CSCut66144	VXML GW fails to handoff call to VXML Application on second VRU leg

Resolved Bugs—Cisco IOS Release 15.4(3)S3

Table 14 Resolved Bugs—Cisco IOS Release 15.4(3)S3

Identifier	Description
CSCut09164	Memory leak in AAA/EAP code in 3.3.5
CSCut31678	Memory leak in AAA/EAP code in 3.3.5
CSCur57035	ASR 1k crash on __be_bfd_fib_nh_change_cb
CSCuq09320	ASR-1002 crashed with LAN BFD and HSRP with ipv4 and ipv6
CSCus20997	ASR1k: BGP Notification of Admin shutdown triggers Graceful-Restart
CSCur66140	Import of Global routes to VRF will fail
CSCun68322	Support BGP GR for VPN AF in platform without MPLS
CSCus26146	VRF LISP routes not exported to global table with valid next hop
CSCus01544	XE3.13 rejects routes from ebgp peer due to malformed ATTR-SET attribute
CSCus54365	Memory leak in tlv_calloc
CSCur87549	ipv6 traffic over bridge-domain not working

Identifier	Description
CSCur88455	7600 IP FRR: MPLStoMPLS traffic Blackhole after VRF Configuration
CSCut31584	c7600 drops Register-Stop messages resulting into punting ASM stream
CSCut27149	POS FRR issue with traffic loss around 1 sec instead of 50ms
CSCus95226	Compact Flash corruption due to call-home directory being created
CSCus38037	crash with "show voice class ctl-file"
CSCut92745	Crash while placing MLPP calls
CSCur70959	Memory leak @ sipContentObjPvtSetBody
CSCus65095	SSTE: QoS Pre-classify was broken
CSCus34949	DHCP defect - crash due to an invalid access to a freed memory structure
CSCur55365	50% ping failure with IPv6 dual stack and dialer configured
CSCus72257	50% ping failure with IPv6 dual stack and dialer configured
CSCus57583	ASR 1K BGP Process Crash Due to EIGRP Route Redistribution
CSCup52101	EnergyWise Denial of Service vulnerabilty
CSCut01967	crashed after executed show ethernet cfm errors
CSCus53146	ASR crashes at hal_get_next_packet
CSCur43251	POODLE protocol-side fix: HTTPS Client
CSCur49548	Upgrade from 3.4.6S to 3.13.0S doesn't work with traceback and error log
CSCus86256	uCode crash when MPLS packet received on LAN side of AppNav intercept
CSCut46126	MARCH 2015 OpenSSL Vulnerabilities
CSCut30579	Dynamic PBR policy inconsistent & never update after path failover
CSCus78750	6RD: Knob to disable security check missing.
CSCur96943	CCSIP_SPI_CONTROL leak in sippmh_parse_record_route
CSCus75907	Router crashes when Fax T38 Protocol Configured
CSCur68999	config change on Tunnel int using shared tunnel protection stops traffic
CSCuq15567	Crash with %SYS-3-OVERRUN with crypto_ipsec_clear_peer_sas
CSCup97873	IPSec datapath should not print debug messages without debugs enabled
CSCuq91734	NHRP Packets are dropped after EzVPN decryption
CSCur29861	Traceback seen on c2900 platform for ike_keepalives
CSCur65486	GETVPN: Fail to delete GMs on sec-KS after 3 scheduled rekeys failure
CSCun57148	High CPU in FNF Cache Ager P
CSCus74192	Link down event does not flush the routes correctly with isis
CSCut24465	Static VFI went down after PTF reset
CSCus89274	Crash with nat/reflective acl and TCP session going through that box
CSCus69732	IOS-XE: Evaluation of glibc GHOST vulnerability - CVE-2015-0235
CSCut57290	Egress LER TTL propagation misbehaviour in per-ce label allocation mode
CSCuo67247	High CPU due to NHRP process on ASR in DMVPN ph3 after upgrading IOS-XE
CSCur28336	Memory leak and possible crash when using a logging discriminator

Identifier	Description
CSCus05038	"revocation-check ocsp none" does not timeout fast for unreachabl server
CSCus77875	List Headers leak verified cert chain Held CCSIP_TLS_SOCKET & Chunk Mgr
CSCus73553	Memory corruption crash in PKI certificate processing
CSCus54238	PKI "revocation check crl none" does not fallback if CRL not available
CSCut17865	ASR1K:13RU IOSd crash @PnP Agent Discovery after router reload
CSCus46259	ASR1k (ISG Radius-Proxy): Memory Leak after excessive client roaming
CSCut26988	Broken bw repartition - traffic is send as w/o configured bw under MQC
CSCut46705	Wrong bandwidth distribution in SIP 200 & 400 causes queue limit of 2
CSCur20444	I/O memory leak due to DHCPv6 packets.
CSCun29420	Crash observed with active IP SLA probes
CSCuq39109	Memory Fragmentation due to IP SLA
CSCus40410	ATM SPA: Incorrect SOM-COM-EOM flag set in packet buffer hdr in Ingress
CSCus88868	IOS openssl leak observed with SSL Anyconnect VPN
CSCuq25323	DLSW peers fail to connect when other DLSw peer sends FIN instead of RST
CSCue88982	MA2b:Supervisor crash seen upon Remote login and the session is idle
CSCut08626	DSMP crash at DSP packet buffer allocation
CSCuu29539	voice statistics CLIs are missing in ISR4k image
CSCut18365	Tracebacks found @ moh_multicast_recv_input
CSCus89791	g722-64 codec crash during dial tone with country code

Resolved Bugs—Cisco IOS Release 15.4(3)S2

Table 15 Resolved Bugs—Cisco IOS Release 15.4(3)S2

Identifier	Description
CSCur51387	NG3K stack: standby gets reloaded due to reason "configuration mismatch"
CSCur13587	ANCP session terminated due to message len check
CSCuq83441	BGP L2VPN uses default static next-hop instead of outging intf-addr
CSCuq99797	BGP Route-Target not advertised when rtfilter address family in use
CSCur66140	Import of Global routes to VRF will fail
CSCup48874	IPv6 neighbor link-local address not learnt after RSP Failover
CSCun68322	Support BGP GR for VPN AF in platform without MPLS
CSCus01544	XE3.13 rejects routes from ebgp peer due to malformed ATTR-SET attribute
CSCue87829	Bridge Domain EVC EFPs not mapped to VLAN post Reload/SSO
CSCun80617	Active SP crashes @ mfib_pltf_entry_extract_source followed by RP crash
CSCur94457	AToM traffic is blackholed after RP switchover
CSCur41785	IXP_MAP-3-QOS_CONFIG: ACL is not programmed after reload or RP SSO
CSCur96372	l2protocol forward feature is missing under SIP400

Identifier	Description
CSCum59931	7200 crash with DHCP suspending WCCP
CSCur10249	ASR1006 crash when IPv6 PPPoE sessions increase to several hundred
CSCup99634	IPV6 dhcp database not working on PI25 and Xe3.13
CSCuq78983	RIPv2 key-chain CLI disappears when doing config replace
CSCur11538	ASR1k lldpMIB walk (1.0.8802.1.1.2.1.3.7.1) , but lldpMIB unsupported
CSCur45606	logging discriminator doesn't work
CSCup99438	MK2:tun_decap_tinfo_control subsys missing in DFC
CSCur78068	Quad+fex mk2 (fc):after issu LV - IPC trace back, sw2(ICS) is crashed
CSCuq17828	ASR: Radius Accounting fails when using EDCSA certs
CSCur23619	IKEv2 reconnect radius accounting stop should mention terminate cause
CSCur85771	ISDN Segmentation Fault on ISR 4451
CSCuq51439	ASR903: ISIS LSP generation delayed after receiving BFD down event
CSCur97045	IS-IS Passive-interface default unavailable
CSCum90471	ASR1k: Ping failure b/w CE1 & CE3 after Switchover.
CSCur78744	LISP mobility with HSRP invalid host detection events
CSCuq85667	Crash@mcast_rw_link_dequeue on config replace in MCAST THS
CSCur36464	mVPN: Inter-AS Option B: Different RDs: proxy vector: local RD is picked
CSCur09682	Router crashes in PIM due to infinite recursion at ip_set_mdb_flag
CSCuo81912	SSTE: Unable to remove performance-monitor once the interface is deleted
CSCup67317	max_chunk_size validation incorrect in funciton chunk_create_inline()
CSCup59760	'sh mpls fwding tabel vrf slot<>' takes longer time & stucks terminal
CSCur92862	TE leaks memory when restarting isis
CSCur07571	Processor memory leak with MRCP_Client at cc_api_get_call_active_entry
CSCur62553	Netconf - Duplicate xml version start tags in hello packet
CSCuq70163	RESTAPI: POST /api/v1/acl/{acl-id}/interfaces does not show in config
CSCus38393	ASR1k:IOSD crash @process_run_degraded_or_crash
CSCur10058	IOS PKI : CRL parsing may fail if HTTP Content-Length is not specified
CSCuq74176	PKI IOS removed valid CA certificate before expiry date
CSCur14783	PnP: ZTD in ISR's blocked due to config wizard
CSCun87941	PPP link interfaces causes SUP to crash
CSCus01735	cbQosTSCfgRate64 is not supported on ASR1k/IOSXE
CSCui23670	Even if show sup-bootdisk is executed, nothing is displayed.
CSCuc68034	IO Memory Leak on FlexWan WS-X6582-2PA exec 'sh cef interface internal'
CSCuo92155	RSVP sync process crash observed with TE NSR configs
CSCup80756	SNMP Engine Crashes in IOS-XE, Segfault When Processing rttMonStats MIB
CSCum87411	software install from tftp get failed fts_client issue
CSCur78381	After a reboot of SPA-4XCT3/DS0, first 4 packet loss in channelized mode

Identifier	Description
CSCuq74492	IOS/IOSd Multiple Vulnerabilities in OpenSSL - August 2014
CSCur44075	AC ICE+ ver <= 4.0 Client unable to connect to XE SSL Headend {CSR1K}
CSCun89616	IOS Does Not Properly Respond to TLS 1.2 Client Hellos
CSCup86552	Issue with qos service installation
CSCuq54260	Session is not syncing to the standby with collect identifier remote-id
CSCuh92882	XE3.11 Seginfo->l2hw_cond_debug is set to "1" when there is no condition
CSCur68259	XE3.13 : Subscribers not pingable after 2nd "clear ip route vrf x *"
CSCur29261	Memory courruption in retrans TCP sanity check causes ISR crash
CSCup41482	TCP snd window stuck with CEF enabled

Resolved Bugs—Cisco IOS Release 15.4(3)S1

All resolved bugs for this 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	15.4(3)S1
Status	Fixed
Severity	2 or higher

Open Bugs—Cisco IOS Release 15.4(3)S

This section describes possibly unexpected behavior by Cisco IOS Release 15.4(3)S. All the bugs listed in this section are open in Cisco IOS Release 15.4(3)S. This section describes only severity 1, severity 2, and select severity 3 bugs.

- CSCuo73442

  Symptom: A Cisco switch may crash after issuing the **no ip dhcp pool** command.

  Conditions: This symptom occurs when DHCP is configured.

  Workaround: There is no workaround.

- CSCup10266

  Symptom: IPv6 default route does not get redistributed into EIGRP without metrics.

  Conditions: This symptom occurs when redistribute static is issued without mentioning metrics.

  Workaround: Mention metrics when issuing the **redistribute static** command under EIGRP.

- CSCup11348

  Symptom: Incremental memory leaks are observed.

  Conditions: This symptom occurs under the following conditions:

  - TFTP server should not be reachable which is mentioned in the DHCP database.
  - Remove and add the DHCP pool.

  Workaround: There is no workaround.

- CSCup13169

  Symptom: The Default static route tag value does not get updated on OSPF.

  Conditions: This symptom occurs under the following conditions:

  1. Add static default route with tag value.
  2. Configure OSPF with redistribue static and default-information originate.

  The tag value does not get updated.

  Workaround: Create a separate route map for updating the tag value. Route map should be tagged with the **default-information originate** command under OSPF.

- CSCup26658

  Symptom: An unexpected process restart occurs after running the following commands in quick succession:

```
no spanning tree mode
default interface <intf>
```

  Conditions: This symptom occurs when service instances are configured on the interface with encapsulation and bridge-domain configuration under the interface. Spanning tree must also be configured before running the commands.

  Workaround: Leave a 10 second gap between entering the above mentioned commands.

- CSCup48742

  Symptom: A Cisco router gets crashed.

  Conditions: This symptom occurs under the following conditions:

  1. Configure the below CLI and make sure that the SCP server IP is unreachable:

```
ip dhcp database scp://tom:cisco@192.168.50.25/dhcp4 write-delay 60 timeout 5
```

  2. Wait for 60 seconds or the following message:

```
%DHCPD-3-WRITE_ERROR: DHCP could not write bindings to
scp://tom:cisco@192.168.50.25/dhcp4
```

  3. Make SSH connect from this device to the other device and exit from that connection so as to be back to the original device (optional).
  4. Press “Enter”.
  5. The following message appears:

```
[Resuming connection 1 to UNKNOWN ... ]
[Connection to UNKNOWN aborted: error status 0]
```

  6. The router would hang or crash. If not, run any show command (show ip int br).
  7. If all the above conditions are met, wait for the router to crash. Cisco ISR routers take around 5-10 minutes to crash and Cisco ASR routers crash immediately most of the times.

  Workaround: Use FTP or TFTP with “ip dhcp database”. Do not use SCP with “ip dhcp database”.

- CSCup54679

  Symptom: TE FRR paths are lost after an SSO.

Conditions: This symptom occurs under the following conditions:

1. TE tunnels are configured between PE1 and PE2.
2. TE NSR is configured on PE1 and FRR node protection is configured on PE1.

Before SSO, the FRR database shows the FRR paths and after SSO the FRR paths are lost.

Workaround: There is no workaround.

Resolved Bugs—Cisco IOS Release 15.4(3)S

- CSCee32792

  Symptom: A Cisco router reloads at snmp_free_variable_element while using SNMPv3 commands.

  Conditions: This symptom occurs while using SNMPv3 commands.

  Workaround: There is no workaround.

- CSCte77398

  Symptom: A Cisco ATM router configured with ATM PVC Range commands report the following error when attempting to configure a PVC Range:

  Unable to configure PVC Range. Possibly multiple users configuring IOS simultaneously.

  Conditions: This problem occurs randomly and even if there are no multiple sessions accessing the pvc-range at the same time.

  Workaround: There is no workaround.

- CSCtq21722

  Symptom: A Cisco switch may reload when configured for SNMP.

  Conditions: This symptom is observed when SNMP inform hosts are configured.

  Workaround: Remove the SNMP host configurations for SNMP informs.

  ```
  Example: no snmp-server host x.x.x.x informs version 2c <removed>
  ```

- CSCtx82890

  Symptom: After removing the encapsulation on MFR member interface, tracebacks are observed.

  Conditions: This symptom is observed when serial interface is configured with FR MLP configuration.

  Workaround: There is no workaround.

- CSCty92208

  Symptom: Customer faced crash on 6509 after configuring WCCP.

  Conditions: Customer configured WCCP with hash assignment and enabled port hashing and it will happen during redirection if packet are software switched.

  Workaround: The possible workarounds are:

  1. Disable port-hashing if we are using hash-assignment.
  2. Use mask-assignment method.

- CSCtz45833

  Symptom: A Cisco router crashes with the following message:

  ```
  Router crash: UNIX-EXT-SIGNAL: Segmentation fault(11), Process = MPLS TE LM
  ```

Conditions: This symptom occurs when a router acts as the mid point for MPLS-TE tunnels and performs an ERO expansion. In case the ERO expansion fails (due to IGP race conditions or inter-AS scenario) and backup tunnels are in use (for MPLS-TE FRR feature), the router may crash.

Workaround: Configure the head-ends to perform a full ERO computation to avoid mid points performing any ERO expansion. This can be done using the dynamic path option or by using the explicit path that specifies strict hops for each node along the desired LSP path (using "loose" hops or partial strict hops can lead to this issue).

- CSCuc60868

  Symptom: A router randomly crashes either due to memory corruption at bgp_timer_wheel or memory chunks near bgp_timer_wheel (For example, BFD event chunks if BFD is configured or AtoM Manager chunks if LDP is configured). A crash occurs right after an LDP neighbor is up in the L2VPN setup.

  Conditions: This symptom occurs when **vpls bgp signaling** is unconfigured and then reconfigured. Both L2VPN and BGP are unconfigured and reconfigured after all L2VPN and BGP data structures are fully deleted (about 3 minutes for 5 BGP VPLS prefixes). For the repro on file, OSPF (for IGP) is also unconfigured and reconfigured. Both LDP and BGP signalling are affected by this bug.

  Workaround: Avoid unconfiguring and reconfiguring BGP L2VPN.

- CSCue00996

  Symptom: The Cisco IOS Software implementation of the Network Address Translation (NAT) feature contains two vulnerabilities when translating IP packets that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

  Cisco has released free software updates that address these vulnerabilities.

  There are no workarounds to mitigate these vulnerabilities.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140326-nat

  Note: The March 26, 2014, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the March 2014 bundled publication.

  Individual publication links are in Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication at the following link:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar14.html

  Conditions: See the published Cisco Security Advisory.

  Workaround: See the published Cisco Security Advisory.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 7.1/5.9:

  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C

  CVE ID CVE-2014-2111 has been assigned to document this issue.

  Additional information on Cisco’s security vulnerability policy can be found at the following URL:

  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCue84703

  Symptom: When a switchover is triggered before the converge of a unicast (and multicast), the MFIB is not in “running state”, and is held in the initializing state forever.

  Conditions: This symptom occurs when a switchover is triggered before the converge of the unicast.

  Workaround: Switchover after the converge of the unicast.

- CSCuf51357

  Symptom: A vulnerability in the Secure Sockets Layer (SSL) VPN subsystem of Cisco IOS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

  The vulnerability is due to a failure to process certain types of HTTP requests. To exploit the vulnerability, an attacker could submit crafted requests designed to consume memory to an affected device. An exploit could allow the attacker to consume and fragment memory on the affected device. This may cause reduced performance, a failure of certain processes, or a restart of the affected device.

  Cisco has released free software updates that address these vulnerabilities.

  There are no workarounds to mitigate this vulnerability.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140326-ios-sslvpn

  Note: The March 26, 2014, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the March 2014 bundled publication.

  Individual publication links are in Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication at the following link:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar14.html

  Conditions: See published Cisco Security Advisory.

  Workaround: See published Cisco Security Advisory.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 7.8/6.4:

  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C

  CVE ID CVE-2014-2112 has been assigned to document this issue.

  Additional information on Cisco’s security vulnerability policy can be found at the following URL:

  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCug17485

  Symptom: A buffer leak is observed on a Cisco router.

  Conditions: This symptom occurs while using SSLVPN.

  Workaround: There is no workaround.

- CSCug45421

  Symptom: The standby RP crashes.

Conditions: Memory corruption occurs in certain cases when the following commands are executed in quick succession. It leads to a crash later when the memory is accessed. The issue is seen only with on-demand PVCs and when the commands are copied and pasted or executed using a script or tool.

```
configure terminal
interface ATM0/0/0.2 multipoint
range pvc 11/41 11/51
create on-demand
/* Prob commands begin */
pvc-in-range 11/45
exit
no pvc-in-range 11/45
/* Prob commands end */
end
```

Workaround: Do not execute the commands in quick succession.

- CSCuh05259

  Symptom: Prompt is provided for configure replace command when **file prompt quiet** is configured.

  Conditions: This symptom is observed when “file prompt quiet” has been configured.

  Workaround: Use “force” along with the **configure replace** command.

- CSCuh09324

  Symptom: UDP based entries are not deleted from the flowmgr table resulting in crash, or poor system response, with CPU hog messages being shown.

  Conditions: Affected Platforms - images

  – ct5760-ipservicesk9.bin

  – cat3k_caa-universalk9.bin

  – cat4500e-universalk9.bin

  Device is configured with UDP services that originate from the device. This includes but not limited to the following features:

  – TFTP

  – Energy Wise

  – DNS

  – Cisco TrustSec

  Workaround: If you suspect that you are affected by this bug, please do the following, for confirmation:

```
Router#config terminal
service internal
end
Router#show flowmgr
```

  The output of this command will show many lines entries holding with the same port numbers. Disabling the feature that is being held in the flows until an upgrade can be performed, is a workaround.

  A reload is required to clear the held flows.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5.4/4.5: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:H/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C

CVE ID CVE-2013-6704 has been assigned to document this issue.

Additional details about the vulnerability described here can be found at: http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2013-6704

Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCuh49066

  Symptom: VSS standby crashes due to LBL sync on issuing the below parser command:

  ```
  parser view li-view
  ```

  Conditions: This symptom occurs in a VSS with parser view configuration.

  Workaround: Remove the "parser view" configuration.

- CSCui05000

  Symptom: A Cisco router may crash upon importing a prefix into VRF after applying **no ipv4 multicast multitopology** under "vrf definition" for that VRF.

  Conditions: This symptom occurs while initially configuring the VRF. **address-family ipv4/6 multicast vrf** must be configured under "router bgp" mode before import route-targets are configured under "vrf definition" mode.

  Workaround: There is no workaround.

  More Info: If the crash does not occur, it is likely that importing of the prefix will not work.

- CSCui17084

  Symptom: Delay between VPN convergence and BGP-based MDT tunnel creation after router reload may cause multicast traffic loss.

  Conditions: In a BGP MVPN setup utilizing MDT SAFI, problem is seen upon BGP exiting read-only mode. VPN prefixes will be advertised immediately, whereas MDT prefixes are advertised after a BGP scanner run.

  Workaround: There is no workaround.

- CSCui63461

  Symptom: The Cisco router crashes when using CCP 2.6 and 2.7 to provision the device.

  Conditions: This symptom is observed under normal condition.

  Workaround: There is no workaround.

- CSCui64807

  Symptom: An active RP crashes during FIB sync because of memory overrun when the standby sup becomes unavailable.

  Conditions: This symptom occurs when redundant RPs are configured in SSO mode and the standby RP becomes unavailable (for instance because of crash or physical removal). The issue occurs only on Cisco 7600 RSP 720, Cisco 7600 Series Supervisor Engine 720, and Cisco 7600 platforms where the tableid "ISSU FOF LC" support is enabled. As of 03/17/2014, the tableid "ISSI FOF LC" feature is only supported on SY releases. This issue does not impact Cisco ASR 1000 Series platforms.

  Workaround: There is no workaround.

- CSCui79766

  Symptom: Upgrading hardware platform from Cisco 2811 Integrated Services Router to Cisco 2911 Integrated Services Router introduces periodic, intermittent delay in the delivery of STUN packets to OEM (Motorola) equipment.

  Conditions: This symptom occurs while upgrading hardware platform from Cisco 2811 Integrated Services Router to Cisco 2911 Integrated Services Router.

  Workaround: There is no workaround.

- CSCui83823

  Symptom: When CU executes “show tech” or any show commands which gives a long output using putty, the SSH2 putty closes prematurely.

  Conditions: This symptom is observed when “term length 0” is enabled. The putty session closes prematurely while executing “show tech show memory”.

  Workaround: Redirect the output to a file.

- CSCuj14595

  Symptom: A Cisco 3945 voice gateway running Cisco IOS Release 15.2(4)M3 or Cisco IOS Release 15.2(4)M4 may have a processor pool memory leak in the CCSIP_TCP_SOCKET process.

  Conditions: This symptom is seen on slow TCP connections, where the response is slow and frequent transmission errors are observed.

  Workaround: There is no workaround.

- CSCuj17827

  Symptom: CCD unable to unpublish hosted DN patterns on forwarders running service-routing code. This can result in stale or duplicate routes in remote cluster’s Learned Pattern table.

  Conditions: This symptom is observed during disabling the advertising service, resetting the CCD sip trunk, rebooting a cluster, or a cluster losing connection to all SAF forwarders may trigger this defect.

  Workaround: No workaround for preventing duplicate or stale routes, these routes can be purged from a remote cluster by resetting that cluster’s requesting service or configuring a temporary Blocked Learn Pattern that matches the affected patterns.

- CSCuj23293

  Symptom: A memory leak is seen in the MALLOCLITE process:

  ```
  show processes memory ----------------- Processor Pool Total: 282793968 Used:
  280754252 Free: 2039716 I/O Pool Total: 41943040 Used: 18560544 Free: 23382496
  PID TTY Allocated Freed Holding Getbufs Retbufs Process 0 0 268189264 170950536
  88785564 1354 634324 *Init* 0 0 0 0 141933756 0 0 *MallocLite* 409 0 451333208
  202702788 40928844 83639 83639 CCSIP_UDP_SOCKET 299003084 Total The memory continues
  to increase there.
  ```

  Conditions: This symptom is observed while parsing to header, Gateway gets errors as below:

  ```
  Feb 26 12:07:28 EST: Parse Error: url_parseSipUrl: Received Bad Port Feb 26 12:07:28
  EST: //2765/000000000000/SIP/Error/sippmh_cmp_tags: Parse Error in request header
  ```

  The correct response for the above should have been to send 400 Bad Request The request cannot be fulfilled due to bad syntax

  The memory associated with the above is not getting released is the side effect of the above.

  Workaround: There is no workaround.

Further Problem Description: This issue was not seen on versions earlier than 15.3X

- CSCuj31290

  Packet of Disconnect (POD) functionality does not work after upgrading router from Cisco IOS Release 15.1 to 15.2 code. POD fails with following error:

  ```
  *Sep 10 16:51:48.063: RADIUS: Dynamic-Author-Error[101] 6 Missing Attribute [402]
  Symptom: Packet of Disconnect (POD) functionality does not work after upgrading router
  from Cisco IOS Release 15.1 to 15.2 code.
  POD fails with following error:
  *Sep 10 16:51:48.063: RADIUS: Dynamic-Author-Error[101] 6 Missing Attribute [402]
  ```

  Conditions: This symptom is observed under the following conditions:

  1. When PoD with just username is sent
  2. IOS device is configured for packet of disconnect
  3. IOS device is running Cisco IOS Release 15.2 Mainline code

  Workaround: Downgrade router back to Cisco IOS Release 15.1 release of code.

- CSCuj40804

  Symptom:

  1. IPDT gets enabled on all bundle ports including RSL port due to which FEX does not come up after a reload, link flap, or SSO. FEX RSL channel members will be in ?u? state, that is unsuitable for a part of the etherchannel.
  2. IPDT also gets enabled on the Service module (FWSM) internal port-channel and there is no way to recover them other than removing NMSP (as internal port-channels are non-configurable and non-accessible).

  Conditions: This symptom occurs after a reload with “NMSP” protocol.

  Workaround: Apply “attachment-suppress” on the port first and bundle the port later. There is no workaround in the case of FWSM internal port-channel.

- CSCuj44818

  Symptom: A warning message is displayed.

  Conditions: This issue occurs while unconfiguring video monitoring.

  Workaround: There is no workaround.

- CSCuj55540

  Symptom: Exception is seen on 3945E with whitelisted scansafe traffic.

  Conditions: This symptom is observed when there is a lot of whitelisted traffic going through the ISR box.

  Workaround: Disable whitelisting.

- CSCuj66067

  Symptom: Router running out of memory after an upgrade to Cisco IOS Releases 15.3(1)S, 15.3(3)S, and 15.4(1)S.

  Conditions: This symptom is observed when huge number of route server (approximately more than 700) contexts configures in the router.

  Workaround: Perform the following workaround:

  1. Reduce the number of Route server contexts.
  2. Downgrade the IOS version to 15.2(4)S or lower release.

- CSCuj68289

  Symptom: Static SGACL permissions are not updated for authentication server assigned SGT.

  Conditions: This symptom is seen with an authentication server assigned SGT.

  Workaround: Use manual SGT or dynamic SGACL.

- CSCuj89036

  Symptom: IOSd crashes following an OIR of an eToken.

  Conditions: This symptom occurs during OIR activity on either USB port of a single eToken.

  Workaround: Do not OIR an eToken.

  More Info: When an eToken is inserted, files on the eToken need to be recursively scanned to build up the master file directory structure. This recursive scanning and building the database can take a very long time depending on the eToken contents. When dual IOSd redundancy mode is enabled, this process appears to take almost twice as long and can easily go over 10 seconds to trip off the IOSd watchdog timeout. Fix is to allow other processes to take over CPU so watchdog timeout will not happen.

- CSCuj89374

  Symptom: CFT was reporting two flows for incoming packets on a dialer interface.

  Conditions: PPPoE on underlying physical interface with ip nat outside configured on the dialer interface.

  Workaround: There is no workaround.

- CSCuj96546

  Symptom: After SSO, egress WCCP stops working in hardware, as netflow does not get installed.

  Conditions: When GRE redirection and hash assignment used for egress redirection and if the tunnel created takes the source address as the WCCP egress interface's IP address.

  Workaround: Create loopback interface and assign highest IP address to it, so that the tunnel created takes this IP address as tunnel source address.

- CSCul10573

  Symptom: On receiving a BGP update from a neighbor, the router will send an illegal network notification and flap the session.

  Conditions: This symptom occurs when the prefix received is a Leaf A-D route (RFC 6514) with an S-PMSI route serving as the Route Key.

  Workaround: There is no workaround.

- CSCul18552

  Symptom: After a switchover, QoS policy map in standby is not synced as in the case of active.

  Conditions: This symptom occurs after a switchover.

  Workaround: There is no workaround.

- CSCul24025

  Symptom: A Cisco ASR 1000 Series router crashes at __be_slaComponentProcessEvent when **ip sla udp-jitter** is unconfigured.

  Conditions:This symptom occurs when 1000+ IP SLA udp-jitter is configured and then all unconfigured immediately.

  Workaround: There is no workaround.

- CSCul27924

  Symptom: Customer experienced crash on ASR-1001 during normal operation.

  Conditions: This symptom is not observed under any specific condition.

  Workaround: There is no workaround.

- CSCul39964

  Symptom: Sessions do not get cleared. They get stuck in WT_ST state.

  Conditions: This symptom occurs when sessions are closed in bulk mode by shutting any trunk link or during a clear all session from DUT.

  Workaround: There is no workaround.

  More Info: The memory leak issue and WT_ST are related. Along with memory leak, sessions are not cleared on active RP They get stuck in WT_ST state.

```
asr1k-1#sh clock
07:18:07.045 CET Thu Nov 14 2013
asr1k-1#su
PTA : Locally terminated sessions
FWDED: Forwarded sessions
TRANS: All other sessions (in transient state)
TOTAL PTA FWDED TRANS
TOTAL 14465 0 6557 7908
GigabitEthernet0/0/0 3024 0 0 3024
GigabitEthernet0/0/1 2587 0 0 2587
GigabitEthernet0/1/0 2297 0 0 2297
GigabitEthernet0/1/1 6557 0 6557 0
asr1k-1#
asr1k-1#
asr1k-1#
asr1k-1#sh clock
07:20:08.295 CET Thu Nov 14 2013
asr1k-1#su
PTA : Locally terminated sessions
FWDED: Forwarded sessions
TRANS: All other sessions (in transient state)
TOTAL PTA FWDED TRANS
TOTAL 14465 0 6557 7908
GigabitEthernet0/0/0 3024 0 0 3024
GigabitEthernet0/0/1 2587 0 0 2587
GigabitEthernet0/1/0 2297 0 0 2297
GigabitEthernet0/1/1 6557 0 6557 0
asr1k-1#
asr1k-1#
asr1k-1#sh clock
07:46:34.113 CET Thu Nov 14 2013
asr1k-1#su
PTA : Locally terminated sessions
FWDED: Forwarded sessions
TRANS: All other sessions (in transient state)
TOTAL PTA FWDED TRANS
TOTAL 14465 0 6557 7908
GigabitEthernet0/0/0 3024 0 0 3024
GigabitEthernet0/0/1 2587 0 0 2587
GigabitEthernet0/1/0 2297 0 0 2297
GigabitEthernet0/1/1 6557 0 6557 0
asr1k-1#
asr1k-1#s
6557 sessions in FORWARDED (FWDED) State
7908 sessions in WAITING_FOR_STATS (WT_ST) State
14465 sessions totalUniq ID PPPoE RemMAC Port VT
```

```
VA State
SID LocMAC VA-st Type
5978 5978 0000.6ca3.0116 Gi0/0/0.2940148 1 Vi2.3091 WT_ST
b414.8901.8e00 VLAN: 294/148 UP
5979 5979 0000.6ca3.0117 Gi0/0/0.2940149 1 Vi2.3092 WT_ST
b414.8901.8e00 VLAN: 294/149 UP
6460 6514 0000.6ca3.0134 Gi0/0/0.2940178 1 Vi2.3354 WT_ST
b414.8901.8e00 VLAN: 294/178 UP
6454 6508 0000.6ca3.0135 Gi0/0/0.2940179 1 Vi2.3350 WT_ST
b414.8901.8e00 VLAN: 294/179 UP
6453 6507 0000.6ca3.0136 Gi0/0/0.2940180 1 Vi2.3349 WT_ST
b414.8901.8e00 VLAN: 294/180 UP
6518 6572 0000.6ca3.0137 Gi0/0/0.2940181 1 Vi2.3395 WT_ST
b414.8901.8e00 VLAN: 294/181 UP
6514 6568 0000.6ca3.0138 Gi0/0/0.2940182 1 Vi2.3393 WT_ST
b414.8901.8e00 VLAN: 294/182 UP
6516 6570 0000.6ca3.0139 Gi0/0/0.2940183 1 Vi2.3394 WT_ST
b414.8901.8e00 VLAN: 294/183 UP
6560 6614 0000.6ca3.013a Gi0/0/0.2940184 1 Vi2.3413 WT_ST
```

- CSCul40478

  Symptom: A crash was seen in the periodic accounting process due to the stale reference of the attribute list with AAA accounting DB (this specific attribute list is used by the periodic accounting process for sending the interim accounting records).

  Conditions: This symptom occurs with Policy Component allocate AAA attribute list handle. This handle reference is shared among multiple components for processing. A component can free the attribute list using this handle. AAA does not validate the handle before usage. The policy will not share the same attribute handle reference with other components. The policy will share a copy of the attribute list to other components so that the component does not refer the same handle.

  Workaround: There is no workaround.

- CSCul43968

  Symptom: Mroute states never expire on egress PE without any active downstream receivers.

  Conditions: This symptom occurs in an IPv6 multicast running in a VRF scenario and during unconfiguration of such a loopback interface that has MLD joins on it.

  Workaround: There is no workaround.

- CSCul46792

  Symptom: VCs remain down on ISSU from previous Cisco XE3.12 to Cisco XE3.12 Release.

  Conditions: This symptom is observed under the following conditions:

  1. VPLS BGP Signalling is configured
  2. VC's are established in the Active RP

  Workaround: There is no workaround.

- CSCul49375

  ```
  Symptom: The Cisco ASR 1000 router displays the following messages in the logs:
  %IDMGR-3-INVALID_ID: bad id in id_get (Out of IDs!) (id: 0x0) -Traceback=
  1#cb40dca901558e45a65b881a8695af4f :400000+8653B3 :400000+893696 :400000+DF330C
  :400000+DED89B :400000+DF8643 :400000+1F57F36 :400000+1F4BBFB :400000+1F33BA7
  :400000+1F336C1 :400000+1F34FF9 :400000+1F27763 :400000+1F29B16 :400000+2546FF3
  :400000+2546EDD :400000+1F2930B
  ```

  No new PPPoE sessions can be established anymore.

Conditions: The conditions to this symptom are unknown.

Workaround: Reload the device.

- CSCul49852

  Symptom: A router might see PPPoE-sessions in the WAITING_FOR_STATS (or WT_ST) status.

  Conditions: This symptom was observed by specific users or because of using a specific profile or service like ShellMaps and Radius. The system is configured as BRAS aggregating PPPoEoA or -oE-sessions.

  Workaround: There is no workaround.

- CSCul54254

  Symptom: Invalid LSAs are not flushed by the router which has their Advertising Router ID. Specifically, Router LSAs which do not have LSID of 0 will not be flushed if the router does not re-originate them, and any LSA with a type that the router does not recognize.

  Lingering LSAs could lead to incorrect routing in some very obscure instances. For example, stale Router LSA fragments from two neighboring routers would need to remain in the network. There would not be a routing problem if only one router’s stale Router LSA fragment was allowed to linger.

  Conditions: There are several possible scenarios that could lead to this symptom. One example is that a router is configured with many interfaces attached to an OSPFv3 instance such that it originates more than one Router LSA fragment. Then the router is reloaded before the configuration is saved, and after the reload it does not reoriginate some of the Router LSA fragments.

  Workaround: There is no workaround.

- CSCul55900

  Symptom: A FlexVPN Scale rate degradation occurs due to more CPU consumed by static processes.

  Conditions: This symptom occurs under the following conditions:

  1. Configure UUT to be the flexvpn server which can scale upto 10K sessions.
  2. Configure IKEv2 Authorization policy.
  3. Try to bring up the flexvpn 10K sessions and monitor the CPU usage.

  Workaround: Remove IKEv2 authorization policy. In such a case, IKEv2 routing and mode configuration cannot be verified.

- CSCul72121

  Symptom: Continuous trace backs on the PTF console is observed and PTF crashes during a soak.

  Conditions: This symptom occurs under the following conditions:

  1. Create an MDS profile as attached.
  2. Leave the setup for soak for 12 hours.

  Workaround: Reload ACT and SBY PTF.

- CSCul75876

  Symptom: A router may crash in an OSPF process during reconfiguration.

  Conditions: This symptom occurs under the following conditions:

  1. Configure the router with “ipfrr” in area 0.
  2. Connect router to area 0 through two links. For some route one interface is the primary path, and the second is the repair path.

3. Configure router as ABR, that is, have a non-zero area with a neighbor. Do not configure “ipfrr” in the non-zero area. Quickly remove the IP address from both the interfaces in area 0 and router the may crash.

Workaround: Changes to the reconfiguration procedure will avoid the crash.

– Shutdown the interface before removing the IP

– Remove the IP from one interface in area 0, wait for a few seconds and remove the IP address from the second interface in area 0.

- CSCul86211

  Symptom: When LNS switches off while the sessions keep on establishing at LAC, LAC finds the l2tp db memory exhausted after sometime. Due to this, it fails to update the session in the database and during this period a crash is observed.

  Conditions: This symptom occurs when LAC tries to add l2tp session in the database and fails to do so. In order to handle this error condition, LAC frees the l2tp and l2x session twice. This double free is the reason for crash.

  Workaround: There is no workaround.

- CSCul87037

  Symptom: An “sg subrte conte” chunk leak occurs while roaming.

  Conditions: This symptom occurs after an account-logoff and if service permit is configured in control policy. In case of a service permit, the subscriber remains unauth and is redirected to the portal once again. Post successful second account logon and the subscriber session is cleared by timeout or cli, the leak is seen and the same client will not be able to create the session once again. The leak is seen after simulating for the second time account-logon. And if service permit is configured.

  In case of service disconnect configured under account-logoff, account-logon is not a practical scenario as the portal is not reachable for the client.

  Workaround: Use **service disconnect** for **event account-logoff**.

  ```
  class type control always event account-logoff 1 service disconnect delay 10 !
  ```

- CSCul88004

  Symptom: DPSS packet injects fails to work.

  Conditions: This has been observed to occur when the onePK application name contains space characters, for example, white space and tab.

  Workaround: Rename the application with no white-spaces.

- CSCul90553

  Symptom: Cisco IOS-XE RP2-based platforms are unable to reach 4000 IPSec tunnels with DMVPN EIGRP.

  Conditions: This symptom occurs when DMVPN with EIGRP is used on Cisco IOS-XE RP2 platforms.

  Workaround: Use previous Cisco IOS XE images (such as Cisco IOS XE Release 3.11).

- CSCul90667

  Symptom: Error messages and tracebacks are printed to the console.

  Conditions: This symptom occurs when IGP times out while Standby RP becomes NSR Active.

  Workaround: Enable NSR under IGP to ensure no timeout occurs.

- CSCul92497

  Symptom: The Cisco 7600 router providing layer2 EoMPLS services may stop forwarding ingress and egress traffic for an xconnect for which a backup peer config has been applied.

  Conditions: This symptom occurs in Cisco 7600 routers running Cisco IOS Release 15.2(4)S4a with ES+ cards (access or core facing) and xconnect configured under a service instance.

  Workaround: Clear the xconnect on the Cisco 7600 router side. Clearing on the remote size does not have an effect.

- CSCul96778

  Symptom: A router may crash and reload with BGP related traceback in an extremely rare timing condition while running “show ip bgp vpnv4 vrf XXXX nei A.A.A.A”.

  Conditions: While making BGP related changes such as moving the same neighbor with quick operation of “no neighbor x.x.x.x” and then “neighbor x.x.x.x” across VRFs. Imediately after this if we type a “show ip bgp vpnv4 vrf XXXX nei A.A.A.A” - on a Cisco router running IOS and BGP, then in extremely rare timing condition the router may crash. The possibility of this to happen increases if the configuration and unconfiguration is done from one console and the show operation done from other console.

  Workaround: When doing configuration and un-configuration and then show, its better to serialize the operation rather than aggressively use multiple consoles to do all actions at the same time.

- CSCul99015

  Symptom: In VPLS using BGP signaling with Inter AS, when a PE on another AS is reachable through multiple ASBRs, the PW destination and the next hop PE address of some or all of the PWs in the standby RP remains as the non-preferred ASBR address instead of the preferred ASBR address.

  Conditions: This symptom occurs under the following conditions:

  1. BGP L2VPN NLRIs received first from an ASBR becomes a less preferred ASBR on receiving NLRIs for the same VE-IDs from a more preferred ASBR.
  2. NLRI received from the more preferred ASBR has the same values (VEID, VBO, VBS, Label Base, MTU and CW) as the ones received previously from the other ASBR.

  Workaround: Bring up the BGP session with the more preferred ASBR first. This would cause no updates to existing NLRIs even if received from other less preferred ASBRs.

- CSCum00056

  Symptom: ASR IOSd crash occurs with the following error:

  ```
  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = ISG CMD HANDLER
  ```

  Conditions: This symptom occurs when changes are made through RADIUS.

  Workaround: There is no workaround.

- CSCum04512

  Symptom: When an RP switchover is done (which is head end for 500 TE tunnel and tail end for 500 TE tunnels), the RSVP label is assigned to the TE tunnel change and this in turn causes a traffic loss of 45 seconds on the pseudowire which is directed through these tunnels.

  Conditions: This symptom occurs under the following conditions:

  – TE RID under the IGP is configured as a loopback other than the first one.

  – SSO is performed.

  Workaround: Configure the TE router ID under the IGP to be the first loopback interface.

- CSCum07119

  Symptom: Router generates tracebacks or crashes depending on platforms when **show application ip route** command is used concurrently with application route deletion.

  Conditions: This symptom is observed when the **show application ip route** command is issued when JAVA onePK SDK is handling route replace operations.

  Workaround:

  1. Use **show ip route** command to display the application routes and not **show application ip route** command.
  2. Use onePK GET ROUTE API to get the status of application added route.
  3. Use **show application ip route** only when there is no route delete is in progress.

- CSCum11118

  Symptom: A Cisco ISR router crashes due to stack overflow in the "ADJ background" process. The following syslog may be seen just before the crash:

  ```
  000105: Dec 9 04:08:44.447 UTC: SYS-6-STACKLOW Stack for process ADJ background
  running low, 20/6000.
  ```

  Can also cause crash due to memory corruption, would show messages like

  current memory block, bp = 0x3B727044, memorypool type is Processor data check, ptr = 0x3B727074

  ```
  next memory block, bp = 0x3B729A60, memorypool type is Processor data check, ptr =
  0x3B729A90
  previous memory block, bp = 0x3B725DCC, memorypool type is Processor data check, ptr =
  0x3B725DFC
  ```

  Conditions: The conditions to this symptom are unknown.

  Workaround: There is no workaround.

- CSCum14830

  Symptom: Leaking IPv6 routes is observed from a VRF table into the global table using BGP. These routes consist of the following:

  1. BGP routes learned from the VRF IPv6 BGP peer.
  2. Redistributed static and connected routes.

  The BGP routes leak fine, but the redistributed static and connected routes have an issue. After the redistributed routes leak, the exit interface shows "null0". Sometimes instead of showing the exit interface as "null0", it shows a random interface which is a part of VRF and has IPv6 enabled on it.

  Conditions: This symptom occurs with IPv6 redistributed connected and static routes into BGP VRF (could also be redistributed from other protocols as well but have not been tested).

  Workaround: There is no workaround.

- CSCum15232

  Symptom: A Cisco IOS router may crash using LDAP while performing TLS operations.

  Conditions: This symptom was observed in Cisco IOS Release 15.3(3)M1.4. Other versions can be affected as well.

  Workaround: There is no workaround.

  More Info: LDAP is used in IOS SSLVPN deployment to authenticate users.

- CSCum17958

  Symptom: An IOSd crash is observed during a configuration replace.

  Conditions: This symptom occurs on configuration with a port-channel interface.

  Workaround: There is no workaround.

- CSCum22612

  Symptom: Since the ASR fails to send MM6 [being a responder] in the absence of a valid certificate, IKE SAs start leaking and hence get stuck in MM_KEY_EXCH state. Multiple MM_KEY_EXCH exist for a single Peer on the ASR, however the Peer does not retain any SAs for ASR in this case. Along with CAC for in-negotiation IKE SAs, these stuck SAs block any new SAs or IKE rekeys even after renewing the certificates on the ASR.

  Conditions: This symptom is observed under the following conditions:

  – ASR acting as IKEv1 termination point [sVTI for example] and is a responder.

  – IKE authentication mode is RSA-SIG [Certificates].

  – On the ASR, the ID-Certificate is either Expired or Not-present for a given sVTI tunnel

  – The ASR also has a IKE in-negotiation CAC of a certain value.

  ```
  Example: crypto call admission limit ike in-negotiation-sa 30
  ```

  Workaround: Perform the following workarounds:

  1. Manually delete stuck SAs by using: **clear crypto isakmp 12345**, where 12345 is conn_id of a stuck SA. Repeat this for each stuck SA
  2. Temporarily increase CAC to accommodate new SA requests: crypto call admission limit ike in-negotiation-sa 60

  More Info: Found and Tested in Cisco Release XE 3.7.4 or Cisco IOS Release 15.2(4)S4.

- CSCum29064

  Symptom: Syncing dual-stack iWAG session to STANDBY does not occur.

  Conditions: This symptom occurs when IPv4 and IPv6 FSOL is received from same client at ISG together (or very less time gap) for a dual-stack session. In this case, the session does not sync to STANDBY for the previous IPv6 FSOL and ISG gets a new IPv4 FSOL.

  Workaround: There is no workaround.

- CSCum34830

  Symptom: A router crash is observed.

  Conditions: This symptom occurs while performing VRRP and VRRS-related configuration changes.

  Workaround: Unconfigure the **ip pim redundancy <>** command before deleting the subinterface or disabling PIM on an interface.

- CSCum36825

  Symptom: No IPv6 global unicast address is assigned to PPP Virtual access interfaces and to IPv6 over IP/GRE tunnel interfaces.

  Conditions: Virtual access interface is configured using the command “ipv6 address autoconfig”.

  Workaround: There are no workarounds.

- CSCum45122

  Symptom: An IPv6 MFIB entry is not removed after the mroute expires.

Conditions: This symptom occurs only with the partitioned MDT profile for mLDP. The PE router could get into a trouble state if it receives traffic first and then almost immediately after that receives an MLD join on the same interface for the same group.

Workaround: Remove VRF context and then reconfigure it.

- CSCum46850

  Symptom: Using LISP set tags on routes imported to the RIB when exporting LISP routes from the RIB to BGP fails.

  Conditions: This symptom occurs when redistribute list route-map is used under bgp with a route-map that contains match tag.

  Workaround: There is no workaround.

- CSCum48221

  Symptom: 3560CG box memory is showing as low as 3.15MB.

  Conditions: This symptom is not observed under any specific conditions.

  Workaround: There is no workaround.

- CSCum52216

  Symptom: After a reload, **ip pim sparse-mode** is gone on interface lisp 0.x (x denoted the LSIP interface number).

  Conditions: This symptom occurs after a reload.

  Workaround: There is no workaround.

- CSCum61595

  Symptom: Alignment errors are observed after upgrading to Cisco IOS Release 15.2(4)M5.

  ```
  Jan 9 19:42:59.623 GMT: %ALIGN-3-CORRECT: Alignment correction made at 0x6477F81Cz
  reading 0x6BE87495 Jan 9 19:42:59.623 GMT: %ALIGN-3-TRACE: -Traceback= 0x6477F81Cz
  0x647805D0z 0x6478FE70z 0x64751088z 0x64B99F4Cz 0x64B99FD4z 0x64752 284z 0x647525ACz
  ```

  Conditions: This symptom does not occur under specific conditions.

  Workaround: There is no workaround.

- CSCum62783

  Symptom: The following alignment errors are seen after a PPPoE session establishment for the first time after a reboot:

  ```
  *Jan 14 07:24:40.591: %ALIGN-3-CORRECT: Alignment correction made at 0x32B2DFF4z
  reading 0xE7790ED *Jan 14 07:24:40.591: %ALIGN-3-TRACE: -Traceback= 0x32B2DFF4z
  0x32B1E274z 0x32B1EECCz 0x32B1EF90z 0x332E550Cz 0x332E54F0z 0xFFFF1A00z 0xFFFF1A00z
  ```

  Conditions: This symptom occurs when **pppoe-client ppp-max-payload** is configured under the Ethernet interface.

  Workaround: There is no workaround.

- CSCum63121

  Symptom: Localhost not reflected in “show call history voice last 2”.

  Conditions: This symptom is observed when UUTs are loaded with c2900-universalk9-mz.SPA.153-3.M1.9.

  Workaround: There is no workaround.

- CSCum64565

  Symptom: Router crashes while getting NTP status.

  Conditions: This symptom is not observed under any specific conditions.

  Workaround: There is no workaround.

- CSCum65451

  Symptom: A crash occurs due to multicast stack overflow memory corruption.

  Conditions: This symptom may occur when PIM is enabled on a LISP interface and Auto-RP is also enabled.

  Workaround: Configure **no ip pim autorp** before any other PIM or LISP configuration.

- CSCum67166

  Symptom: The router hangs after loading an image.

  Conditions: This symptom occurs with the latest whales-universal-mz mcp_dev image.

  Workaround: There is no workaround.

- CSCum71701

  Symptom: This bug can stop traffic from being forwarded by an upstream router when the **ip pim join-prune-interval** command is configured on the downstream router's upstream LISP interface.

  Conditions: This symptom occurs when the **ip pim join-prune-interval** command is configured with a value greater than the default on a LISP interface.

  Workaround: There is no workaround.

- CSCum78363

  Symptom: Local circuit keeps DOWN state.

  Conditions: This symptom is observed when L2TPv3 session is configured.

  Workaround: There is no workaround.

- CSCum85493

  Symptom: Ping fails with tunnel protection applied.

  Conditions: Tunnel protection applied on GRE tunnel interface, using IKEv1 to negotiate IPsec SAs and remote node (IKEv1 responder) behind NAT.

  Workaround: The users can switch to IKEv2.

- CSCum85813

  Symptom: Shut primary static router and secondary static is not installed automatically.

  Conditions: This symptom is seen on the sites where the BFD state of the backup static route is marked as "U" in the output of "show ip static route bfd".

  Workaround: Reinstall the default backup static route.

- CSCum85923

  Symptom: Router-solicitation (RS) messages are dropped on the switch port that have IPv6 RA guard enabled. On removing RA guard, RS messages go through.

  Releases tested:

  Affected releases: 151-2.SG2 and 152-1.E.bin

  Unaffected releases: 150-2.SG.bin

Conditions: This symptom occurs when "ipv6 nd raguard" is enabled.

Workaround: There is no workaround.

- CSCum86841

  Symptom: When upgrading from Cisco IOS XE Release 3.2S to Cisco IOS XE Release 3.9S, the DHCP server NACKs the client while sending renew. This worked in Cisco IOS XE Release 3.2S and not in Cisco IOS XE Release 3.9S.

  Conditions: This symptom occurs when the DHCP server is provisioned to give out an IP address using a host pool (where the MAC address is tied to IP address). After the client gets the IP address, it downloads the configurations from the TFTP server and update the new MAC address after which when the client sends a renew, the DHCP server NACKs the client till the binding is present.

  Workaround: There is no workaround. Downgrade to Cisco IOS XE Release 3.2S.

- CSCum88382

  Symptom: BFD session not established upon RP Switchover and back.

  Conditions: This symptom is observed during RP switchover and switchback.

  Workaround: There is no workaround.

- CSCum89148

  Symptom: Map-requests are forwarded to sites whose locators do not match the configured allowed-locator policy.

  Conditions: This symptom is observed when the {ipv4 | ipv6} map-resolver allowed-locator registered is configured, and allowed-locator configuration is present under "site".

  Workaround: There is no workaround.

- CSCum93027

  Symptom: A Cisco router reloads unexpectedly.

  Conditions: This symptom occurs when the following conditions are reproduced:

  1. Configure a subinterface with IPv6.
  2. Configure OSPFv3 on the subinterface.
  3. Configure IPSec authentication for OSPFv3 on the subinterface.
  4. Shutdown the subinterface.
  5. Remove the subinterface.

  Workaround: Unconfigure the OSPFv3 IPSec authentication configuration before removing the subinterface.

- CSCum93078

  Symptom: Image installation fails for K10.

  Conditions: This symptom occurs after trying to install a tar image on K10. Installation of a bin image fails.

  Workaround: Reboot the switch.

- CSCum94228

  Symptom: Local CAC displaying all information about each flows. This may impact show output for customer in a set up where we could possibly have large number of flows.

  Conditions: This symptom is observed in a scaled configuration.

Workaround: There is no workaround.

- CSCum95330

  Symptom: Removing an Ethernet service instance which is a member of a bridge domain may cause the router to reload.

  Conditions: This symptom is observed when the last service instance is removed from the bridge domain and there are still members of the bridge domain which are not service instances (such as VFIs).

  Workaround: Completely unconfigure the bridge domain and reconfigure it.

- CSCun00488

  Symptom: Duplicate records are exported from MMA.

  Conditions: This symptom occurs in the following topology:

  ```
  SRC --- UUT --DST | collector
  ```

  Set the configuration at the UUT to export all the records to the collector. At the exporter, duplicate records are noticed.

  Workaround: There is no workaround.

- CSCun04467

  Symptom: Prior to receiving a label via the Label Distribution Protocol (LDP), the output of **show mpls l2transport vc detailed** and **show l2vpn atom vc detailed** fail to properly indicate the lack of a remote binding.

  Conditions: This symptom has been observed in Cisco IOS Release 15.4(02)S.

  Workaround: There is no workaround.

- CSCun07772

  Symptom: A Cisco router crashes.

  Conditions: This symptom occurs on deleting a subcriber’s session in attempting state by a COA script as shown below:

  ```
  #!/bin/sh CISCO=$1 # bras SessionID=$2 CoaSecret=’secret’ #clear ISG session on BRAS
  /bin/echo
  "User-Name="undef",Acct-Session-Id="$SessionID",cisco-avpair="subscriber:command=accou
  nt-logoff"" | /usr/bin/radclient -x $CISCO:1700 coa $CoaSecret
  ```

  Workaround: Do not use the COA script for deleting the subscriber’s session.

- CSCun11782

  Symptom: Rtfilter prefixes are sent with incorrect next-hop equal to next-hop of the default static route in GRT instead of BGP router-id.

  Conditions: This symptom occurs with a default static route present in GRT pointing, for example, to the next-hop known behind the connected interface.

  Workaround: Replace the default static route with a more specific static route or remove static and clear BGP.

- CSCun11927

  Symptom: Link-OAM breaks after link flap between the Cisco Catalyst 4500-X Series Switch and the Cisco ASR 9000 Series Router. With an interface with LACP + Link-OAM configuration when the connection between the Catalyst 4500-X Series Switch(IOS XE) and Cisco ASR 9000 Series

Router(IOS XR) flaps, the link does not restore due to the following deadlock : LACP PDU does not start unless OAM starts on the Cisco ASR 9000 Series Router side and Link-OAM PDU does not start unless LACP starts on the Catalyst 4500-X Series Switch side.

With the above scenario after a link flap the link gets stuck in (suspended) LACP state on the Catalyst 4500-X Series Switch and non-connected state on Cisco ASR 9000 Series Router. The link has to be restored with manual reconfiguration in a particular sequence to avoid the above dead lock.

Conditions: This symptom occurs due to a combination of Link-OAM and LACP between a Catalyst 4500-X Series Switch and a Cisco ASR 9000 Series Router.

Workaround: Manually restart the link-OAM session and toggle LACP. To restore the link, change the configuration sequence on the Catalyst 4500-X Series Switch side in such a way that the LACP packet goes ahead first and then the Link-OAM PDU.

```
interface x/x
shut
no ethernet oam
no channel-group <x> active
no shut
channel-group <x> active
ethernet oam
```

or

Disable EFD on the Cisco ASR 9000 Series Router side.

or

Toggle OAM on the Cisco ASR 9000 Series Router side.

- CSCun13399

  Symptom: Flow-ids are not synced on the standby for some of the IMA VCs on an HA setup.

  Conditions: This symptom occurs when an HA router is reloaded with IMA VCs enabled on it.

  Workaround: There is no workaround.

- CSCun13688

  Symptom: The Cisco Catalyst 6500 Supervisor Engine 2T with CLNS routing configured crashes after **show clnbs route**.

  Conditions: This symptom occurs when CLNS routing is configured.

  Workaround: There is no workaround.

- CSCun19455

  Symptom: When an access-list is applied to an interface using onePK, the “ip access-group” configuration will appear in the running configuration. When the app terminates, this configuration is removed. Additionally, any manually configured access-group for that interface is removed.

  Conditions: This occurs when using onePK 1.1.0. The ACL lifetime need not be set to persistent.

  Workaround: There is no workaround.

- CSCun25912

  Symptom: Configurations dynamically applied to the virtual-access interface might be lost over the reconnection while using the autoreconnect feature on Cisco Anyconnect on the ASR platform.

  For example, the interface after initial connection establishment would have a QOS service policy applied:

```
ROUTER#sh derived-config int virtual-access 1
!
```

```
interface Virtual-Access1
ip unnumbered GigabitEthernet0/0/1
tunnel source 10.1.1.1
tunnel mode ipsec ipv4
tunnel destination 10.10.1.100
tunnel protection ipsec profile ipsec-profile
no tunnel protection ipsec initiate
service-policy input INPUT-POLICY
end
```

After reconnection the INPUT-POLICY is missing:

```
ROUTER#sh derived-config int virtual-access 1
!
interface Virtual-Access1
ip unnumbered GigabitEthernet0/0/1
tunnel source 10.1.1.1
tunnel mode ipsec ipv4
tunnel destination 10.10.1.100
tunnel protection ipsec profile ipsec-profile
no tunnel protection ipsec initiate
end
```

Conditions: This symptom is observed with configurations being applied from the user AAA profile over radius authentication. Affected parameters observed are QOS service policies and access-group.

Workaround:

1. Do not use the reconnect feature.

or

2. Apply the configurations directly to the virtual-template (if this is an option).

- CSCun28171

  Symptom: An ISG will stop processing CoAs for a subscriber session when CoAs are received in rapid succession. The received CoAs are queued but never processed.

  Conditions: This symptom occurs when multiple CoAs for a single subscriber session are received in short time (milliseconds).

  Workaround: The subscriber session needs to be reset to recover. There is no workaround known yet to avoid the situation from happening.

- CSCun31021

  Symptom: A vulnerability in IKE module of Cisco IOS and Cisco IOS XE could allow an unauthenticated, remote attacker to affect already established Security Associations (SA)..

  The vulnerability is due to a wrong handling of rogue IKE Main Mode packets. An attacker could exploit this vulnerability by sending a crafted Main Mode packet to an affected device. An exploit could allow the attacker to cause dropping of valid, established IKE Security Associations on an affected device.

  Conditions: Device configured to process IKE request that already has a number of established security associations.

  Workaround: There is no workaround.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4.3/3.6: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:N/A:P/E:F/RL:OF/RC:C CVE ID

  CVE-2014-2143 has been assigned to document this issue.

Additional details about the vulnerability described here can be found at: http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-2143

Additional information on Cisco’s security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCun31450

  Symptom: CPU hog followed by crash.

  Platforms

  – ct5760-ipservices.bin

  – cat3k_caa-universalk9.bin

  – cat4500e-universalk9.bin

  Conditions: This issue occurs while running udp IP SLA applications.

  Workaround: There is no workaround.

- CSCun36655

  Symptom: If the terminal adjacency of a lisp interface is removed and then re-added, the lisp interface MTU may remain at the invalid value of 65535. This can be seen in the **show cef interface** <*intf*> **internal** command output.

  IPsec will obtain the MTU value from CEF and LISP, and the incorrect MTU will cause drops of large packets.

  IPSEC MTU incorrectly computed - causing packet drops on large packets traversing from “inside” to “outside” are dropped.

  Conditions: This symptom is observed in the following Cisco C800 Series: Cisco IOS Software, C890 Software (C890-UNIVERSALK9-M), Version 15.3(3)XB12, RELEASE SOFTWARE (fc2)

  Workaround: A workaround is to toggle the IP MTU config on the lisp interface. Use “show run lisp0.1” to determine the MTU. Then use “ip mtu <mtu>” to first set it to a lower value, and then to set it back to the original value.

```
Example:
sh run interface lisp0.1
interface LISP0.1 ip mtu 1398 crypto map CM end
conf t
interface lisp0.1
ip mtu 1200
ip mtu 1398

More Info: Originally [Cisco IOS Release 15.3(1)T] the MTU was accurately computed as:
RTR13-xTR#sh cry ipse sa vrf DeptA | in mtu path mtu 1456, ip mtu 1456, ip mtu idb
LISP0.1 path mtu 1456, ip mtu 1456, ip mtu idb LISP0.1 path mtu 1456, ipv6 mtu 1456,
ipv6 mtu idb LISP0.1 path mtu 1456, ipv6 mtu 1456, ipv6 mtu idb LISP0.1 RTR13-xTR#
```

  In 153-3.XB12, the MTU is as follows:

```
!
RTR#show crypto ipsec sa
| inc mtu ! plaintext mtu 65458, path mtu 65535, ip mtu 65535, ip mtu idb LISP0
```

- CSCun38333

  Symptom: Locator ID Separation Protocol (LISP) local EID database locator configured through the “database-mapping <eid-prefix> ipv6-interface <interface> priority <priority> weight <weight>” command uses deprecated IPv6 address on specified interface.

  Conditions: Multiple IPv6 addresses available on an interface with the lexicographically first address being deprecated.

Workaround: There is no workaround.

- CSCun40868

  Symptom: The following messages are seen continuously on t_base_4 image:

  ```
  *Feb 28 00:18:00.359: %CFT_API-3-CFT_ERRMSG_NO_MEMORY: CFT could not allocate memory
  for the flow cft_private_insert_pre_flow_tuple, parent_fid: 0
  ```

  Conditions: The issue is seen after configuring the router with Medianet.

  Workaround: There is no workaround.

- CSCun41292

  Symptom: On a Cisco ASR 1001 router running Cisco IOS Release 15.3(1)S, a crash occurs when the "show ip ei vrf X topo X.X.X.X/X" command is executed. The X.X.X.X/X must be in "FD is infinity" status in EIGRP as CSCtz01338.

  asr1001_bew_03# show ip ei vrf

  ```
  * to all | i Infinity P 174.162.XX.XX/24, 0 successors, FD is Infinity, U, serno 37,
  refcount 1 snip P 174.180.XX.XX/29, 0 successors, FD is Infinity, U, serno 46,
  refcount 1
  asr1001_bew_03#show ip ei vrf 1 to 174.162.XX.XX/24

  Exception to IOS Thread: Frame pointer 0x7F63DF6602D0, PC = 0x1956C8D
  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = Exec -Traceback=
  1#980611ad3b9665cd80fe5178bcd6036a :400000+1556C8D :400000+1556B09 :400000+15569D1
  :400000+157DE39 :400000+15197A2 :400000+1518659 :400000+156BA5E :400000+15591D1
  :400000+1189768 :400000+1188E6D :400000+1186E15 :400000+484F270 :400000+11A1CA0
  Fastpath Thread backtrace: -Traceback= 1#980611ad3b9665cd80fe5178bcd6036a
  c:7F64154A4000+BE002
  Auxiliary Thread backtrace: -Traceback= 1#980611ad3b9665cd80fe5178bcd6036a
  pthread:7F640ED43000+A7C9
  ```

  Conditions: This symptom occurs when X.X.X.X/X is in "FD is infinity" status in EIGRP.

  Workaround: There is no workaround.

- CSCun45272

  Symptom:

  1. Standby RP will have out-of-sync entries. With MPLS-TE NSR enabled, the standby RP will have out-of-sync entries which will result in flapping of the path-protected LSP of the tunnel after an SSO.
  2. Leaking an LSP. A third LSP will be signaled and leaked (there is no management of the LSP). There are supposed to be two LSPs at steady state (primary and path protected), but with this defect, there will be primary, path protected, and leaked LSP.

  Conditions: This symptom occurs with a reoptimization of a tunnel that has failed with path protection enabled.

  Workaround: There is no workaround.

- CSCun46486

  Symptom: A Cisco device crashes every 2-3 days when the SNMPSET operation is used to create guest users.

  Conditions: This symptom occurs when guest users are created through SNMPSET operations at a very high rate.

  Workaround: There is no workaround.

- CSCun48344

  Symptom: A config-sync failure occurs due to the **address-family ipv6 unicast vrf** command during the immediate unconfiguration and reconfiguration of VRF definition.

  Conditions: This symptom occurs with attached running configurations.

  Workaround: There is no workaround.

- CSCun52430

  Symptom: Removing explicitly configured queue-limit configuration via “no queue-limit” on a user-defined class may not actually remove the preconfigured queue-limit parameter from PD.

  Conditions: This symptom is observed when an explicitly created queue-limit is removed.

  Workaround: Reconfigure queue-limit with a desired (or default) value.

- CSCun65000

  Symptom: Traffic loss of about 200-500 ms is observed.

  Conditions: This symptom is observed on an RLFA cutover.

  Workaround: There is no workaround.

- CSCun67364

  Symptom: Convergence on Local link failure with rLFA is higher than one second.

  Conditions: Configure rLFA and perform local link failure. The problem is likely seen when configuring a small spf-interval value.

  Workaround: Do not configure too small spf-interval.

- CSCun68542

  Symptom: CSR1000V router running XE3.11 (15.4(1)S) working as Route Reflector.

  The route-reflector is advertising prefixes with incorrect subnet masks to ibgp peers and route-reflector clients. The incorrect prefixes are not present in the bgp table of the route-reflector itself, however they do get installed in the bgp table of the router receiving the update.

  Conditions: This symptom is observed when BGP route reflector uses the additional paths feature.

  Workaround: Disable additional path feature either globally under address-family or per neighbor.

- CSCun71301

  Symptom: A higher layer app such as LISP ends up using a deprecated IPv6 address as returned by the IPv6 service even if a valid address exists for an interface.

  Conditions: This symptom occurs when multiple IPv6 addresses are available on an interface with the lexicographically first address being deprecated.

  Workaround: There is no workaround.

- CSCun72459

  Symptom: High traffic loss is observed with setups having BGP and microloop avoidance combination.

  Conditions: This symptom occurs with the following combination:

  1. IP FRR is turned on.
  2. Cisco IOS XE Release 3.11 code (or newer) that enables microloop avoidance by default.
  3. BGP configurations.

Workaround: Disable the microloop avoidance feature. For example, in ISIS, execute the following commands:

```
router isis <process name>
microloop avoidance disable
!
```

However, there will be some traffic loss due to the lack of microloop avoidance.

- CSCun72939

  Symptom: QoS Egress Marking does not work for GRE Tunnels.

  Conditions: This symptom is observed under the following conditions:

  - The issue happens for fragmented packet.
  - The issue is found on Cisco IOS Release 15.3(3)M2.

  Workaround: There is no workaround.

- CSCun73515

  Symptom: A router crashes due to RMON.

  Conditions: This symptom occurs on activation of an RMON event.

  Workaround: There is no workaround.

- CSCun73782

  Symptom:

  A vulnerability in LISP control messages processing on Cisco IOS and Cisco IOS XE could allow an unauthenticated, remote attacker to cause a vulnerable device to disable CEF forwarding and eventually drop traffic passing through.

  The vulnerability is due to insufficient checking of certain parameters in LISP control messages on ITR. An attacker could exploit this vulnerability by sending malformed LISP control messages to ITR. An exploit could allow the attacker to cause a vulnerable device to disable CEF forwarding and eventually drop traffic passing through.

  Conditions: Malformed messages can only be generated by a device that is already registered to a LISP system: a valid ETR or ALT.

  Workaround: There is no workaround.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4.3/3.6: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:N/A:P/E:F/RL:OF/RC:C

  CVE ID CVE-2014-3262 has been assigned to document this issue.

  Additional details about the vulnerability described here can be found at: http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-3262

  Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCun75719

  Symptom: After a switchover, standby device crashes with traceback.

  Conditions: At present, this is observed only on advipservices images in mtrose branches.

  Workaround: There is no workaround.

- CSCun76733

  Symptom: BFD goes down and remains in Admindown state.

  Conditions: This symptom occurs after applying ACL chaining and flapping of the interface.

  Workaround: There is no workaround.

  More Info: An IPv4 BFD neighbor remains in admindown state on the PE. The ACE configured in ACL for BFD is matched and the receive counters on BFD neighbors are incremented but the BFD is still down.

  This issue occurs only after ACL chaining is applied.

- CSCun77010

  Symptom: A router may crash after or during the execution of the **show ipv6 ospf rib** command.

  Conditions: This symptom occurs when many routes or route paths are present in the OSPFv3 rib. The OSPFv3 rib is significantly recomputed during execution of commands.

  Workaround: Limit the use of the **show ipv6 ospf rib** command.

- CSCun78309

  Symptom: An Mroute entry on FHR is stuck in a registering state in MVPNv4. show ip mroute vrf <vpn-name> -->> shows the mroute entry in registering state

  Conditions: This symptom occurs when the source address of the encapsulation tunnel for PIM registers on the FHR is one of the interfaces that is not in the same VRF as the register tunnel itself.

  Workaround: There is no workaround.

  More Info: Output:

  ```
  PE2#show ip mroute vrf vpn1
  (215.12.1.2, 229.40.1.1), 00:00:29/00:02:30, flags: FT Incoming interface:
  GigabitEthernet3/3.1, RPF nbr 0.0.0.0, Registering Outgoing interface list: Tunnel764,
  Forward/Sparse, 00:00:29/00:03:00
  ```

- CSCun81749

  Symptom: MVPN traffic is unexpectedly terminated since the last-hop PIM router does not send an “SG Join” message on the MDT tunnel.

  Conditions: This symptom occurs when the same IP address is used for the MDT tunnel IP address on the last-hop PIM router and the source IP address of multicast traffic.

  Workaround: There is no workaround.

- CSCun86606

  Symptom: An IOSD crash occurs due to “Process = Virtual Exec”.

  Conditions: This symptom occurs when the **show ip cef internal** command and routing table is cleared in parallel.

  Workaround: When clearing the routing table (for example, clear ip ospf process) avoid running ip cef-related show commands in parallel.

- CSCun87557

  Symptom: A Cisco router crashes.

  Conditions: Set the VTY Service Set maximum response to a small number, for example, 10, and then send multiple commands separated by newline using the same write, for example, “show ver\nshow ver\n”.

  Workaround: Set Maximum response to a bigger number.

- CSCun88267

  Symptom: A Cisco router stops forwarding traffic when an SSLVPN session is established and stops responding.

  Conditions: This symptom occurs with SSLVPN and DTLS enabled. Cisco ISR-G2 platforms may experience a Queue Wedge.

  Workaround: Disable DTLS by configuring **no svc dtls** under policy group.

- CSCun92081

  Symptom: A traceback is seen while removing IPv6 unicast-routing configuration.

  Conditions: This symptom occurs when ISIS IPv4 is not enabled and ISIS is runs on IPv6 multitopology mode.

  Workaround: There is no workaround.

  More Info: The traceback is generated due a warning message that the adjacency database is not empty when ISIS is switching out of the IP mode.

- CSCun92095

  Symptom: IOS-XE running router may reload when unconfiguring BGP along with other removal operations in a scaled setup.

  Conditions: BGP is configured with 1Million+ nets and 4000 VRFs. Then the bgp instance is removed using "no router bgp <>"

  Workaround: Shut down the bgp neighbor sending big scale nets to remove the nets first from BGP and RIB. Then remove the BGP using "no router bgp <>".

- CSCun99811

  Symptom: If a Cisco IOS box does not support Ethernet Y.1731 delay DMM version 1 (DMMv1), but supports DMM version 0 (DMM), it will not respond to a box trying to run a DMMv1 session.

  Conditions: This symptom occurs with an initiator box running DMMv1 to a Cisco IOS box that supports DMM but does not support DMMv1. Rather than responding as though it were receiving DMMs version 0, as is the required behavior, the session will be rejected.

  Workaround: All boxes that support DMMv1 will also support DMM version 0, so this can be used between two boxes instead. The normal DMM version 0 restrictions apply in this case.

- CSCuo09249

  Symptom: An xTR changes its RLOC, map-request packets from that new RLOC are dropped on the MS/MR due to policy violation, for example:

  ```
  *Apr 2 15:29:15 JST: LISP-0: AF IID 100 IPv4, Map resolver filtered incoming map
  request from 2400:A:A:9999:C267:AFFF:FE52:287 because it does not conform to the
  configured allowed-locator policy.
  ```

  Conditions: This symptom is observed when {ipv4|ipv6} map-resolver map-request validate source registered is configured on the MS/MR and the xTR RLOC is updated, for example, by DHCP when the {ipv4|ipv6}-interface configuration is used in the database-mapping configuration. Both the new and the old RLOC must have been valid.

  Workaround: Remove and re-add database-mapping configuration on xTR, possibly using EEM script on address change Remove "{ipv4|ipv6} map-resolver map-request validate source registered" configuration on MS/MR clear lisp site <name> on the MS.

- CSCuo11238

  Symptom: Router crashes when removing address-family from VRF definition, or when removing the VRF definition.

  Conditions: This symptom is observed when PIM is configured for the LISP interface associated with the VRF.

  Workaround: Unconfigure LISP for the VRF, or remove PIM configuration from the LISP interface associated with the VRF, before removing VRF configuration.

- CSCuo12245

  ```
  Symptom: The following error message is observed with traceback :
  OCE_PUNT_PROCESS-3-LABEL_CACHE_INVALID: inlabel pointer was NULL
  ```

  Conditions: Multicast traffic is label switched in the mpls P2MP tree and replicated at branch bud nodes along the P2MP tree. The error condition is observed at a bud node, where the replicated traffic is dropped with the error.

  Workaround: There is no workaround.

- CSCuo15799

  Symptom: Memory leaks are observed on the node.

  Conditions: This symptom occurs with flaps in the REP segment generating TCNs that are being sent into a different REP segment.

  Workaround: There is no workaround.

- CSCuo21431

  Symptom: NTLM may not work properly.

  Conditions: This symptom occurs when the LDAP server goes down and comes up.

  Workaround: Add a new server as a part of the AAA group server ldap adgroup.

- CSCuo26634

  Symptom: Crash is observed.

  Conditions: This symptom is observed with command “sh frr-manager client client-name <name> det” when the client with the specified name does not exist.

  Workaround: There is no workaround.

- CSCuo34395

  Symptom: BFD OSPF client does not react at interface events on a remote endpoint.

  Conditions: This symptom occurs under the following conditions:

  – BFD is enabled - OSPF is enabled

  – One of the devices where BFD is enabled is running Cisco IOS Release 15.3(3)M2

  Workaround: There is no workaround.

- CSCuo35867

  Symptom:

  1. CPOS-based PPP serial interface is UP/DOWN; but HDLC is UP/UP; loopback local for PPP is also UP/DOWN.
  2. From debug, the following output is seen:

  ```
  *Apr 16 20:46:50.330: AAA/ID(00100066): PPP allocated ....
  ```

```
*Apr 16 20:46:50.831: CCM: Failed to create session, session already exists
<<<<<<<<<<<<
*Apr 16 20:46:50.831: AAA/ID(NA): PPP allocating
*Apr 16 20:46:50.831: CCM GROUP:ERROR group not found with shdb 0
*Apr 16 20:46:50.831: AAA/ID(NA): propagate hw:Se1/0/0.1/1/6/1:0,0x42352E64
sw:Se1/0/0.1/1/6/1:0,0x42353C48 other:nil base:nil unit:0/1 slot:1 shelf:0 tty:nil
*Apr 16 20:46:50.831: aaa_uid_propogate grabbed_id = 1048678
*Apr 16 20:46:50.831: AAA/ID(00100066): PPP allocated
*Apr 16 20:46:52.847: Se1/0/0.1/1/6/1:0 PPP: Missed a Link-Up transition, starting PPP
<<<<<<<<<<<<<
```

Conditions: This symptom occurs with PPP serial interface flapping.

Workaround: Chassis reload can temporarily make PPP interface UP/UP, but the problem will reoccur after a few days.

- CSCuo37123

  Symptom: High CPU is seen due to a PIM process after an SSO to standby RP. Huge PIM hello bursts can be seen from the router facing the issue. The severity and duration of high CPU can increase with the uptime of the active route processor.

  Conditions: This symptom occurs due to an SSO.

  Workaround: Disable PIM auto-rp “no ip pim auto-rp” if the CLI is available.

- CSCuo44562

  Symptom: The Cisco ASR 1000 Series Router crashes.

  Conditions: This symptom occurs with duty cycle testing with a lot of negative events.

  Workaround: There is no workaround.

- CSCuo47685

  Symptom: While evaluating the Cisco IOS Release 15.3(3)S3 early release image, the following error message was observed when using the CoPP configuration given below which matches based on precedence only as shown:

  ```
  class-map match-any coppclass-protocol match precedence 6 7
  ```

  ```
  "Match precedence in IPv4/IPv6 packets is not supported for this interface error:
  failed to install policy map CoPP"
  ```

  Upon occurrence, the entire CoPP policy map is not loaded. There is a concern that some field devices on the current release (Cisco IOS Release 15.0(1)S6) may have the above configuration and as such is prone to this error (CoPP installation failure during upgrade).

  Conditions: This symptom occurs while evaluating the Cisco IOS Release 15.3(3)S3 early release image.

  Workaround: There is no workaround.

- CSCuo48507

  Symptom: While testing ISSU from XE310<->XE311 with ikev2_dvti and GRE features, packet drops is observed after a switchover.

  Conditions: This symptom is observed during upgrade to Cisco IOS Release 3.11 and downgrade to Cisco IOS Release XE 3.10.

  Workaround: There is no workaround.

- CSCuo49923

  Symptom: Performing an ISSU upgrade with the CEF table consistency checkers enabled may result in a crash on “issu runversion”.

  Conditions: This symptom occurs with a Cisco Catalyst 6500 Series Switch running Cisco IOS Release 15.1(02)SY.

  Workaround: Turn off the CEF table consistency checkers before performing an ISSU upgrade.

- CSCuo51246

  Symptom: Traffic flow is not as expected when IPv6 policing is enabled on UUT.

  Conditions: This symptom is observed on loading the Cisco IOS Release 15.4(2.10)T image.

  Workaround: There is no workaround.

- CSCuo53561

  Symptom: BGP fails to apply an inbound route map on prefixes after a switch over.

  Conditions: This symptom occurs when NSR is enabled and RP switchover is performed twice.

  Workaround: Enable the knob “bgp sso route-refresh-enable” or manually do a soft refresh to get the routes back from NSR peers on the new active RP.

- CSCuo55180

  Symptom: A vulnerability in PPPoE processing code of Cisco IOS XE could allow an unauthenticated, adjacent attacker to cause a reload of the affected device and eventually a denial of service (DoS) condition.

  The vulnerability is due to improper processing of certain malformed PPPoE packets. An attacker could exploit this vulnerability by sending a malformed PPPoE packet to an IOS XE ASR1000 device, configured with PPPoE termination. An exploit could allow the attacker to cause a reload of the affected device and eventually a denial of service (DoS) condition.

  Conditions: Cisco ASR 1000 with IOS XE, configured for PPPoE termination.

  Workaround: There is no workaround.

  Further Problem Description: A device crashing, may print the following messages on the console:

  ```
  %SYS-3-OVERRUN: Block overrun at 7F7FAE750B58 (red zone 44534C5F00000000)
  %SYS-6-MTRACE: mallocfree: addr, pc ? %SYS-6-BLKINFO: Corrupted redzone blk
  7F7FAE750B58, words 404, alloc 6374D1B, InUse, dealloc 10001, rfcnt 1 ?
  %Software-forced reload
  Exception to IOS Thread: Frame pointer 0x7F7FA0AB5AD8, PC = 0x7F80A8469565
  UNIX-EXT-SIGNAL: Aborted(6), Process = Check heaps -Traceback=
  1#c3a5522ccb47820b036322d6b7226e1c c:7F80A8438000+31565
  Fastpath Thread backtrace: -Traceback= 1#c3a5522ccb47820b036322d6b7226e1c
  c:7F80A8438000+BDDD2
  Auxiliary Thread backtrace: -Traceback= 1#c3a5522ccb47820b036322d6b7226e1c
  pthread:7F80A3697000+A7C9
  ```

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.1/5: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:A/AC:L/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C

  CVE ID CVE-2014-3284 has been assigned to document this issue.

  Additional details about the vulnerability described here can be found at: http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-3284

Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCuo56173

  Symptom: When PW's remote peer is ALU, it takes 5 to 10 minutes for the PWs to come up.

  Conditions: This symptom occurs when Provision PW is done first on the ALU and then on the Cisco router.

  Workaround: Provision PW on the Cisco router first.

- CSCuo56871

  Symptom: A Cisco ASR 1001 router running Cisco IOS Release 15.2(4)S4 acting as a route server crashes when **clear bgp ipv4 unicast *** is executed.

  Conditions: This symptom occurs when a router is configured as as route server and a command executed in an IPv4 table is reset via **clear bgp ipv4 unicast ***.

  Workaround: Do not execute command **clear bgp ipv4 unicast ***. Instead, one could use the **clear ip bgp *** to hard reset all the BGP tables.

- CSCuo60344

  Symptom: With loss of traffic on primary flow in MoFRR, the secondary flow may not be treated as primary since it is random and the new flow may become the primary.

  Conditions: This symptom occurs in ECMP or TI flow based MoFRR and when there is a loss of primary flow.

  Workaround: There is no workaround.

- CSCuo66491

  Symptom: While using PfR, traffic classes oscillate from controlled to default to uncontrolled when probe creation fails for alternate external interfaces (due to lack of parent route).

  Conditions: This symptom does not occur under specific conditions.

  Workaround: Configure monitor mode active or monitor mode both instead of monitor mode fast.

- CSCuo72301

  Symptom: Crash occurs when IKEv2 attempts to clean up its contexts when it times-out waiting for received Certificate to be Validated by PKI component.

  Conditions: Authentication with certificates and PKI component's response to certificate validation is delayed.

  Workaround: There is no workaround.

- CSCuo72961

  Symptom: An error message is logged in during QoS configuration during an FPM test.

  Conditions: This symptom occurs due to a policy with FPM class.

  Workaround: There is no workaround.

- CSCuo75681

  Symptom: The RP crashes due to "%SYS-2-CHUNKBADMAGIC" in checkheaps.

  Conditions: This symptom does not occur under specific conditions.

  Workaround: There is no workaround.

- CSCuo83510

  Symptoms: A stack overflow and boot loop can occur when configuring OSPFv3 for IPv6 using a non-broadcast network type on IOS XE

  Conditions: SVI or Layer-3 Interface using the ospf non-broadcast network type.

  Workaround: Remove the non-broadcast network configuration.

  Further Problem Description: This issue was found during a security audit of the product.

  PSIRT Evaluation: The Cisco PSIRT has evaluated this issue and does not meet the criteria for PSIRT ownership or involvement. This issue will be addressed via normal resolution channels.

  If you believe that there is new information that would cause a change in the severity of this issue, please contact psirt@cisco.com for another evaluation.

  Additional information on Cisco's security vulnerability policy can be found at the following URL:

  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCuo83554

  Symptom: A vulnerability in the Autonomic Network Discovery Packets of Cisco IOS XE could allow an unauthenticated, adjacent attacker to receive arbitrary data from other traffic passing through the device

  The vulnerability is due to uninitialized memory used in packet creation. An attacker could exploit this vulnerability by capturing packets on the segment.

  Conditions: Device configured with default configuration.

  Workaround: Not applicable or available.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 3.3/3: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:A/AC:L/Au:N/C:P/I:N/A:N/E:POC/RL:U/RC:C

  No CVE ID has been assigned to this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCuo84660

  Symptom: The following error message is seen:

  ```
  *May 15 20:22:43.699: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error, -PC=
  :10000000+D90018 -Traceback= 1#10ebf8a777fd9b28d42b106d039edefc :10000000+78F240
  :10000000+78F5F0 :10000000+7B9268 :10000000+7548448 :10000000+D90018 :10000000+D8A6D0
  :10000000+D9B2C4 :10000000+DA3BEC :10000000+6A6DC4 :10000000+6ADDB0 :10000000+49DBB2C
  :10000000+6BF11C
  ```

  Conditions: This symptom occurs while updating the running configuration using any type of remote file transfer (via SNMP or copy command). When the source IP resolves to a DNS hostname longer than 63 bytes, an error message will be seen. There is no impact to the system. The running configuration will update as expected.

  Workaround: Copy the file to a local storage first and then copy it from the local storage to the running configuration.

- CSCuo86953

  Symptom: A Cisco router or switch may crash while issuing the **show logging** command.

Conditions: This symptom occurs while issuing the **show logging** command. Let the output of the **show logging** command remain at the more prompt in the trap logging session. While changing the **logging host** command in a different session, resume the output of the **show logging** command. There is a chance that both actions at the same time will make the device crash.

Workaround: Do not make changes to the **logging host** command while the output of the **show logging** command is still outstanding.

- CSCuo88282

  Symptom: A Cisco ASR router crashes.

  Conditions: This symptom occurs under the following conditions:

  Configure a DHCP database as follows: ip dhcp database tftp://192.168.50.100/dhcp write-delay 60 timeout 30 The router is unable to write the database as TFTP is not installed on 192.168.50.100 or TFTP IPis not reachable (both scenarios leading to crash). After a few seconds the router gets crashed.

  Workaround: There is no workaround.

- CSCuo91745

  Symptom: The black hole should not drop TC when TC is learnt at the beginning.

  Conditions: This symptom occurs when the black hole is added in the class as follows: class http sequence 10 match application http policy custom priority 1 one-way-delay threshold 100 path-preference SP1 fallback blackhole

  The HTTP traffic is added. When the TC is learning, it is uncontrolled and hence during this time traffic will be dropped. The dropping will start at the TC learnt and end at the TC controlled. The duration will be a minimum of 30s.

  Workaround: There is no workaround.

- CSCuo93299

  Symptom: ZTB does not work.

  Conditions: This symptom occurs when the image is loaded and left without aborting the setup dialogue box.

  Workaround: This issue has been fixed.

- CSCuo93711

  Symptom: RSVP HA Services leaks memory on the standby RP. Standby RP eventually hits the “out of memory” condition and will reload. There is no traffic impact as the active RP is not affected.

  Conditions: This symptom occurs when the **mpls traffic-eng nsr** command is configured.

  Workaround: There is no workaround.

  More Info: The leak is specific to MPLS-TE tunnel tails. A small memory block is leaked whenever a tunnel tail is setup or torn.

- CSCuo95313

  Symptom: Duplicate cookies are observed in every access request.

  Conditions: This symptom occurs when multilogon or logoff is performed on the same session.

  Workaround: Tear down the session during the logoff event. Do not configure any delay on the account logoff event.

- CSCuo96504

  Symptom: A FlexVPN client router may report alignment errors and experience high cpu utilization in IKEv2 FlexVPN process.

  Conditions: The tunnel interface in use with the FlexVPN client configuration must flap while the client is processing an IKEv2 redirect. The high cpu utilization is seen only if the client is configured to auto connect.

  Workaround: Remove and reconfigure the IKEv2 client configuration block.

- CSCuo97889

  Symptom: IPv4 and IPv6 traffic will be dropped after performing an SSO.

  Conditions: This symptom occurs when you perform an SSO with ISIS as NSR configured, and MPLS-TE as GR configured.

  Workaround: Change ISIS to non-NSR.

- CSCuo98907

  Symptom: Platform-specific images do not build.

  Conditions: This symptom occurs when any platform-specific image is built.

  Workaround: This issue is fixed.

- CSCup00882

  Symptom: A router running Cisco IOS experiences an unexpected reload after removing OSPF IPFRR or OSPF Remote LFA from the configuration.

  Conditions: This symptom occurs when the router was configured for OSPF IPFRR and, possibly, OSPF Remote LFA and IPFRR and (or) rLFA configuration commands are being removed at the same time when IPFRR SPF is running on the router.

  Workaround: There is no workaround.

  More Info: This symptom occurs if IPFRR SPF is running at the time the configuration is being removed.

- CSCup01885

  Symptom: A crash is observed due to a corrupted stack in AAA. This issue was observed on a Cisco ASR 1000 router when an authentication request was sent from IKE (crypto) with a password expiry feature configured.

  Conditions: The symptom is seen with the password expiry feature. The configuration needed is:

  ```
  aaa authentication login <method> passwd-expiry group <radius/tacacs>
  ```

  Workaround: Remove the configuration.

  More Info: With “aaa authentication login userauthen passwd-expiry group radius” configured, over a period of time, there is AAA stack corruption because of a value read from a wrong offset in the memory. It is not specific to any platform.

- CSCup08772

  Symptom: A Cisco device hangs.

  Conditions: This symptom occurs after a save and reload with intent configured.

  Workaround: There is no workaround.

  More Info:

  1. Configure registrar.

2. Configure intent.
3. Save and reload the device.

- CSCup09007

  Symptom: When a CEM interface is configured, the router crashes when it is unconfigured without logging out of the CEM configuration mode.

  Conditions: This symptom occurs when a CEM interface is configured and unconfigured.

  Workaround: Exit from the submode before performing **no xconnect**.

- CSCup10447

  Symptom: When an Any Transport over MPLS (AToM) xconnect is configured on a dual-RP system, memory leaks may be observed on the standby RP.

```
router-stby#sh memory debug leaks chunks Adding blocks for GD...
kernel memory
Address Size Alloc_pc PID Alloc-Proc Name
Chunk Elements:
AllocPC Address Size Parent Name
lsmpi_io memory
Address Size Alloc_pc PID Alloc-Proc Name
Chunk Elements:
AllocPC Address Size Parent Name
Processor memory
Address Size Alloc_pc PID Alloc-Proc Name
Chunk Elements:
AllocPC Address Size Parent Name NA 3DDDFCB4 180 3DDD06C0 (AToM VC binding) NA
3DDDFE24 180 3DDD06C0 (AToM VC binding) NA 3DDDFF94 180 3DDD06C0 (AToM VC binding) NA
3DDE0104 180 3DDD06C0 (AToM VC binding) NA 3DDE0274 180 3DDD06C0 (AToM VC binding) NA
3DDE03E4 180 3DDD06C0 (AToM VC binding) NA 3DDE0554 180 3DDD06C0 (AToM VC binding)
```

  Conditions: This symptom is observed when a label advertisement is received from the peer and checkpointed to the standby RP.

  Workaround: There is no workaround.

- CSCup21524

  Symptom: A crash is observed with the following error messages:

```
Exception to Fastpath Thread: Frame pointer 0x7FEA1735D570, PC = 0x7FEB1F732559
-Traceback= 1#bb8f9a461a7850b52eefb2d5dc713d87 c:7FEB1F701000+31559
c:7FEB1F701000+32A09 :400000+442C515 :400000+4430C38 iosd_unix:7FEB1FED3000+1B0B6
:400000+6D46665 :400000+7AD419 :400000+2534AFB :400000+4422F8B :400000+70D1E1F
:400000+7117396 :400000+71154E6 :400000+6D6801F :400000+6D6787F :400000+4417B48
:400000+441AE07
IOS Thread backtrace: UNIX-EXT-SIGNAL: User defined signal 2(12), Process = SSM
connection manager -Traceback= 1#bb8f9a461a7850b52eefb2d5dc713d87
pthread:7FEB1D279000+83BF
Auxiliary Thread backtrace: -Traceback= 1#bb8f9a461a7850b52eefb2d5dc713d87
pthread:7FEB1D279000+A7C9
```

  Conditions: This symptom occurs after a switchover from the active RP to the standby RP and the device has 1000 PPPoA sessions. Call Admission Control (CAC) is also configured.

  Workaround: Remove CAC configurations. For example:

  call admission new-model call admission limit 1000 call admission cpu-limit 80

- CSCup23792

  Symptom: A loss of service-group configuration under a subinterface is observed.

Conditions: This symptom occurs only when the router is reloaded. It is not seen with a particular LC reload where the interface exists.

Workaround: There is no workaround.

- CSCup33759

  Symptom: ISIS IPv6 distribute-list filters of the form:

  router isis address-family ipv6 distribute-list prefix-list {name} in {interface}

  should be removed from the configuration when the specified interface is deleted or is no longer enabled for IPv6. In some cases this is not happening, which can cause errors when a saved configuration is used during a subsequent reboot.

  On systems with a redundant RP, configuration sync will fail because the distribute-list command will be rejected by the standby RP.

  Conditions: This symptom is observed when using ISIS to route IPv6 traffic.

  Workaround: Ensure that IPv6 is enabled on any interfaces referenced by ISIS IPv6 distribute-list commands. This can be accomplished either by configuring one or more IPv6 addresses on the interface, or by using the command “ipv6 enable”.

- CSCup39674

  Symptom: A traceback is observed consistently during a cleanup.

  Conditions: This symptom occurs when MPLS-TP tunnels are configured and unconfigured.

  Workaround: There is no workaround.

- CSCup47507

  Symptom: In Cisco IOS Release 15.4(3)S or Cisco IOS XE Release 3.13S, the ISIS **summary-address** and **summary-prefix** commands are not synchronized to the standby RP.

  Conditions: The symptom is seen on a router with redundant RPs.

  Workaround: There is no workaround.

- CSCup49636

  Symptom: Estimated Channel Egress Bandwidth gets accounted incorrectly with fast-monitor enabled per DSCP.

  ```
  For example, with monitor-interval as 1s, all TCs on SP1, Total TC BW: 18Mbps, then
  Estimated Channel BW: 540Mbps;
  ```

  Conditions: This symptom occurs when fast-monitor gets enabled for a specific DSCP channel.

  Workaround: There is no workaround.

Bugs for Cisco IOS Release 15.4(2)S

Open and Resolved Bugs

The open and resolved bugs for this release are accessible through the Cisco Bug Search Tool. This web-based tool provides you with access to the Cisco bug tracking system, which maintains information about bugs and vulnerabilities in this product and other Cisco hardware and software products.

Within the Cisco Bug Search Tool, each bug is given a unique identifier (ID) with a pattern of CSCxxNNNNN, where x is any letter (a-z) and N is any number (0-9). The bug IDs are frequently referenced in Cisco documentation, such as Security Advisories, Field Notices and other Cisco support documents. Technical Assistance Center (TAC) engineers or other Cisco staff can also provide you with the ID for a specific bug.

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

Note 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:

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

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 Bug Search Tool Help & FAQ
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 this 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	15.4(2)S2
Status	Fixed
Severity	2 or higher

Resolved Bugs—Cisco IOS Release 15.4(2)S4

Table 1 Resolved Bugs—Cisco IOS Release 15.4(2)S4

Identifier	Description
CSCuu93699	Crash on IKEv2 cluster hub when anyconnect client tries reconnect
CSCuq46955	IOS ISR AM IKEv1 doesnt work with rsa-sig
CSCus19794	Cisco IOS and IOS XE IPv6 SEND Denial of Service Vulnerability
CSCuu82607	Evaluation of all for OpenSSL June 2015
CSCuq74492	IOS/IOSd Multiple Vulnerabilities in OpenSSL - August 2014
CSCus61884	JANUARY 2015 OpenSSL Vulnerabilities
CSCut46130	MARCH 2015 OpenSSL Vulnerabilities

Resolved Bugs—Cisco IOS Release 15.4(2)S3

Table 2 Resolved Bugs—Cisco IOS Release 15.4(2)S3

Identifier	Description
CSCug18580	ASR1k crash: UNIX-EXT-SIGNAL SEGFAULT, Process = AAA ACCT Proc
CSCur51387	NG3K stack: standby gets reloaded due to reason "configuration mismatch"
CSCur27466	WebUI in IOS-XE : evaluation of SSLv3 POODLE vulnerability
CSCup62315	Autonomic Networking Infrastructure Device Reload DoS Vulnerability
CSCup62191	Autonomic Networking Registration Authority Spoofing Vulnerability
CSCuq35209	BGP advertising incorrect Link Local ipv6 address
CSCuq83441	BGP L2VPN uses default static next-hop instead of outging intf-addr
CSCuq99797	BGP Route-Target not advertised when rtfilter address family in use
CSCuq13985	BGP Router process crash due to recevied BGP withdraw
CSCur66140	Import of Global routes to VRF will fail
CSCuq24984	In rare high BGP update churn case, sh ip bgp x.x.x.x may crash

Identifier	Description
CSCun68322	Support BGP GR for VPN AF in platform without MPLS
CSCuo66933	Switch sent Failure packet after reboot and caused PC to fail authen
CSCus57583	ASR 1K BGP Process Crash Due to EIGRP Route Redistribution
CSCur13495	Service-data of a service change is not updated by SAF forwarder
CSCuq93406	IOSd crash on Ethernet CFM receiving a malformed CFM frame
CSCur43251	POODLE protocol-side fix: HTTPS Client
CSCuo84660	copy command yields DATACORRPUTION error
CSCuq96691	Utah crash during ezconfig installation.
CSCuq17828	ASR: Radius Accounting fails when using EDCSA certs
CSCum90471	ASR1k: Ping failure b/w CE1 & CE3 after Switchover.
CSCus48386	POODLE related fix : LDAPv3 client REQUIRED to support TLS
CSCur36464	mVPN: Inter-AS Option B: Different RDs: proxy vector: local RD is picked
CSCur09682	Router crashes in PIM due to infinite recursion at ip_set_mdb_flag
CSCuq57261	cBR-8 SUP HA Long M-BGP and LDP Resync Delay
CSCur92862	TE leaks memory when restarting isis
CSCul73513	Clock is not matching between server-client after leap configuration
CSCuo29389	NTP clients of 3900 loses sync sporadically,due to high offsetvariations
CSCun62014	Router crash with %SYS-3-BADFREEPTRS after reconfiguring pppoe
CSCut14355	GETVPN - IOS-XE using SW-TCAM - Deny policy classification incorrect
CSCus95855	ISR4451 FMAN-FP Crash
CSCus01735	cbQosTSCfgRate64 is not supported on ASR1k/IOSXE
CSCum87411	software install from tftp get failed fts_client issue
CSCuq41114	ENH: SSH configuration option to restrict cipher public key and HMAC
CSCur23656	Cisco IOS and IOSd in IOS-XE : evaluation of SSLv3 POODLE vulnerability
CSCur44075	AC ICE+ ver <= 4.0 Client unable to connect to XE SSL Headend {CSR1K}
CSCup86552	Issue with qos service installation
CSCuh92882	XE3.11 Seginfo->l2hw_cond_debug is set to "1" when there is no condition
CSCup52725	XE3.13: asr1k RP Crash while 72 hour longevity run
CSCum94811	TCP Packet Memory Leak Vulnerability
CSCup41482	TCP snd window stuck with CEF enabled
CSCuh09324	udp entries not deleted from flowmgr table
CSCus47361	DSMP statistic request timeout cause 4 more seconds to disconnect

Resolved Bugs—Cisco IOS Release 15.4(2)S2

All resolved bugs for this release are available in the Cisco Bug Search Tool through the fixed bug search.

Resolved Bugs—Cisco IOS Release 15.4(2)S1

- CSCee32792

  Symptom: A Cisco router reloads at snmp_free_variable_element while using SNMPv3 commands.

  Conditions: This symptom occurs while using SNMPv3 commands.

  Workaround: There is no workaround.

- CSCtz45833

  Symptom: A Cisco router crashes with the following message:

  ```
  Router crash: UNIX-EXT-SIGNAL: Segmentation fault(11), Process = MPLS TE LM
  ```

  Conditions: This symptom occurs when a router acts as the mid point for MPLS-TE tunnels and performs an ERO expansion. In case the ERO expansion fails (due to IGP race conditions or inter-AS scenario) and backup tunnels are in use (for MPLS-TE FRR feature), the router may crash.

  Workaround: Configure the head-ends to perform a full ERO computation to avoid mid points performing any ERO expansion. This can be done using the dynamic path option or by using the explicit path that specifies strict hops for each node along the desired LSP path (using “loose” hops or partial strict hops can lead to this issue).

- CSCuc60868

  Symptom: A router randomly crashes either due to memory corruption at bgp_timer_wheel or memory chunks near bgp_timer_wheel (For example, BFD event chunks if BFD is configured or AtoM Manager chunks if LDP is configured). A crash occurs right after an LDP neighbor is up in the L2VPN setup.

  Conditions: This symptom occurs when **vpls bgp signaling** is unconfigured and then reconfigured. Both L2VPN and BGP are unconfigured and reconfigured after all L2VPN and BGP data structures are fully deleted (about 3 minutes for 5 BGP VPLS prefixes). For the repro on file, OSPF (for IGP) is also unconfigured and reconfigured. Both LDP and BGP signaling are affected by this bug.

  Workaround: Avoid unconfiguring and reconfiguring BGP L2VPN.

- CSCue23898

  Symptom: A Cisco router running Cisco IOS Release 15.3(1)T may crash with a bus error immediately after issuing the **write memory** command.

  ```
  Example: 14:44:33 CST Thu Feb 14 2013: TLB (load or instruction fetch) exception, CPU
  signal 10, PC = 0x228B2C70
  ```

  Conditions: This symptom occurs while updating the router’s running configuration with the **write memory** command. It has been seen while updating various different commands such as, those under “call-manager-fallback” ip route statements interface sub-commands.

  Workaround: There is no workaround.

- CSCug17485

  Symptom: A buffer leak is observed on a Cisco router.

  Conditions: This symptom occurs while using SSLVPN.

  Workaround: There is no workaround.

- CSCug45421

  Symptom: The standby RP crashes.

Conditions: Memory corruption occurs in certain cases when the following commands are executed in quick succession. It leads to a crash later when the memory is accessed. The issue is seen only with on-demand PVCs and when the commands are copied and pasted or executed using a script or tool.

```
configure terminal
interface ATM0/0/0.2 multipoint
range pvc 11/41 11/51
create on-demand
/* Prob commands begin */
pvc-in-range 11/45
exit
no pvc-in-range 11/45
/* Prob commands end */
end
```

Workaround: Do not execute the commands in quick succession.

- CSCuh09324

  Symptom: UDP based entries are not deleted from the flowmgr table resulting in crash, or poor system response, with CPU hog messages being shown.

  Conditions: This symptom occurs in the following images

  - ct5760-ipservicesk9.bin
  - cat3k_caa-universalk9.bin
  - cat4500e-universalk9.bin

  The device is configured with UDP services that originate from the device. This includes but not limited to the following features:

  - TFTP
  - Energy Wise
  - DNS
  - Cisco TrustSec

  Workaround: If you suspect that you are affected by this bug, please do the following, for confirmation:

```
Router#config terminal
service internal
end
Router#show flowmgr
```

  The output of this command will show many lines entries holding with the same port numbers. Disabling the feature that is being held in the flows until an upgrade can be performed, is a workaround.

  A reload is required to clear the held flows.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5.4/4.5: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:H/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C

  CVE ID CVE-2013-6704 has been assigned to document this issue.

  Additional details about the vulnerability described here can be found at: http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2013-6704

Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCui05000

  Symptom: A Cisco router may crash upon importing a prefix into VRF after applying **no ipv4 multicast multitopology** under "vrf definition" for that VRF.

  Conditions: This symptom occurs while initially configuring the VRF. **address-family ipv4/6 multicast vrf** must be configured under "router bgp" mode before import route-targets are configured under "vrf definition" mode.

  Workaround: There is no workaround.

  More Info: If the crash does not occur, it is likely that importing of the prefix will not work.

- CSCui29745

  Symptom: Member links under MLPPP go down as the LCP negotiation of those PPP links fails.

  Conditions: This symptom occurs after the router reloads and the traffic is flowing through the multilink.

  Workaround: Reload SPA/LC on the other end of the link.

- CSCui34165

  Symptom: Port-channel QoS features might fail to work after a router reload, followed by QoS configuration modification.

  Conditions: This symptom occurs when a vlan load-balanced port-channel is used with policy aggregation configuration where the QoS policy is configured on member links and the port-channel sub-interface, and after a system reload (configuration is from startup configuration).

  Workaround: Reload the router without port-channel QoS configuration, and add port-channel QoS configuration to the running configuration after the router boots up.

- CSCui59984

  Symptom: REP FLAPs with low LSL timers with the following scale:

  1. Scale of MAC address OR
  2. Scale of Bridge-domain OR
  3. Repeated/multiple REP topology changes OR
  4. CPU-intensive activities.

  Conditions: This symptom occurs with REP configured with low LSL age timer with scale of configuration or any CPU-intensive activities.

  Workaround: Use default LSL timers.

- CSCui64807

  Symptom: An active RP crashes during FIB sync because of memory overrun when the standby sup becomes unavailable.

  Conditions: This symptom occurs when redundant RPs are configured in SSO mode and the standby RP becomes unavailable (for instance because of crash or physical removal). The issue occurs only on Cisco 7600 RSP 720, Cisco 7600 Series Supervisor Engine 720, and Cisco 7600 platforms where the tableid "ISSU FOF LC" support is enabled. As of 03/17/2014, the tableid "ISSI FOF LC" feature is only supported on SY releases. This issue does not impact Cisco ASR 1000 Series platforms.

  Workaround: There is no workaround.

- CSCul22914

  Symptom: A Cisco router does not give the necessary failure information if the crypto NIST/KAT tests on boot fail. During test failures, users will not be notified. The logs do not contain information on the failures.

  Conditions: This symptom occurs with a crypto NIST/KAT self test. The message below is a generic message and is not specific to a crypto self test failure.

  ```
  *Nov 5 17:48:19.128: %CMRP-3-CHASSIS_MONITOR_READY_TIME_EXCEEDED:cmand: Reloading F0
  because it has failed to become ready for packet processing
  ```

  This message does not give enough information for the user to take a proper course of action.

  Workaround: There is no workaround.

  More Info: A failure in one of the POST Known Answer Test (KAT) test during boot-up triggers this issue. The issue will not occur if all the KAT tests are passes.

- CSCul24443

  Symptom: A Cisco router crashes while scaling service instances to 3600 whenever the memory is utilized fully and it throws an error as there is no memory to display the output of the **show running** command.

  Conditions: This symptom occurs when the service instance is scaled to 3600.

  Workaround: Reload the router.

- CSCul27924

  Symptom: Customer experienced crash on ASR-1001 during normal operation.

  Conditions: This symptom is not observed under any specific condition.

  Workaround: There is no workaround.

- CSCul29918

  Symptom: A vulnerability in IPSec tunnel implementation of Cisco IOS Software could allow an unauthenticated, remote attacker to change the tunnel MTU or path MTU and potentially cause IPSec tunnel to drop.

  The vulnerability is due to incorrect processing of certain ICMP packets. An attacker could exploit this vulnerability by sending specific ICMP packets to an affected device in order to change the configured MTU value of the tunnel interface. An exploit could allow the attacker to change the tunnel MTU or path MTU and potentially cause IPSec tunnel to drop.

  Conditions: This symtpom occurs on a device configured for IPSec VTI and with path-mtu-discovery disabled.

  Workaround: The issue is caused by ICMP unreachables. Blocking ICMP is a workaround.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4.3/4.1: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:N/A:P/E:F/RL:U/RC:C

  CVE ID CVE-2013-6694 has been assigned to document this issue.

  Additional details about the vulnerability described here can be found at: http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2013-6694

  Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCul39964

  Symptom: Sessions do not get cleared. They get stuck in WT_ST state.

  Conditions: This symptom occurs when sessions are closed in bulk mode by shutting any trunk link or during a clear all session from DUT.

  Workaround: There is no workaround.

  More Info: The memory leak issue and WT_ST are related. Along with memory leak, sessions are not cleared on the active RP as they get stuck in WT_ST state.

```
asr1k-1#sh clock
07:18:07.045 CET Thu Nov 14 2013
asr1k-1#su
PTA : Locally terminated sessions
FWDED: Forwarded sessions
TRANS: All other sessions (in transient state)
TOTAL PTA FWDED TRANS
TOTAL 14465 0 6557 7908
GigabitEthernet0/0/0 3024 0 0 3024
GigabitEthernet0/0/1 2587 0 0 2587
GigabitEthernet0/1/0 2297 0 0 2297
GigabitEthernet0/1/1 6557 0 6557 0
asr1k-1#
asr1k-1#
asr1k-1#
asr1k-1#sh clock
07:20:08.295 CET Thu Nov 14 2013
asr1k-1#su
PTA : Locally terminated sessions
FWDED: Forwarded sessions
TRANS: All other sessions (in transient state)
TOTAL PTA FWDED TRANS
TOTAL 14465 0 6557 7908
GigabitEthernet0/0/0 3024 0 0 3024
GigabitEthernet0/0/1 2587 0 0 2587
GigabitEthernet0/1/0 2297 0 0 2297
GigabitEthernet0/1/1 6557 0 6557 0
asr1k-1#
asr1k-1#
asr1k-1#sh clock
07:46:34.113 CET Thu Nov 14 2013
asr1k-1#su
PTA : Locally terminated sessions
FWDED: Forwarded sessions
TRANS: All other sessions (in transient state)
TOTAL PTA FWDED TRANS
TOTAL 14465 0 6557 7908
GigabitEthernet0/0/0 3024 0 0 3024
GigabitEthernet0/0/1 2587 0 0 2587
GigabitEthernet0/1/0 2297 0 0 2297
GigabitEthernet0/1/1 6557 0 6557 0
asr1k-1#
asr1k-1#s
6557 sessions in FORWARDED (FWDED) State
7908 sessions in WAITING_FOR_STATS (WT_ST) State
14465 sessions totalUniq ID PPPoE RemMAC Port VT
VA State
SID LocMAC VA-st Type
5978 5978 0000.6ca3.0116 Gi0/0/0.2940148 1 Vi2.3091 WT_ST
b414.8901.8e00 VLAN: 294/148 UP
5979 5979 0000.6ca3.0117 Gi0/0/0.2940149 1 Vi2.3092 WT_ST
b414.8901.8e00 VLAN: 294/149 UP
6460 6514 0000.6ca3.0134 Gi0/0/0.2940178 1 Vi2.3354 WT_ST
```

```
b414.8901.8e00 VLAN: 294/178 UP
6454 6508 0000.6ca3.0135 Gi0/0/0.2940179 1 Vi2.3350 WT_ST
b414.8901.8e00 VLAN: 294/179 UP
6453 6507 0000.6ca3.0136 Gi0/0/0.2940180 1 Vi2.3349 WT_ST
b414.8901.8e00 VLAN: 294/180 UP
6518 6572 0000.6ca3.0137 Gi0/0/0.2940181 1 Vi2.3395 WT_ST
b414.8901.8e00 VLAN: 294/181 UP
6514 6568 0000.6ca3.0138 Gi0/0/0.2940182 1 Vi2.3393 WT_ST
b414.8901.8e00 VLAN: 294/182 UP
6516 6570 0000.6ca3.0139 Gi0/0/0.2940183 1 Vi2.3394 WT_ST
b414.8901.8e00 VLAN: 294/183 UP
6560 6614 0000.6ca3.013a Gi0/0/0.2940184 1 Vi2.3413 WT_ST
```

- CSCul49375

  Symptom: The Cisco ASR 1000 router displays the following messages in the logs:

  ```
  %IDMGR-3-INVALID_ID: bad id in id_get (Out of IDs!) (id: 0x0) -Traceback=
  1#cb40dca901558e45a65b881a8695af4f :400000+8653B3 :400000+893696 :400000+DF330C
  :400000+DED89B :400000+DF8643 :400000+1F57F36 :400000+1F4BBFB :400000+1F33BA7
  :400000+1F336C1 :400000+1F34FF9 :400000+1F27763 :400000+1F29B16 :400000+2546FF3
  :400000+2546EDD :400000+1F2930B
  ```

  No new PPPoE sessions can be established anymore.

  Conditions: The conditions to this symptom are unknown.

  Workaround: Reload the device.

- CSCul94606

  Symptom: Standby CUBE crashes while handling an agent transfer.

  Conditions: This symptom is observed when an agent transfers the call to another agent.

  Workaround: There is no workaround.

- CSCum09990

  Symptom: Basic mgcp t38-fax call fails between T1/cas endpoints as call not getting confirmed at terminating end.

  Conditions: This symptom occurs on Cisco 2900 routers which have been booted with Cisco IOS Release 15.4(1.14)T images.

  Workaround: There is no workaround.

- CSCum14830

  Symptom: Leaking IPv6 routes is observed from a VRF table into the global table using BGP. These routes consist of the following:

  1. BGP routes learned from the VRF IPv6 BGP peer.
  2. Redistributed static and connected routes.

  The BGP routes leak fine, but the redistributed static and connected routes have an issue. After the redistributed routes leak, the exit interface shows “null0”. Sometimes instead of showing the exit interface as “null0”, it shows a random interface which is a part of VRF and has IPv6 enabled on it.

  Conditions: This symptom occurs with IPv6 redistributed connected and static routes into BGP VRF (could also be redistributed from other protocols as well but have not been tested).

  Workaround: There is no workaround.

- CSCum20647

  Symptom: A traceback is seen in fn_resiliency_phase2 Script Cisco XE3.12/PI24 Release.

Conditions: A traceback is seen in fn_resiliency_phase2 Script Cisco XE3.12/PI24 Release. Functionality test is going fine but test fail when routers health check is done during cleanup.

Workaround: There is no workaround.

More Info: The issue seen only when GETVPN group is removed.

- CSCum33167

  Symptom: When PPPoE-IA is enabled, a Cisco switch forwards PADR/PADT packets to an untrusted port.

  Conditions: This symptoms occurs under the following conditions:

  – Configure PPPoE IA globally on node 1.

  – Configure service instance on interface gig0/1,gig 0/2 and gig 0/3.

  – Configure PPPoE IA on the interface and on the service instance.

  – Configure gig 0/1 and gig 0/3 as an untrusted port and gig 0/2 as a trusted port.

  – Send a PADI Packet from client 1 and send a PADO packet from the server.

  The PADO packet is received on client 2, but it should be received only on client 1. Send a PADR packet from client 1, client 2 also receives the packet. But it should not receive the packet. The PADR/PADT packet should be forwarded only to a trusted port.

  Workaround: There is no workaround.

- CSCum40306

  Symptom: A Cisco router crashes during call transfer in SRST mode.

  Conditions: This symptom is observed during call transfer in SRST mode, including SCCP phones.

  Workaround: There is no workaround.

- CSCum48221

  Symptom: 3560CG box memory is showing as low as 3.15MB.

  Conditions: This symptom is not observed under any specific conditions.

  Workaround: There is no workaround.

- CSCum52216

  Symptom: After a reload, **ip pim sparse-mode** is gone on interface lisp 0.x (x denoted the LSIP interface number).

  Conditions: This symptom occurs after a reload.

  Workaround: There is no workaround.

- CSCum60848

  Symptom: Under certain conditions, a DSP will hang in certain call scenarios including REFER passthrough.

  Conditions: This symptom is observed under heavy load.

  Workaround: There is no workaround.

- CSCum61595

  Symptom: Alignment errors are observed after upgrading to Cisco IOS Release 15.2(4)M5.

```
Jan 9 19:42:59.623 GMT: %ALIGN-3-CORRECT: Alignment correction made at 0x6477F81Cz
reading 0x6BE87495 Jan 9 19:42:59.623 GMT: %ALIGN-3-TRACE: -Traceback= 0x6477F81Cz
0x647805D0z 0x6478FE70z 0x64751088z 0x64B99F4Cz 0x64B99FD4z 0x64752 284z 0x647525ACz
```

Conditions: This symptom does not occur under specific conditions.

Workaround: There is no workaround.

- CSCum62783

  Symptom: The following alignment errors are seen after a PPPoE session establishment for the first time after a reboot:

  ```
  *Jan 14 07:24:40.591: %ALIGN-3-CORRECT: Alignment correction made at 0x32B2DFF4z
  reading 0xE7790ED *Jan 14 07:24:40.591: %ALIGN-3-TRACE: -Traceback= 0x32B2DFF4z
  0x32B1E274z 0x32B1EECCz 0x32B1EF90z 0x332E550Cz 0x332E54F0z 0xFFFF1A00z 0xFFFF1A00z
  ```

  Conditions: This symptom occurs when **pppoe-client ppp-max-payload** is configured under the Ethernet interface.

  Workaround: There is no workaround.

- CSCum66102

  Symptom: A Cisco router may crash when the CLI i**p nbar custom** <*name*> <*byte-offset*> **ascii** <*pattern*> **tcp** <*port*> is used. The crash occurs only when the ascii flavor of the **ip nbar custom** command is used.

  Conditions: This symptom is not observed under any specific conditions. It occurs on all types of ASR and ISR-G2 routrs as well as on 7200.

  Workaround: Avoid using the ascii flavor of the **ip nbar custom** command (Example: i**p nbar custom** <*name*> <*byte-offset*> **ascii**)

- CSCum67229

  Symptom: Entitymib does not respond for OC3/OC12/T3/E3 controller ports on the Cisco ME3600x-24CX-M platform.

  Conditions: This symptom occurs with the Cisco ME 3600X-24CX-M platform running Cisco IOS XE Release 3.10.

  Workaround: There is no workaround.

- CSCum81041

  Symptom: One way audio incoming calls redirected through CVP.

  Conditions: Call flow: ------------

  ```
  Caller----G711----TDM GW----SIP-----ASR1K----SIP-----CUSP----SIP----CVP(Vz0)----IP-IVR
  | | -----SIP---CVP (BAMS) | |--------SIP---CUCM---Agent Phone (G729 only)
  ```

  Initially the caller is connected to IP-IVR, both ingress and egress leg of the CUBE is doing G711. Call is connected to the IP-IVR, then CVP sends a refer to the VXML GW for playing prompts and ringback tone etc. When the call is transferred to the agent, CUBE negotiated G729 at the sip level with the CVP, but because of mid-call signaling block on the ingress side, continue with the G711. Hence xcoder is invoked on the CUBE to handle G729 to G711 and vise versa, but CUBE is still sending G711 media to the agent phone side while the agent phone is sending G729 media to the CUBE.

  Workaround: There is no workaround.

- CSCum84999

  Symptom: SUBSCRIBE received from CVP after BYE and NOTIFY with subscription-state : terminates is send by CUBE.

  Conditions: This symptom is observed when SUBSCRIBE IS received after call is terminated with BYE.

Workaround: There is no workaround.

- CSCum85493

  Symptom: Ping fails with tunnel protection applied.

  Conditions: Tunnel protection applied on GRE tunnel interface, using IKEv1 to negotiate IPsec SAs and remote node (IKEv1 responder) behind NAT.

  Workaround: The users can switch to IKEv2.

- CSCum85813

  Symptom: Shut primary static router and secondary static is not installed automatically.

  Conditions: This symptom is seen on the sites where the BFD state of the backup static route is marked as “U” in the output of **show ip static route bfd**.

  Workaround: Reinstall the default backup static route.

- CSCum94228

  Symptom: Local CAC displaying all information about each flows. This may impact show output for customer in a set up where we could possibly have large number of flows.

  Conditions: This symptom is observed in a scaled configuration.

  Workaround: There is no workaround.

- CSCum95078

  Symptom: Large IPSEC packets get dropped when fragmentation is done after IPSEC encapsulation.

  Conditions: This symptom is not observed under any specific conditions.

  Workaround: There is no workaround.

- CSCum95330

  Symptom: Removing an Ethernet service instance which is a member of a bridge domain may cause the router to reload.

  Conditions: This symptom is observed when the last service instance is removed from the bridge domain and there are still members of the bridge domain which are not service instances (such as VFIs).

  Workaround: Completely unconfigure the bridge domain and reconfigure it.

- CSCun02605

  Symptom: ASR crashes with no known trigger in CCSIP_SPI_CONTROL process.

  Conditions: It is an error scenario where crash occurs when router is not able to send ACK for 200 OK where branch parameters differ.

  ```
  CUBE INVITE | INVITE (Via branch=ABC) ----------------------------->|
  ----------------------------------------> | 200 OK (Via branch=DEF) |
  <----------------------------------------- |
  ```

  Cube fails to send ACK to 200 OK for some reason and causes a crash

  Workaround: There is no workaround.

- CSCun07843

  Symptom: A critical alarm is observed on the FPGA port 0/5/0.

  Conditions: This symptom occurs after performing an SSO.

  Workaround: There is no workaround.

- CSCun10381

  Symptom: A traffic drop was observed because labels do not get programmed.

  Conditions: This symptom occurs when scalable EoMPLS with L3VPN is configured. When notifications on atom-imps arrive, they have to get programmed.

  Workaround: Clear ip route.

  More Info: Traffic was seen to be dropped as the atom-imps could not be programmed because label entry could not be found for the atom-imps.

- CSCun11782

  Symptom: Rtfilter prefixes are sent with incorrect next-hop equal to next-hop of the default static route in GRT instead of BGP router-id.

  Conditions: This symptom occurs with a default static route present in GRT pointing, for example, to the next-hop known behind the connected interface.

  Workaround: Replace the default static route with a more specific static route or remove static and clear BGP.

- CSCun13688

  Symptom: The Cisco Catalyst 6500 Supervisor Engine 2T with CLNS routing configured crashes after **show clnbs route**.

  Conditions: This symptom occurs when CLNS routing is configured.

  Workaround: There is no workaround.

- CSCun20187

  Symptom: HSRP communication fails between two PEs (Cisco 7600 Series router) right after removing a neighbor from VFI.

  Conditions: Assume that a VPLS circuit is running between more than two PEs say A,B, and C and HSRP is running between A and B. Removing VPLS peer C on either A or B would cause HSRP communication failure between A and B. This failure is not expected as data path is still available between A and B.

  Workaround: Perform shut/no shut on the SVI.

- CSCun21602

  Symptom: Traffic is not forwarded by the router out of any interface.

  Conditions: This symptom occurs on toggling of the **ip routing** command in global configuration mode.

  Workaround: Perform shut and no shut of the interface which is involved in forwarding or reload the device with **ip routing** enabled.

- CSCun31021

  Symptom: A vulnerability in IKE module of Cisco IOS and Cisco IOS XE could allow an unauthenticated, remote attacker to affect already established Security Associations (SA)..

  The vulnerability is due to a wrong handling of rogue IKE Main Mode packets. An attacker could exploit this vulnerability by sending a crafted Main Mode packet to an affected device. An exploit could allow the attacker to cause dropping of valid, established IKE Security Associations on an affected device.

  Conditions: This symptom occurs on a device configured to process IKE request that already has a number of established security associations.

  Workaround: There is no workaround.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4.3/3.6: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:N/A:P/E:F/RL:OF/RC:C

CVE ID CVE-2014-2143 has been assigned to document this issue.

Additional details about the vulnerability described here can be found at: http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-2143

Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCun31359

  Symptom: Memory corruption crash while processing the sip-profile rule.

  Conditions: This symptom occurs on a Cisco 3900 device running Cisco IOS Release 15.3(1)T.

  Workaround: Perform the following workaround:

  – Using history-info pass-through feature (voice service voip -> sip -> history-info)

  – Using header pass-through feature

- CSCun31450

  Symptom: CPU hog followed by crash.

  Platforms affected are:

  – ct5760-ipservices.bin

  – cat3k_caa-universalk9.bin

  – cat4500e-universalk9.bin

  Conditions: This issue occurs while running udp IP SLA applications.

  Workaround: There is no workaround.

- CSCun35055

  Symptom: The RPF is not cleared when the internal VLAN is freed by shutting down an interface with RPF configuration. This affects the new interface assigned with this internal VLAN.

  Conditions: This symptom occurs when an interface with RPF configuration is shut down.

  Workaround: Flap the RPF configuration for the new interface.

- CSCun35070

  Symptom: Targeted LDP sessions between Customer Edge devices will flap every 3 minutes. IGP, Interface LDP between CE devices will run fine.

  Conditions: This symptom occurs when an MPLS LDP packet is carried over an L2VPN cloud with the control word OFF.

  Workaround: Configure the control word ON in an L2VPN cloud.

- CSCun36655

  Symptom: If the terminal adjacency of a lisp interface is removed and then re-added, the lisp interface MTU may remain at the invalid value of 65535. This can be seen in the **show cef interface** <*intf*> **internal** command output.

  IPsec will obtain the MTU value from CEF and LISP, and the incorrect MTU will cause drops of large packets.

IPSEC MTU incorrectly computed - causing packet drops on large packets traversing from “inside” to “outside” are dropped.

Conditions: This symptom is observed in the following Cisco C800 Series:

Cisco IOS Software, C890 Software (C890-UNIVERSALK9-M), Version 15.3(3)XB12, RELEASE SOFTWARE (fc2)

Workaround: A workaround is to toggle the IP MTU config on the lisp interface. Use “show run lisp0.1” to determine the MTU. Then use “ip mtu <mtu>” to first set it to a lower value, and then to set it back to the original value.

```
Example:
sh run interface lisp0.1
interface LISP0.1
ip mtu 1398
crypto map CM
end

conf t
interface lisp0.1
ip mtu 1200
ip mtu 1398
```

More Info: Originally [Cisco IOS Release 15.3(1)T] the MTU was accurately computed as:

```
RTR13-xTR#sh cry ipse sa vrf DeptA | in mtu
    path mtu 1456, ip mtu 1456, ip mtu idb LISP0.1
    path mtu 1456, ip mtu 1456, ip mtu idb LISP0.1
    path mtu 1456, ipv6 mtu 1456, ipv6 mtu idb LISP0.1
    path mtu 1456, ipv6 mtu 1456, ipv6 mtu idb LISP0.1
RTR13-xTR#
```

In 153-3.XB12, the MTU is as follows:

```
!RTR#show crypto ipsec sa | inc mtu
!     plaintext mtu 65458, path mtu 65535, ip mtu 65535, ip mtu idb LISP0
```

- CSCun36866

  Symptom: A Cisco router providing Layer 2 EoMPLS services may stop forwarding ingress and egress traffic for an xconnect for which a backup peer configuration has been applied.

  Conditions: This symptom occurs in Cisco 7600 Series routers and Cisco ASR 1000 Series routers running Cisco IOS Release 15.3(3)S or 15.4(02)S with xconnect configured under a service instance.

  Workaround: Clear the xconnect on the Cisco 7600 router side. Clearing the remote side does not have an effect.

- CSCun41292

  Symptom: On a Cisco ASR 1001 router running Cisco IOS Release 15.3(1)S, a crash occurs when the “show ip ei vrf X topo X.X.X.X/X” command is executed. The X.X.X.X/X must be in “FD is infinity” status in EIGRP as CSCtz01338.

```
asr1001_bew_03# show ip ei vrf * to all |
i Infinity P 174.162.XX.XX/24, 0 successors, FD is Infinity, U, serno 37, refcount 1
snip P 174.180.XX.XX/29, 0 successors, FD is Infinity, U, serno 46, refcount 1
asr1001_bew_03#show ip ei vrf 1 to 174.162.XX.XX/24
Exception to IOS Thread: Frame pointer 0x7F63DF6602D0, PC = 0x1956C8D
UNIX-EXT-SIGNAL: Segmentation fault(11), Process = Exec -Traceback=
1#980611ad3b9665cd80fe5178bcd6036a :400000+1556C8D :400000+1556B09 :400000+15569D1
:400000+157DE39 :400000+15197A2 :400000+1518659 :400000+156BA5E :400000+15591D1
:400000+1189768 :400000+1188E6D :400000+1186E15 :400000+484F270 :400000+11A1CA0
```

```
Fastpath Thread backtrace: -Traceback= 1#980611ad3b9665cd80fe5178bcd6036a
c:7F64154A4000+BE002
Auxiliary Thread backtrace: -Traceback= 1#980611ad3b9665cd80fe5178bcd6036a
pthread:7F640ED43000+A7C9
```

Conditions: This symptom occurs when X.X.X.X/X is in “FD is infinity” status in EIGRP.

Workaround: There is no workaround.

- CSCun45272

  Symptom:

  1. Standby RP will have out-of-sync entries. With MPLS-TE NSR enabled, the standby RP will have out-of-sync entries which will result in flapping of the path-protected LSP of the tunnel after an SSO.
  2. Leaking an LSP. A third LSP will be signaled and leaked (there is no management of the LSP). There are supposed to be two LSPs at steady state (primary and path protected), but with this defect, there will be primary, path protected, and leaked LSP.

  Conditions: This symptom occurs with a reoptimization of a tunnel that has failed with path protection enabled.

  Workaround: There is no workaround.

- CSCun45299

  Symptom: IPv6 traffic is dropped for packets with extension headers.

  Conditions: This symptom occurs when extension header packets are punted to the CPU.

  Workaround: There is no workaround.

- CSCun46486

  Symptom: A Cisco device crashes every 2-3 days when the SNMPSET operation is used to create guest users.

  Conditions: This symptom occurs when guest users are created through SNMPSET operations at a very high rate.

  Workaround: There is no workaround.

- CSCun47357

  Symptom: Enabling PBR breaks the EIGRP multicast.

  Conditions: This symptom occurs under the following conditions:

  1. Create a route map for any random IP address (not necessarily related to multicast/protocol IP).
  2. Enable the PBR on an interface with EIGRP peering. It is observed that the EIGRP peering goes down.

  Workaround: There is no workaround.

- CSCun47461

  Symptom: A crash occurs on issuing the **no switchport** command on an interface applied with a MAC ACL.

  Conditions: This symptom occurs on issuing the **no switchport** command on an interface applied with a MAC ACL.

  Workaround: There is no workaround.

- CSCun48344

  Symptom: A config-sync failure occurs due to the **address-family ipv6 unicast vrf** command during the immediate unconfiguration and reconfiguration of VRF definition.

  Conditions: This symptom occurs with attached running configurations.

  Workaround: There is no workaround.

- CSCun50243

  Symptom: When CED/ANSam/2100Hz answer tone is detected in the early media phase of the call, the gateway does not switchover and starts sending distorted audio to the originating fax. Fax transmission fails.

  Conditions: This symptom is observed when modem passthrough nse codec g711ulaw is used as the fax protocol.

  ```
  Fax -> VG224 --SCCP--> CUCM -SIP--> 3945 GW--ISDN T1 PRI-->PSTN 3945 IOS: 15.1.4M5
  VG224:15.1.4M2
  ```

  Workaround: Perform the following workaround:

  – Use “progress_ind” to strip PI=8 if the Early Media is opened via an ISDN ALERTING message: (config-dial-peer)#progress_ind alert strip

  – Check with Carrier if they can avoid opening early media for Fax/Modem calls.

  – More Info: Early media cut-through for fax/modem calls is not supported. The expected flow transition to the Voice Band Data (VBD) mode or modem up-speed as we commonly call it,requires a VoIP call to be first established (call is connected). It is then, when normally a 2100Hz answer tone is detected as the media flows in both direction and triggers Voice Band Data (VBD) upspeed.

- CSCun58030

  Symptom: A Cisco ME3600-24CX platform does not display time source information while running the PTP dataset time properties show command. Functional issues are not noticed with PTP time sync. The time source field says “Unknown”.

  Conditions: This symptom does not occur under specific conditions. A simple Ordinary Clock(OC) Slave- Master connectivity would make the Slave show up as “Time Source Unknown”.

  Workaround: There is no workaround.

- CSCun58224

  Symptom: A memory corruption is observed on scaling NAT sessions.

  Conditions: This symptom occurs due to multiple translation entries of NAT with overload.

  Workaround: There is no workaround.

- CSCun62420

  Symptom: Any ingress policy on an EFP affects other EFPs on the same physical port with local-connect configuration.

  Conditions: This symptom occurs when an ingress QoS policy is enabled on an EFP and another EFP of the same port is bound to the other port’s EFP by the “connect” statement.

  Workaround:

  1. Apply an ingress policy on all EFPs with a local-connect configuration and detach the policy.
  2. Configure an independent service-policy on the erroneously affected EFPs of the same physical interface.

- CSCun65000

  Symptom: Traffic loss of about 200-500 ms is observed.

  Conditions: This symptom is observed on an RLFA cutover.

  Workaround: There is no workaround.

- CSCun65380

  Symptom: CME Crashed while Inbound SIP profile added globally.

  Conditions: This symptom is observed when inbound SIP profile is added.

  Workaround: Do not configure inbound sip profile.

- CSCun67364

  Symptom: Convergence on Local link failure with rLFA is higher than one second.

  Conditions: Configure rLFA and perform local link failure. The problem is likely seen when configuring a small spf-interval value.

  Workaround: Do not configure too small spf-interval.

- CSCun68723

  Symptom: Incorrect information is present on the E1/T1 ports on the Cisco ME 3600X 24CX platform in the IfTable of IF-MIB.

  The incorrect information includes the following:

  1. ifType of the interface is 0 which is not a valid ifType.
  2. ifAdminStatus value is always testing, and does not reflect the actual state.
  3. ifOperStatus value is always unknown and does not reflect the actual state.
  4. ifSpeed value is 0 which is incorrect.

  Conditions: This symptom occurs on any Cisco ME 3600X 24CX device running Cisco IOS Release 15.3(3)S.

  Workaround: The correct information on the E1/T1 ports is available in CLI.

- CSCun72459

  Symptom: High traffic loss is observed with setups having BGP and microloop avoidance combination.

  Conditions: This symptom occurs with the following combination:

  1. IP FRR is turned on.
  2. Cisco IOS XE Release 3.11 code (or newer) that enables microloop avoidance by default.
  3. BGP configurations.

  Workaround: Disable the microloop avoidance feature. For example, in ISIS, execute the following commands:

  router isis <process name>

  microloop avoidance disable

  !

  However, there will be some traffic loss due to the lack of microloop avoidance.

- CSCun72939

  Symptom: QoS Egress Marking does not work for GRE Tunnels.

Conditions: This symptom is observed under the following conditions: -The issue happens for fragmented packet. -The issue is found on Cisco IOS Release 15.3(3)M2.

Workaround: There is no workaround.

- CSCun73782

  Symptom:

  A vulnerability in LISP control messages processing on Cisco IOS and Cisco IOS XE could allow an unauthenticated, remote attacker to cause a vulnerable device to disable CEF forwarding and eventually drop traffic passing through.

  The vulnerability is due to insufficient checking of certain parameters in LISP control messages on ITR. An attacker could exploit this vulnerability by sending malformed LISP control messages to ITR. An exploit could allow the attacker to cause a vulnerable device to disable CEF forwarding and eventually drop traffic passing through.

  Conditions: Malformed messages can only be generated by a device that is already registered to a LISP system: a valid ETR or ALT.

  Workaround: There is no workaround.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4.3/3.6: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:N/A:P/E:F/RL:OF/RC:C

  CVE ID CVE-2014-3262 has been assigned to document this issue.

  Additional details about the vulnerability described here can be found at: http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-3262

  Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCun75719

  Symptom: After a switchover, standby device crashes with traceback.

  Conditions: At present, this is observed only on advipservices images in mtrose branches.

  Workaround: There is no workaround.

- CSCun76733

  Symptom: BFD goes down and remains in Admindown state.

  Conditions: This symptom occurs after applying ACL chaining and flapping of the interface.

  Workaround: There is no workaround.

  More Info: An IPv4 BFD neighbor remains in admindown state on the PE. The ACE configured in ACL for BFD is matched and the receive counters on BFD neighbors are incremented but the BFD is still down.

  This issue occurs only after ACL chaining is applied.

- CSCun77010

  Symptom: A router may crash after or during the execution of the **show ipv6 ospf rib** command.

  Conditions: This symptom occurs when many routes or route paths are present in the OSPFv3 rib. The OSPFv3 rib is significantly recomputed during execution of commands.

  Workaround: Limit the use of the **show ipv6 ospf rib** command.

- CSCun78309

  Symptom: An Mroute entry on FHR is stuck in a registering state in MVPNv4.

  ```
  show ip mroute vrf <vpn-name> -->> shows the mroute entry in registering state
  ```

  Conditions: This symptom occurs when the source address of the encapsulation tunnel for PIM registers on the FHR is one of the interfaces that is not in the same VRF as the register tunnel itself.

  Workaround: There is no workaround.

  More Info: sample Output:

  ```
  PE2#show ip mroute vrf vpn1
  (215.12.1.2, 229.40.1.1), 00:00:29/00:02:30, flags: FT Incoming interface:
  GigabitEthernet3/3.1, RPF nbr 0.0.0.0, Registering Outgoing interface list: Tunnel764,
  Forward/Sparse, 00:00:29/00:03:00
  ```

- CSCun81754

  Symptom: snmpEngineBoots integer does not increment on Cisco ME 3800 and Cisco ME 3600 devices once they are reloaded. They get reinitialized.

  Conditions: This symptom occurs only when the device gets rebooted. A warm restart increases the value.

  Workaround: There is no workaround.

- CSCun85501

  Symptom: IPv6 traffic is not forwarded in the hardware for templates other than default and video (like VPNv4-only, VPNv4-v6). However, IPv4 traffic works fine.

  Conditions: This symptom occurs when the template is not default or not video

  Workaround: There is no workaround.

  Further Problem Description: IPv6 traffic is punted to the CPU.

- CSCun87557

  Symptom: A Cisco router crashes.

  Conditions: This symptom occurs when the VTY Service Set maximum response is set to a small number, for example, 10, and then multiple commands are sent separated by a newline using the same write, for example, “show ver\nshow ver\n”.

  Workaround: Set the maximum response to a bigger number.

- CSCun91720

  Symptom: IPv6 mcast traffic is punted to the host queue (inl3idc_vlan.bridgeBasedMcastIp=1).

  Conditions: This symptom occurs on a Layer 2 device with no multicast configurations.

  Workaround: There is no workaround.

  More Info: Instead of bridging the IPv6 traffic, the switch punts it to the CPU.

- CSCun91923

  Symptom: Router crash observed on CUBE for Carbon2-SIP signaling forking.

  Conditions: Crash is seen while you configure CUBE for SIP signaling forking on PI19.

  Workaround: There is no workaround.

- CSCun92095

  Symptom: IOS-XE running router may reload when unconfiguring BGP along with other removal operations in a scaled setup.

  Conditions: This symptom occurs when the BGP is configured with 1Million+ nets and 4000 VRFs. Then the BGP instance is removed using "no router bgp <>"

  Workaround: Shut down the BGP neighbor sending big scale nets to remove the nets first from BGP and RIB. Then remove the BGP using "no router bgp <>".

- CSCuo09249

  Symptom: An xTR changes its RLOC, map-request packets from that new RLOC are dropped on the MS/MR due to policy violation, for example:

  ```
  *Apr 2 15:29:15 JST: LISP-0: AF IID 100 IPv4, Map resolver filtered incoming map
  request from 2400:A:A:9999:C267:AFFF:FE52:287 because it does not conform to the
  configured allowed-locator policy.
  ```

  Conditions: This symptom is observed when {ipv4|ipv6} map-resolver map-request validate source registered is configured on the MS/MR and the xTR RLOC is updated, for example, by DHCP when the {ipv4|ipv6}-interface configuration is used in the database-mapping configuration. Both the new and the old RLOC must have been valid.

  Workaround: Remove and re-add database-mapping configuration on xTR, possibly using EEM script on address change Remove "{ipv4|ipv6} map-resolver map-request validate source registered" configuration on MS/MR clear lisp site <name> on the MS

- CSCuo11238

  Symptom: Router crashes when removing address-family from VRF definition, or when removing the VRF definition.

  Conditions: This symptom is observed when PIM is configured for the LISP interface associated with the VRF.

  Workaround: Unconfigure LISP for the VRF, or remove PIM configuration from the LISP interface associated with the VRF, before removing VRF configuration.

- CSCuo11703

  Symptom: The **show network-clock synchronization** command flaps between different QL values on the same interface. Depending on the values with which the interface flaps, this could lead to triggering of network-clock selection algorithm and subsequent selection of primary reference clock for the system.

  Conditions: This symptom could occur when the network-clock synchronization mode is unprovisioned from automatic selection, and then the monitor interfaces are removed and a new set of interfaces are added for network-clock monitoring with automatic selection reprovisioned.

  Workaround: Adding back the older set of interfaces and removing them would resolve the issue.

- CSCuo12245

  Symptom: The following error message is observed with traceback:

  ```
  OCE_PUNT_PROCESS-3-LABEL_CACHE_INVALID: inlabel pointer was NULL
  ```

  Conditions: Multicast traffic is label switched in the mpls P2MP tree and replicated at branch bud nodes along the P2MP tree. The error condition is observed at a bud node, where the replicated traffic is dropped with the error.

  Workaround: There is no workaround.

- CSCuo13314

  Symptom: ES+ crashes while deleting the imposition table from LC.

  Conditions: This symptom occurs while flapping the scalable EoMPLS.

  Workaround: There is no workaround.

- CSCuo16717

  Symptom: PPPoX brings up sessions failure with IPv6 configurations.

  Conditions: This symptom occurs when "vpdn authen-before-forward" is configured.

  Workaround: Do not configure "vpdn authen-before-forward".

- CSCuo19730

  Symptom: Cisco IOS XE includes a version of OpenSSL that is affected by the vulnerability identified by the Common Vulnerability and Exposures (CVE) ID CVE-2014-0160.

  This bug has been opened to address the potential impact on this product.

  Conditions: Cisco IOS XE devices running release 3.11.0S, 3.11.1S or 3.12.0S and with the WebUI interface over HTTPs enabled. No other versions of Cisco IOS XE are affected.

  Devices with the WebUI interface enabled and using HTTPs as transport protocol will include the following configuration:

  transport-map type persistent webui http-webui secure-server ip http secure-server transport type persistent webui input http-webui

  Devices running IOS XE release 3.11.0S, 3.11.1S or 3.12.0S but WITHOUT the WebUI interface enabled, or with the WebUI interface enabled but NOT using HTTPs as transport protocol are NOT AFFECTED by this vulnerability.

  Devices running IOS XE release 3.11.0S, 3.11.1S or 3.12.0S and with the HTTPs server enabled (by including in their configuration the line "ip http secure-server") are NOT affected. Both the HTTPs server and the WebUI interface need to be enabled for a device to be vulnerable.

  The WebUI configuration guide is available at http://www.cisco.com/c/en/us/td/docs/routers/asr1000/configuration/guide/chassis/asrswcfg/webui.html

  Workaround: Not currently available.

  Further Problem Description: Additional details about this vulnerability can be found at http://cve.mitre.org/cve/cve.html

  Software version and Fixes:

  The first column is the Cisco IOS XE Software Release.

  The second column is the First Fixed Release.

  2.x.x Not Vulnerable

  3.1.xS Not Vulnerable

  3.1.xSG Not Vulnerable

  3.2.xS Not Vulnerable

  3.2xSE Not Vulnerable

  3.2.xSG Not Vulnerable

  3.2.xXO Not Vulnerable

  3.2.xSQ Not Vulnerable

3.3.xS Not Vulnerable

3.3.xSE Not Vulnerable

3.3xSG Not Vulnerable

3.3xXO Not Vulnerable

3.3xSQ Not Vulnerable

3.4.xS Not Vulnerable

3.4.xSG Not Vulnerable

3.5.xS Not Vulnerable

3.5.xE Not Vulnerable

3.6.xS Not Vulnerable

3.6.xE Not Vulnerable

3.7.xS Not Vulnerable

3.8.xS Not Vulnerable

3.9.xS Not Vulnerable

3.10.xS Not Vulnerable

3.11.xS Vulnerable

3.12.xS Vulnerable

3.12.0aS Not Vulnerable

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4.3/4.3:

https://intellishield.cisco.com/security/alertmanager/cvss?target=new&version=2.0&vector=AV:N/AC:M/Au:N/C:P/I:N/A:N/E:H/RL:U/RC:C

The Cisco PSIRT has assigned this score based on information obtained from multiple sources. This includes the CVSS score assigned by the third-party vendor when available. The CVSS score assigned may not reflect the actual impact on the Cisco Product.

CVE-2014-0160 has been assigned to document this issue.

Additional information on Cisco's security vulnerability policy can be found at the following URL:

http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

- CSCuo22184

  Symptom: The VPLS bit is not set in the flood VLAN LTL index which causes a traffic drop.

  Conditions: This symptom occurs under the following conditions:

  - Have a port-channel with member links on different NP (say NP2 and NP1) and a physical interface on the same LC and NP (say NP2) to different neighbors, say PE1 and PE2 respectively.
  - Shut down the member link of NP1.
  - Remote shut the VLAN or access interface on PE2 (reached by physical interface).
  - The V-bit is not set and this affects the traffic towards PE1 (reached by port-channel interface).

  Workaround:

  - Either no-shut the remote VLAN or AC on PE2.

  - Perform shut and no-shut the port-channel.

- CSCuo24235

  Symptom: SVI counters are not updated for IPv6 traffic.

  Conditions: This symptom does not occur under specific conditions.

  Workaround: There is no workaround.

- CSCuo35867

  Symptom:

  1. CPOS-based PPP serial interface is UP/DOWN; but HDLC is UP/UP; loopback local for PPP is also UP/DOWN;
  2. From debug, the following output is seen:

```
*Apr 16 20:46:50.330: AAA/ID(00100066): PPP allocated .... *Apr 16 20:46:50.831: CCM:
Failed to create session, session already exists <<<<<<<<<<<< *Apr 16 20:46:50.831:
AAA/ID(NA): PPP allocating *Apr 16 20:46:50.831: CCM GROUP:ERROR group not found with
shdb 0 *Apr 16 20:46:50.831: AAA/ID(NA): propagate hw:Se1/0/0.1/1/6/1:0,0x42352E64
sw:Se1/0/0.1/1/6/1:0,0x42353C48 other:nil base:nil unit:0/1 slot:1 shelf:0 tty:nil
*Apr 16 20:46:50.831: aaa_uid_propogate grabbed_id = 1048678 *Apr 16 20:46:50.831:
AAA/ID(00100066): PPP allocated *Apr 16 20:46:52.847: Se1/0/0.1/1/6/1:0 PPP: Missed a
Link-Up transition, starting PPP <<<<<<<<<<<<<
```

  Conditions: This symptom occurs with PPP serial interface flapping.

  Workaround: Chassis reload can temporarily make PPP interface UP/UP, but the problem will reoccur after a few days.

- CSCuo46609

  Symptom: A router configured as an SSL VPN hub may experience a crash due to memory corruption in the I/O pool. The following may be observed in the crashinfo file:

```
<i>validblock_diagnose, code = 1
current memory block, bp = 0xC020750, memorypool type is I/O data check, ptr =
0xC020780
next memory block, bp = 0xC020890, memorypool type is I/O data check, ptr = 0xC0208C0
previous memory block, bp = 0xC020610, memorypool type is I/O data check, ptr =
0xC020640
<memory dump omitted>
Apr 24 13:32:27.860: %SYS-3-OVERRUN: Block overrun at C020750 (red zone 75F405A7)
-Traceback= 60213FD4z 60217688z 649D8D98z 649D54A0z 63C66204z 63C661E8z Apr 24
13:32:27.860: %SYS-6-MTRACE: mallocfree: addr, pc 52E00584,63462AA0 52E00584,63462670
52E00584,30000012 5266D34C,62E3E0B8 52670418,62E3E0B8 53A44BE0,60000284
53A444CC,626CF044 50B6BC0C,62E63294 Apr 24 13:32:27.860: %SYS-6-MTRACE: mallocfree:
addr, pc 5310B904,62E23040 50B6BC0C,62E58E78 50B6BC0C,3000002E 53A45014,6000006A
53A44BE0,64C7A348 53A44BE0,64C79E10 53A44BE0,40000202 53929890,60000266 Apr 24
13:32:27.860: %SYS-6-BLKINFO: Corrupted redzone blk C020750, words 136, alloc
602191F4, InUse, dealloc A2A4170, rfcnt 1 -Traceback= 64049030z 60213FD4z 60217688z
649D8D98z 649D54A0z 63C66204z 63C661E8z Apr 24 13:32:27.864: %SYS-6-MEMDUMP:
0xC020750: 0xAB1234CD 0xFFFE0000 0x0 0x6500240C Apr 24 13:32:27.864: %SYS-6-MEMDUMP:
0xC020760: 0x602191F4 0xC020890 0xC020624 0x80000088 Apr 24 13:32:27.864:
%SYS-6-MEMDUMP: 0xC020770: 0x1 0x0 0x1000001 0x682757A8
%Software-forced reload
14:32:27 SUMMER Thu Apr 24 2014: Breakpoint exception, CPU signal 23, PC =
0x6064C738</i>
```

  Conditions: This has been observed on the following conditions:

  1. 7200 router running Cisco IOS Release 15.2(4)M2 and 15.3(3)M2.
  2. Router is configured as an SSL VPN host.

Workaround: There is no workaround at this time.

- CSCuo47380

  Symptom: Traffic drops in the MST region during IM-OIR followed by an SSO. When an IM is removed from the router, the MST states are not reflected in the standby RSP. If a switchover happens at this state, it could cause total traffic drop.

  Conditions: This symptom is seen in HA routers. If this issue is hit, the IM that was previously removed should not be inserted back, as it could cause a traffic loop.

  Workaround: There is no workaround.

- CSCuo47685

  Symptom: While evaluating the Cisco IOS Release 15.3(3)S3 early release image, the following error message was observed when using the CoPP configuration given below which matches based on precedence only as shown:

  ```
  class-map match-any coppclass-protocol match precedence 6 7
  ```

  ```
  "Match precedence in IPv4/IPv6 packets is not supported for this interface error:
  failed to install policy map CoPP"
  ```

  Upon occurrence, the entire CoPP policy map is not loaded. There is a concern that some field devices on the current release (Cisco IOS Release 15.0(1)S6) may have the above configuration and as such is prone to this error (CoPP installation failure during upgrade).

  Conditions: This symptom occurs while evaluating the Cisco IOS Release 15.3(3)S3 early release image.

  Workaround: There is no workaround.

- CSCuo49923

  Symptom: Performing an ISSU upgrade with the CEF table consistency checkers enabled may result in a crash on “issu runversion”.

  Conditions: This symptom occurs with a Cisco Catalyst 6500 Series Switch running Cisco IOS Release 15.1(02)SY.

  Workaround: Turn off the CEF table consistency checkers before performing an ISSU upgrade.

- CSCuo55180

  Symptom: A vulnerability in PPPoE processing code of Cisco IOS XE could allow an unauthenticated, adjacent attacker to cause a reload of the affected device and eventually a denial of service (DoS) condition.

  The vulnerability is due to improper processing of certain malformed PPPoE packets. An attacker could exploit this vulnerability by sending a malformed PPPoE packet to an IOS XE ASR1000 device, configured with PPPoE termination. An exploit could allow the attacker to cause a reload of the affected device and eventually a denial of service (DoS) condition.

  Conditions: Cisco ASR 1000 with IOS XE, configured for PPPoE termination.

  Workaround: There is no workaround.

  Further Problem Description: A device crashing, may print the following messages on the console:

  ```
  %SYS-3-OVERRUN: Block overrun at 7F7FAE750B58 (red zone 44534C5F00000000)
  %SYS-6-MTRACE: mallocfree: addr, pc ? %SYS-6-BLKINFO: Corrupted redzone blk
  7F7FAE750B58, words 404, alloc 6374D1B, InUse, dealloc 10001, rfcnt 1 ?
  %Software-forced reload
  Exception to IOS Thread: Frame pointer 0x7F7FA0AB5AD8, PC = 0x7F80A8469565
  UNIX-EXT-SIGNAL: Aborted(6), Process = Check heaps -Traceback=
  1#c3a5522ccb47820b036322d6b7226e1c c:7F80A8438000+31565
  ```

```
Fastpath Thread backtrace: -Traceback= 1#c3a5522ccb47820b036322d6b7226e1c
c:7F80A8438000+BDDD2
Auxiliary Thread backtrace: -Traceback= 1#c3a5522ccb47820b036322d6b7226e1c
pthread:7F80A3697000+A7C9
```

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.1/5: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:A/AC:L/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C

CVE ID CVE-2014-3284 has been assigned to document this issue.

Additional details about the vulnerability described here can be found at: http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-3284

Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCuo55440

  Symptom: The ME3600-24CX device crashes whenever it is reloaded.

  Conditions: This symptom occurs when the ME3600-24CX device is reloaded.

  Workaround: There is no workaround.

- CSCuo56173

  Symptom: When PW's remote peer is ALU, it takes 5 to 10 minutes for the PWs to come up.

  Conditions: This symptom occurs when Provision PW is done first on the ALU and then on the Cisco router.

  Workaround: Provision PW on the Cisco router first.

- CSCuo72301

  Symptom: Crash occurs when IKEv2 attempts to clean up its contexts when it times-out waiting for received Certificate to be Validated by PKI component.

  Conditions: Authentication with certificates and PKI component's response to certificate validation is delayed.

  Workaround: There is no workaround.

- CSCuo77574

  Symptom: An error is seen while enabling "auto negotiation".

  Conditions: This symptom is observed when "auto negotiation" is configured on an interface.

  Workaround: There is no workaround.

- CSCuo82355

  Symptom: A BFD session fails to come up.

  Conditions: This symptom occurs when BFD is running on Cisco IOS Release 15.4(1)S to any other lower release.

  Workaround: Upgrade the device.

- CSCuo86424

  Symptom: An ESP crashes while using packet-trace to debug packets.

  Conditions: This symptom occurs when a ping is initiated while using packet-trace to debug packets on Cisco IOS XE Release 3.11.2 or Cisco IOS Release 15.4(2)S2. This issue is only visible in the Cisco IOS Release 15.4(1)S2 maintenance release.

Workaround: Use packet-trace in a circular mode and choose a large number of packets.

```
Example: debug platform packet-trace packet 8192 circular
```

This will only reduce the chances of seeing the crash but will not eliminate it completely.

- CSCup22590

  Symptom: Some Cisco Internetwork Operating System (IOS) releases may be affected by the following vulnerabilities:

  These products include a version of openssl that is affected by the vulnerabilities identified by the Common Vulnerability and Exposures (CVE) IDs:

  CVE-2014-0195 - DTLS invalid fragment vulnerability CVE-2014-0221 - DTLS recursion flaw CVE-2014-0224 - SSL/TLS MITM vulnerability

  This bug has been opened to address the potential impact on this product.

  Conditions: This symptom occurs in devices running an affected version of Cisco IOS and utilizing an affected configuration.

  One of more of these vulnerabilities affect all versions of IOS prior to the versions listed in the Integrated In field of this defect.

  Workaround: None currently available.

  Further Problem Description: CVE-2014-0224: All Cisco IOS services that provide a form of TLS or SSL encryption are affected by this vulnerability. This includes features such as the HTTPS Web Management interface.

  CVE-2014-0195: Cisco IOS devices that support SSLVPN (AnyConnect) and have the feature configured and enabled are affected by this vulnerability.

  CVE-2014-0221: Cisco IOS devices that support SSLVPN (AnyConnect) and have the feature configured and enabled are affected by this vulnerability.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 10/9.5:

  https://intellishield.cisco.com/security/alertmanager/cvss?target=new&version=2.0&vector=AV:N/AC:L/Au:N/C:C/I:C/A:C/E:F/RL:U/RC:C

  The Cisco PSIRT has assigned this score based on information obtained from multiple sources. This includes the CVSS score assigned by the third-party vendor when available. The CVSS score assigned may not reflect the actual impact on the Cisco Product.

  Additional information on Cisco's security vulnerability policy can be found at the following URL:

  http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

Open Bugs—Cisco IOS Release 15.4(2)S

This section describes possibly unexpected behavior by Cisco IOS Release 15.4(2)S. All the bugs listed in this section are open in Cisco IOS Release 15.4(2)S. This section describes only severity 1, severity 2, and select severity 3 bugs.

- CSCum90044

  Symptom: FRR database value does not exist.

  Conditions: This symptom occurs on tunnelling intf with Auto-Tunnel_Primary_SSO_Configuration.

Workaround: There is no workaround.

Resolved Bugs—Cisco IOS Release 15.4(2)S

- CSCtb34814

  Symptom: The %DATACORRUPTION-1-DATAINCONSISTENCY: copy error is observed without any traceback just before the system crashes.

  Conditions: This issue occurs under normal conditions.

  Workaround: There is no workaround.

- CSCte77398

  Symptom: A Cisco ATM router configured with ATM PVC Range commands report the following error when attempting to configure a PVC Range:

  ```
  Unable to configure PVC Range. Possibly multiple users configuring IOS simultaneously.
  ```

  Conditions: This problem occurs randomly and even if there are no multiple sessions accessing the pvc-range at the same time.

  Workaround: There is no workaround.

- CSCts14036

  Symptom: Memory “Holding” continues to increases on process “IP SNMP”. This could lead to an out of memory crash.

  Conditions: This symptom only affects Cisco IOS release 12.2(53)SG5, under the following conditions:

  1. Switch is configured to receive informs

  and/or

  2. Traps received and consumed by switch (traps broadcast)

  Use “show proc memory | inc IP SNMP” and compare outputs across several collections of this command.

  Workaround: Upgrade to Cisco IOS release 12.2(53)SG8.

- CSCty92208

  Symptom: A crash is seen on the Cisco Catalyst 6509 Switch after configuring WCCP.

  Conditions: This symptom occurs when WCCP is configured with a hash assignment and port hashing is enabled. It will occur during redirection if packets are software switched.

  Workaround:

  1. Disable port-hashing if hash-assignment is used.
  2. Use the mask-assignment method.

- CSCtz66347

  Symptom: Router crashes on executing **show tech-support** from the linux client to the IOS server over an SSH session with the rekey enabled.

  Conditions: This symptom occurs when the rekey value “ip ssh rekey volume 400” is configured.

  Workaround: Disable the rekey feature by configuring the **no ip ssh rekey** command.

- CSCuc24927

  Symptom: A segmentation fault is seen when IMA, CEM and Serial are configured on different controllers and an image is loaded.

  Conditions: This symptom is seen when IMA, CEM, and Serial are configured on different controllers. and try to load image. The issue is consistently reproduced and is sometimes seen when CEM on TDM and MLPPP QoS on OC3 IM is configured and multiple reloads are done. When there is a segmentation fault, the RSP will not come up and will go to the ROMmon mode.

  Workaround: Do not combine IMA, CEM and Serial configurations. Test each feature individually.

- CSCuc60868

  Symptom: A router randomly crashes either due to memory corruption at bgp_timer_wheel or memory chunks near bgp_timer_wheel (For example, BFD event chunks if BFD is configured or AtoM Manager chunks if LDP is configured). A crash occurs right after an LDP neighbor is up in the L2VPN setup.

  Conditions: This symptom occurs when **vpls bgp signaling** is unconfigured and then reconfigured. Both L2VPN and BGP are unconfigured and reconfigured after all L2VPN and BGP data structures are fully deleted (about 3 minutes for 5 BGP VPLS prefixes). For the repro on file, OSPF (for IGP) is also unconfigured and reconfigured. Both LDP and BGP signalling are affected by this bug.

  Workaround: Avoid unconfiguring and reconfiguring BGP L2VPN.

- CSCue59450

  Symptom: IOS XE Watchdog message seen along with RP and SIP crash.

  Conditions: This symptom is observed in an ARP request on the interface having VRF receive configured on it.

  Workaround: There is no workaround.

- CSCuf53543

  Symptom: MPLS-TP L2 VCs are down after an SIP reload and RP switchover.

  Conditions: This symptom occurs when VCs are configured through an MPLS-TP tunnel in a hardware redundant platform.

  Workaround: There is no workaround.

- CSCug08561

  Symptom: After a web-logon, users do not get the web-logon response page sent by the portal. If the web-logon is successful, users are not redirected to the web address which they have entered initially but are redirected to the portal for authentication.

  Conditions: This symptom occurs under the following conditions:

  1. Walkby feature is enabled with L4R & PBHK features applied to the lite session.
  2. User initiated the web-logon request.

  Workaround: There is no workaround.

  More Info: When a user does a web-logon, an account-logon coa request is triggered from the portal to ISG. In ISG, the account-logon request triggers a lite session conversion to a dedicated session. During the conversion, lite session and its associated resources (L4R and PBHK mappings) are removed from PD and a dedicated session gets provisioned. Once the conversion is done, ISG replies back with COA ACK/NACK to the portal. Based on the response from ISG, the portal generates a weblogon response (SUCCESS/FAILURE) page and sends it back to the client. But when it reaches ISG, the response packet does not get classified to session in the downstream direction and gets dropped in ISG because PBHK & L4R maping are deleted.

- CSCug43009

  Symptom: SYS-SP-2-MALLOCFAIL memory allocation fails due to I/O buffer memory leak in process_online_diag_pak.

  Conditions: This symptom occurs when some diag packets get en-queued to a queue which is not being watched. Hence, there is no dequeueing on that queue which leads to I/O memory leak.

  Workaround: Reload the box to clear the I/O pool when it is full.

- CSCuh44420

  Symptom: When a Cisco IOS router with one or more mpls ldp neighbors undergoes an **mpls ldp router-id** configuration change and non-stop routing had been previously enabled and disabled prior to the router-id configuration change, sessions fail to become NSR-ready once **mpls ldp nsr** is reconfigured.

  Conditions: This symptom occurs when the **mpls ldp router-id** command is reconfigured after **mpls ldp nsr** has been enabled and then disabled. After the router-id change, **mpls ldp nsr** must be reconfigured in order to encounter this issue.

  Workaround: Reload the standby RP.

- CSCuh45042

  Symptom: Traffic on some GIG subinterfaces are seen to be dropped at the SPA. The SPA TCAM is seen to have two entries sharing the same logical address as a result of which one entry is seen to overwrite the other.

  Conditions: This symptom was observed after a router/LC/SPA reload. The exact condition that triggers this symptom is not known.

  Workaround: There is no workaround.

- CSCuh89168

  Symptom: The standby resets in a continuous loop.

  Conditions: This symptom occurs on insertion of a new standby RSP with a different license than the one on the active RSP.

  Workaround: There is no workaround.

- CSCuh91645

  Symptom: WS-SUP720-3B crashes while receiving DHCP packets.

  Conditions: This symptom occurs with the **ip dhcp relay information policy-action encapsulate** command.

  Workaround 1. Use the **ip dhcp relay information policy-action replace** command.

  Workaround 2. Use the **no ip dhcp relay information trusted** command.

- CSCui04530

  Symptom: Upon FPD upgrade, you get this error on Cisco IOS c7600 switch:

  ```
  ! %FPD_MGMT-3-BUNDLE_EXTRACT_ERROR: Cannot extract the ssc-600-fpd.bndl bundle from
  sup-bootdisk:c7600-fpd-pkg.151kg - The required bundle is not in the package file.
  Please make sure that you have the right FPD image package file. % Cannot get the
  required data from the indicated file, please verify that you have a valid file and
  entered a valid URL. !
  ```

  Conditions: This symptom is observed under the following conditions:

  ```
  IOS: c7600s72033-advipservicesk9-mz.122-33.SRB3
  CARDS: WS-SSC-600 WS-IPSEC-3
  ```

```
CLI: upgrade hw-module slot x fpd file sup-bootdisk:c7600-fpd-pkg.151-3.S2.pkg
```

Workaround: Upgrade to FPD image that includes corresponding *.bndl image.

- CSCui11998

  Symptom: A CEM-SSO Standy crash occurs with 576 CEMoMPLS configured on the mobile profile testbed after defaulting the CEM interface configuration and during reconfiguration.

  Conditions: This symptom occurs during dynamic syncing of cem-xconnect configurations to the standby.

  Workaround: Apply reconfiguration CLIs through TFTP. If the reconfiguration CLIs are done in the router, the crash is observed.

- CSCui24744

  Symptom: An iosd crash is seen.

  Conditions: This symptom occurs on removing **bfd-template single-hop sw-no-echo-sha1** configuration.

  Workaround: There is no workaround.

- CSCui32105

  Symptom: In rare occasions the standby RP on a dual RP system may crash after performing a switchover.

  Conditions: This symptom occurs when an invalid message is sent from the RP to the RRP.

  Workaround: There is no workaround.

- CSCui34165

  Symptom: Port-channel QoS features might fail to work after a router reload, followed by QoS configuration modification.

  Conditions: This symptom occurs when a vlan load-balanced port-channel is used with policy aggregation configuration where the QoS policy is configured on member links and the port-channel sub-interface, and after a system reload (configuration is from startup config).

  Workaround: Reload the router without port-channel QoS configuration, and add port-channel QoS configuration to the running configuration after the router boots up.

- CSCui47602

  Symptom: Traces at IDMGR-3-INVALID_ID when queried for mplsTunnelTable MIB.

  Conditions: This symptom occurs when there is a GETONE SNMP query for non-existing mplsTunnelTable entries.

  Workaround: Avoid using GETONE SNMP query for non-existing objects. Use GETNEXT queries instead of GETONE whenever possible.

- CSCui49185

  Symptom: On a Cisco IOS ASR 1002x series router running Cisco IOS Release 15.4(01)S, a crash occurs.

  Conditions: This symptom occurs when MLDP over GRE is configured, with paths being added and removed. The counter of the number of paths in a CEF path list is not updated correctly. When they wrap at 256 this may cause a crash. The problem occurs when a path is removed without decrementing the counter properly. The problem is observed when a path is added/removed from a path list 256 times.

  Workaround: Do not modify paths using the method described.

- CSCui51363

  Symptom: The multilink does not pass traffic even though it is in an up/up state.

  Conditions: This symptom occurs when the auto DNR status is set and the sip400 ucode crashes.

  Workaround: Perform a shut/no shut in the multilink.

- CSCui53213

  Symptom: Traffic forwards through the VC even when the EVC is in a shut state.

  Conditions: This symptom occurs in scalable EoMPLS.

  Workaround: There is no workaround.

- CSCui56771

  Symptom: When **shutdown** and **no shutdown** are executed at an external interface on a router acting as a PfR border, the router may unexpectedly reload.

  Conditions: This symptom occurs on a Cisco router when heavy traffic is going through an external interface.

  Workaround: There is no workaround.

- CSCui62441

  Symptom: Complete traffic drop for few seconds is seen after few minutes of performing SSO switchover.

  Conditions: This symptom occurs only after a few minutes of performing an SSO switchover.

  Workaround: There is no workaround.

- CSCui65914

  Symptom: Minor or major temperature alarms are reported in the syslog along with the following DATACORRUPTION logs:

  ```
  Aug 5 15:54:30.972 Buc: DATACORRUPTION-SP-1-DATAINCONSISTENCY copy error, -PC=
  0x414DEED4z -Traceback= 4027C4F4 419551C0 414DEED4 414E5BC4 414E0CA0 414E0F00 Aug 5
  15:54:30.972 Buc: C6KENV-SP-4-MINORTEMPALARM interface 10/0 outlet temperature crossed
  threshold #1(=60C). It has exceeded normal operating temperature range.
  ```

  Conditions: The symptom is observed on ES+ series linecards of Cisco 7600 Series Routers.

  Workaround: There is no workaround.

- CSCui67308

  Symptom: Cisco IOS Router constantly crashes after enabling TE tunnel over BDI interface.

  Conditions: This symptom is observed when TE tunnel is exits a BDI interface. This is not a supported design.

  Workaround: Use physical interface for TE tunnels.

- CSCui71298

  Symptom: A router crash is observed.

  Conditions: This symptom occurs when the configuration is replaced with CEM circuit.

  Workaround: There is no workaround.

- CSCui72518

  Symptom: A tunnel down (times out) occurs when the primary link is used again following FRR.

Conditions: This symptom occurs with FRR and reoptimizing the path back to the primary link with RSVP authentication enabled globally.

Workaround: Use interface CFG for RSVP authentication, as it has least impact on data traffic. The only fall out would be that the reopt may fail leaving FRR active LSP to timeout which will then impact traffic. The global CFG model can be used if you always use multi-hop backup tunnels.

- CSCui74609

  Symptom: After an RSP switchover the backup pseudowire state is down and never recovers to standby state.

  Conditions: This symptom occurs on CEM circuits in an SAToP environment after an SSO switchover.

  Workaround: There is no workaround.

- CSCui76564

  Symptom: A roaming mobile customer (example: iPASS, Boingo etc.) logs on via a Web-Portal-Page and the ISG doesn’t send in the radius accounting-request packet from the V-Cookie to the Radius Server.

  Conditions: This symptom occurs depending on the ISG setup. In this case L & V Cookie must be sent in accounting-request from the ISG to the AAA Server.

  Workaround: There is no workaround.

- CSCui82757

  Symptom: Session query responses in lite sessions have inconsistent calling-station-ID behavior.

  Conditions: This symptom occurs under the following conditions:

  1. Walkby feature is enabled with L4R & PBHK features applied to lite session.
  2. Session query is sent to ISG.

  Workaround: Do not use calling-station-ID.

- CSCui83823

  Symptom: When CU executes show tech or any show commands which gives a long output using putty the SSH2 putty closes prematurely.

  Conditions: This symptom is observed when “term length 0” is enabled, the putty session closes prematurely while executing show tech show memory.

  Workaround: Redirect the output to a file.

- CSCui85019

  Symptom: When the command **show xconnect** is entered, it may result in a memory leak. This can be observed by entering the command **show memory debug leaks chunks** and seeing entries like this:

```
router#show memory debug leaks chunks
Adding blocks for GD...
I/O memory
Address Size Alloc_pc PID Alloc-Proc Name
Chunk Elements:
AllocPC Address Size Parent Name
Processor memory
Address Size Alloc_pc PID Alloc-Proc Name AA3F8B4 2348 6D0B528 97 Exec
PW/UDP VC event trace
```

Conditions: This symptom is observed when one or more xconnects are configured with UDP encapsulation.

Workaround: There is no workaround.

- CSCui90811

  Symptom: While running the Cisco IOS 15.3S release and Cisco IOS 15.4S release software for the L2VPN pseudowire redundancy feature on a Cisco router, the traffic is dropped when the primary pseudowire becomes active.

  Conditions: Initially the primary pseudowire is down due to either a local or a remote core-facing interface being shutdown. The backup pseudowire is active and traffic flows through the backup pseudowire. Later, when the backup pseudowire is down, the primary pseudowire is brought up and becomes active and traffic is not able to flow through primary pseudowire and is dropped.

  Workaround: There is no workaround.

- CSCui95398

  Symptom: Config CLI to enable and disable the diag gives a false alarm detection and fails.

  Conditions: This symptom occurs when sprp_inband ping test fails.

  Workaround: There is no workaround.

- CSCui95880

  Symptom: HSRP for IPv6 flaps when there is a loop in the network, but IPv4 HSRP state remains stable for the same vlan.

```
%HSRP-5-STATECHANGE: Vlan154 Grp 154 state Speak -> Standby %HSRP-5-STATECHANGE:
Vlan154 Grp 154 state Standby -> Listen %HSRP-5-STATECHANGE: Vlan154 Grp 154 state
Standby -> Listen %HSRP-5-STATECHANGE: Vlan154 Grp 154 state Speak -> Standby
%HSRP-5-STATECHANGE: Vlan154 Grp 154 state Standby -> Active
```

  Conditions: This symptom is observed when a Layer 2 loop is in the network.

  Workaround: Create an IPv6 access-list, denying udp traffic sourced from device own Ipv6 link local address to any address & permit all other traffic. Apply that access-list to svi interface in inbound direction on the respective HSRP cores running IPv6 HSRP, then the HSRP group will not flap.

- CSCui99031

  Symptom: In a pair of Cisco 7609-S routers running c7600rsp72043-advipservicesk9-mz.151-3.S5.bin IOS, phase 1 fails to establish due to a “signature invalid!” error when rsa-sig is used for phase 1 authentication.

  Conditions: This symptom occurs under the following conditions:

  – rsa-sig is used for phase 1 authentication

  – site to site tunnel

  Workaround: Use PSK instead of PKI.

- CSCuj00746

  Symptom: On performing an upgrade from 9.512 to 9.523, there is a label allocation failure in VPWS circuits as they are trying to utilize the labels that are already used by the VPLS circuits that are present in the database.

  Conditions: This symptom occurs when both VPWS and VPLS circuits are configured on the same node before upgrading.

  Workaround: Removing the VPLS circuit brings up the VPWS circuits. Re-configuring the VPLS circuit is also successful with a different local label assigned.

- CSCuj04178

  Symptom: A crash occurs at vpdn_apply_vpdn_template_pptp.

  Conditions: The conditions for this symptom are unknown.

  Workaround: There is no workaround.

- CSCuj11232

  Symptom: Changing the local label on an existing static (no signaling) Any Transport over MPLS (AToM) pseudowire, or changing the static pseudowire to a dynamic one (with LDP signaling) may cause traffic to fail to traverse the pseudowire.

  Conditions: This symptom is observed when either the configured value of the static local label is changed, or if the pseudowire is changed to a dynamic one.

  Workaround: Completely unconfigure the existing xconnect or pseudowire before entering the new configuration.

- CSCuj16367

  Symptom: Traffic does not flow on a few multilinks.

  Conditions: This symptom occurs during a microcode reload (due to any exception) during a multilink flap in Prowler SPA in SIP-400. This sometimes results in the DNR getting stuck.

  Workaround: Reload the SPA.

- CSCuj16742

  Symptom: In a pseudowire redundancy configuration, packets may fail to flow even though the xconnect virtual circuit appears to be up.

  Conditions: This symptom has been observed when the xconnect is re-provisioned while the primary pseudowire is down and the backup pseudowire is up. The issue has only been observed on Circuit Emulation (CEM) attachment circuits, but it is possible other attachment circuit types may be affected as well.

  Workaround: Completely unconfigure the xconnect and then reconfigure it.

- CSCuj22189

  Symptom: On a Cisco ASR series router, a crash occurs when **mpls ip** is added under the interface.

  Conditions: This symptom occurs when the hidden command **snmp-server hc poll** is already configured.

  Workaround: Ensure that the hidden command **snmp-server hc poll** has not been configured.

- CSCuj26593

  Symptom: Simple IP Dual stack and IPv6 sessions failed to survive an RP switchover.

  Conditions: This symptom occurs when the dual stack session exists.

  Workaround: Do not use the dual stack session.

- CSCuj30702

  Symptom: This bug is specific to port channel sub interface configuration in ES+ card. This bug is not relevant to any other port channel configuration in ES+, that is, EVC/Bridge-Domain over PoCH sub-int etc, and other card types, such as ES20/ LAN cards are free from this bug. Any type of IP communication on port channel sub interfaces in ES+ cards fail. Such an issue is seen only with port channel sub interfaces on ES+ and not seen with port channel main interfaces.

  Conditions: This symptom will only be seen with images where the fix of CSCuh40617 is integrated.

Workaround: The connections will work fine if it is moved to the main interface or by using EVC BD configurations.

- CSCuj31090

  Symptom: When L2TPv3-based pseudowire is configured between two PE routers and different VLAN ids are used on the ACs on both sides, ES+ on egress PE does not rewrite a dot1q VLAN tag when sending a frame toward CE.

  Conditions: This symptom occurs under the following conditions:

  1. Both ACs are Ethernet VLAN type.
  2. Different dot1q tag is used on both ACs.

  Workaround: Configure the same dot1q tag for the ACs on both PEs.

- CSCuj47238

  Symptom: There is a difference in the Y1731 probe within **show ip sla statistics**.

  Conditions: This symptom is seen in the Cisco 7600 series routers.

```
service instance 400 ethernet evc1000 description -- EVC Cliente BUSINESS---
encapsulation dot1q 400 second-dot1q 100 <==HERE rewrite ingress tag pop 2 symmetric
<==HERE xconnect 172.16.12.6 1000 encapsulation mpls cfm mep domain OPM mpid 2
mdr-rm01#sh ip sla statistics 1 IPSLAs Latest Operation Statistics
IPSLA operation id: 1 Delay Statistics for Y1731 Operation 1 Type of operation: Y1731
Delay Measurement Latest operation start time: 12:06:21.041 CET Wed Sep 11 2013 Latest
operation return code: OK Distribution Statistics:
Interval Start time: 12:06:21.041 CET Wed Sep 11 2013 Elapsed time: 50 seconds Number
of measurements initiated: 44 <== HERE Number of measurements completed: 32 <== HERE
Flag: OK
```

  Workaround: There is no workaround.

- CSCuj47554

  Symptom: PBHK bundles are not released even after the session is cleared.

  Conditions: This symptom occurs after the session is cleared and the port-bundle status is not shown correctly with **show ip portbundle status** command.

  Workaround: There is no workaround.

- CSCuj52396

  Symptom: In a VPLS Inter-Autonomous System Option B configuration, the virtual circuits between the Autonomous System Border Router (ASBR) and the PE may fail to come up.

  Conditions: This symptom is observed while initially establishing VCs after the ASBR has reloaded.

  Workaround: The **clear xconnect** exec command can be used to clear the VCs that are down.

- CSCuj55914

  Symptom: The MPLS label of the labeled route is missing. This causes a traffic loss as only one path (non-labeled path) takes on the full load of the shared traffic setup.

  Conditions: This symptom occurs when there are two routes to a network and one of them is a sham-link, and the routes are learned via OSPF and redistributed by BGP, and one of the routes is labeled and the other is not, and the unlabeled route gets installed after the labeled route (for example, flapping). And both of the routes have the same metrics (that is, show ip route vrf <> x.x.x.x and show ip cef vrf <> x.x.x.x will have both entries).

  Workaround: Flap the unlabeled route and then the labeled route.

- CSCuj57367

  Symptom: A 10 gig line card crashes on a Cisco 7600 platform with the following or similar errors:

  ```
  %SYS-DFC3-3-MGDTIMER: Uninitialized timer, timer stop, timer = 30CCCFB0. -Process= "RO
  Notify Timers", ipl= 0, pid= 7 -Traceback= 2060E1BCz 2060E8E4z %SYS-DFC3-3-MGDTIMER:
  Uninitialized timer, timer stop, timer = 30CCD154. -Process= "RO Notify Timers", ipl=
  0, pid= 7 -Traceback= 2060E1BCz 2060E8E4z %SYS-DFC3-3-MGDTIMER: Uninitialized timer,
  timer stop, timer = 30CCCFB0. -Process= "RO Notify Timers", ipl= 0, pid= 7 -Traceback=
  2060E1BCz 2060E8E4z
  08:54:43 Central Tue Oct 1 2013: Address Error (load or instruction fetch) exception,
  CPU signal 10, PC = 0x20642A08
  ```

  Conditions: This symptom occurs when a large number of IPC messages are used.

  Workaround: There is no workaround.

  More Info: On mac-scaling, the L2-DRV application sends more ICC messages(though not always). But periodically(approximately 2-3 minutes), some burst of around 150 ICC messages are sent by the SP towards the RP. This means that mac-scaling has a direct correlation with the number of IPC messages being sent.

- CSCuj60533

  Symptom: Repeated CPUHOG messages may be seen along with a crash when “reload” is issued just after a bootup.

  Conditions: This symptom occurs when the line cards are still booting up and are in other states.

  Workaround: Issue “reload” after the line cards have booted.

- CSCuj64806

  Symptom: VRRPv2 priority may be incorrectly calculated when tracking tunnel interfaces. After reloading the router, the track decrement value is decremented twice. As a result, VRRPv2 with tracking does not work as expected.

  Conditions: This symptom is observed when you use tracking tunnel for VRRP priority.

  Workaround: Use VRRPv3.

- CSCuj65057

  Symptom: The **ip vrf forwarding** command under “aaa” is deleted after reloading the stack master.

  Conditions: This symptom occurs after reloading the stack master switch.

  ```
  aaa new-model ! aaa group server tacacs+ TACACS+ ip vrf forwarding VRF01 ! ip vrf
  VRF01 rd x.x.x.x
  ```

  Workaround: Use the **vrf definition** command instead of the **ip vrf command to define vrf. (This command is supported on Cisco IOS Release 12.2(58)SE or later releases.)**

- CSCuj66352

  Symptom: A system crash is observed in the SNMP engine.

  Conditions: This symptom occurs under the following conditions:

  - ?show subscriber session?
  - polling the ISG-MIB
  - clearing the subscriber

  Workaround: Do not use SNMP polling.

- CSCuj68109

  Symptom: The Cisco 7600-SIP-400 router crashes.

Conditions: This symptom occurs when there is an Egress ESF Engine: ME Breakpoint error.

Workaround: There is no workaround.

- CSCuj68932

  Symptom: L2TPv3 tunnel with digest fails to establish. Cisco IOS device gives the following messages when “debug l2tp all” and “debug l2tp packet detail” are enabled:

  ```
  L2TP _____:________: ERROR: SCCRQ AVP 59, vendor 0: unknown L2TP _____:________:
  Unknown IETF AVP 59 in CM SCCRQ
  ```

  Conditions: This issue is observed when IOS device peers with non-IOS device that sends IETF L2TPv3 digest AVP (IETF AVP 59) in L2TP control message. This issue is present in S images starting from Cisco IOS Release 12.2(33)XNC and in T train from Cisco IOS Release 15.3(2)T.

  Workaround: There is no workaround.

- CSCuj75952

  Symptom: The Cisco ASR 1000 route processor reloads.

  Conditions: This symptom occurs during PPPoA session establishment if CAC determines that resources are low and HW-assisted CAC needs to be enabled. The router is used to terminate PPPoA sessions and Call Admission Control (CAC) is enabled.

  Workaround: Disable Call Admission Control.

- CSCuj78636

  Symptom: A memory leak is observed in the IP Switching segment.

  Conditions: This symptom occurs if a subscriber roams with the same MAC address but a different IP address. This happens only for L2 roaming and not for L3 roaming.

  Workaround: There is no workaround.

- CSCuj82897

  Symptom: The “control-word” length is not set properly for small HDLC packets running over HDLC AToM VC with SIP-200. For example: SPA-8XCHT1/E1.

  Conditions: This symptom occurs when HDLC AToM VC with SIP-200 is deployed, for example, SPA-8XCHT1/E1, will result in a packet length mismatch issue or dropping by the remote PE router when HDLCoverMPLS runs over the Ethernet link adding an additional padding which cannot be classified at all.

  Workaround: Use SIP-400.

- CSCuj87734

  Symptom: NVRAM startup configuration fails to load.

  Conditions: This symptom occurs on enabling the service compress configuration.

  Workaround: Disable the compress configuration CLI and save the configuration and reload the chassis. The chassis comes up with the NVRAM configuration.

- CSCuj88523

  Symptom: In a pseudowire redundancy configuration, traffic may fail to flow after a switchover to a backup pseudowire.

  Conditions: This symptom occurs on the Cisco 7600 series routers.

  Workaround: Execute the following commands on the attachment circuit interface:

  – **shutdown**

  - **no shutdown**

- CSCuj89036

  Symptom: IOSd crashes following an OIR of an eToken..

  Conditions: This symptom occurs during OIR activity on either USB port of a single eToken.

  Workaround: Do not OIR an eToken.

  More Info: When an eToken is inserted, files on the eToken need to be recursively scanned to build up the master file directory structure. This recursive scanning and building the database can take a very long time depending on the eToken contents. When dual IOSd redundancy mode is enabled, this process appears to take almost twice as long and can easily go over 10 seconds to trip off the IOSd watchdog timeout. Fix is to allow other processes to take over CPU so watchdog timeout will not happen.

- CSCuj94571

  Symptom: To run the BERT test, remove **keepalive** from the interface. After completing the BERT test, adding **keepalive** causes the standby RSP to reset.

  Conditions: This symptom is consistent and affects 15.1(3)S1.

  Workaround: After the completion of the BERT test, remove the BERT test with "**no bert pattern qrss interval** *interval* and then add **keepalive**. This will avoid standby RSP reset.

- CSCuj96186

  Symptom: When auto-tunnel and RSVP graceful restart are configured, the standby crashes after an SSO (NSR is not configured).

  Conditions: This symptom occurs under the following conditions:

  - Configure auto-tunnel
  - Configure RSVP graceful restart without NSR
  - Perform an SSO

  Workaround: Disable RSVP graceful restart or remove the auto-tunnel configuration.

- CSCuj99537

  Symptom: Not all LI streams that are properly configured via SNMPv3 and appropriate ACLs and are programmed in TCAM, are intercepted and forwarded towards MD.

  Conditions: This symptom occurs in an SIP-400 based LI.

  Workaround: Remove and reapply the problematic tap but it doesn't prevent the problem from reoccurring if new LI taps are applied via SNMPv3

- CSCul04006

  Symptom: The c7600rsp72043 router crashes while booting from the bootdisk with the following error message:

  ```
  Unable to open file to add LC tar
  bootdisk:c7600rsp72043-advipservicesk9-mz.152-4.S3a.bin
  ```

  Conditions: This symptom occurs while booting from the "bootdisk" on a c7600rsp72043 router.

  Workaround:

  1. After the new image file or the image file which is to be upgraded is copied to "sup-bootdisk", run the verify command to check that the new image file is copied properly. "verify /md5 sup-bootdisk:/<new-image-file> <expected-checksum>". The expected checksum can be found from the CCO site. If "verify" succeeds, then the new image can be booted.

2. Format “sup-bootdisk” and copy the new image to “sup-bootdisk” and run the “verify” command as mentioned above. If "verify" succeeds, then the boot can be tried.

- CSCul04692

  Symptom: A T1 controller flaps in CHT1/ET1 SPA.

  Conditions: This symptom is seen in T1 mode with “cablelength short 100ft” or “cablelength long 0db” when connected with a PURA box.

  Workaround: Configure “cablelength long -7.5db”.

- CSCul11738

  Symptom: Scaling to maximum number of TE tunnels fails.

  Conditions: This symptom occurs when there are sufficient tail-end tunnels on the node.

  Workaround: There is no workaround.

- CSCul11961

  Symptom: While performing an ISSU super-pkg downgrade with broadband IP-based session features from Cisco IOS XE Release 3.12.0 to Cisco IOS XE Release 3.11.0, standby FP gets stuck in an "init" state after run version. There are Standby FP pending issues.

  Conditions: This symptom occurs while performing an ISSU super-pkg downgrade with broadband IP-based session features from Cisco IOS XE Release 3.12.0 to Cisco IOS XE Release 3.11.0.

  Workaround: There is no workaround.

  More Info: The issue will not occurs in the following cases:

  1. ISSU sub-pkg upgrade or downgrade between XE311 and XE312.
  2. ISSU sup-pkg upgrade from XE311 to XE312.
  3. PPP-session features in ISSU super-pkg upgrade or downgrade between XE311 and XE312.

  The upgrade from 3.11.0(without the fix for CSCul11961) to 3.12(with the fix of CSCul11961) works fine.

  The downgrade from 3.12(with the fix of CSCul11961) to 3.11.0(without the fix for CSCul11961) fails with IP-based sessions. With this downgrade bug for 3.11.0, the fix will go out in 3.11.1 and 3.12.0.

- CSCul11995

  Symptom: An L2TPv3 session fails to establish and Cisco IOS receives a StopCCN message from the peer with the following message in response to its ICRP message:

  ```
  “No handler for attr 68 (68)”
  ```

  Conditions: This symptom occurs when IOS device peers with non-IOS devices send IETF L2TPv3 Pseudowire Type AVP (IETF AVP 68) in an ICRP message.

  Workaround: There is no workaround.

- CSCul12583

  Symptom: L4R is not removed after an account logon when DRL is present.

  Conditions: This symptom occurs if per user merge is present.

  Workaround: There is no workaround.

- CSCul24025

  Symptom: A Cisco ASR 1000 Series router crashes when the **ip sla udp-jitter** command is unconfigured.

Conditions: This symptom occurs when 1000+ IP SLA udp-jitter is configured and then all unconfigured immediately.

Workaround: There is no workaround.

- CSCul24682

  Symptom: L2TP LNS puts a non-negotiated magic number to LCP packets. The PPPoE client may terminate the session prematurely due to the unknown magic number.

  Conditions: This symptom occurs when L2TP LAC does not negotiate the magic number with the PPPoE client and L2TP LNS does not renegotiate options with the PPPoE client.

  Workaround: Configure **lcp renegotiation always** on L2TP LNS.

- CSCul27327

  Symptom: On the Cisco c7600 router, if PIM is configured on the port-channel and on the port members, any failure on one of the port members will disable the FE CAM.

  Conditions: This symptom occurs when PIM is configured on the port members.

  Workaround:

  1. Do not configure PIM sparse-mode on the port members even though the CLI is accepted.
  2. In case the PIM sparse-mode is configured on the port members, remove it from the port members and the port-channel and then reapply the PIM configuration on the port-channel only.

  Further Problem Description: A similar issue (CSCtf75608) is seen on the Cisco Catalyst 6500 Series Switches, but the workaround is to configure PIM on the port-channel and the port members to avert the FE CAM to be disabled in the event of one of the port members failing.

- CSCul31953

  Symptom: The wrong value is fetched for plaintext mtu of IPSec SA.

  Conditions: This symptom occurs while configuring Cisco Group Encrypted Transport VPN(GETVPN) within LISP network.

  Workaround: There is no known workaround.

- CSCul38081

  Symptom: In a scaled environment, when a preferred path configuration is removed and is followed by a RP switchover the pseudowire interfaces goes down. The psudowire interface comes up if we add the preferred path or just remove and add the neighbor statement.

  Conditions: This symptom is not observed under any specific conditions.

  Workaround: There is no workaround.

- CSCul40176

  Symptom: PBR next-hop verify availability for global does not work after a reload.

  Conditions: This symptom occurs in **show run** after a reload.

  Workaround: There is no workaround.

- CSCul40898

  Symptom: After reloading the router or fresh service-instance configuration, traffic received from the access is sent to the core without a dummy VLAN header. This traffic is received by a remote PE2 and sent to switch with a missing VLAN header. Therefore CE2 drops received packets. When the issue is removed, captured traffic in the core contains a dummy VLAN header.

  Conditions: This symptom is occasionally observed when the router is reloaded and is consistently observed when a new service instance is configured as an xconnect member.

Workaround: Perform **shutdown** followed by **no shutdown** on the service instance.

- CSCul42480

  Symptom: A router crashes upon booting due to lack of memory for the image.

  Conditions: There are no specific conditions for this symptom.

  Workaround: There is no workaround.

- CSCul47135

  Symptom: On Cisco ASR 1000 routers, services are not removed or applied from the active subscriber sessions when CoA is sent from the radius server. The router sends wrong values in response to the CoA request packet.

  Conditions: This symptom occurs when 15.2(20130918:081157) is run.

  Workaround: There is no workaround.

- CSCul49852

  Symptom: A router might see PPPoE-sessions in the WAITING_FOR_STATS (or WT_ST) status.

  Conditions: This symptom was observed by specific users or because of using a specific profile or service like ShellMaps and Radius. The system is configured as BRAS aggregating PPPoEoA or -oE-sessions.

  Workaround: There is no workaround.

- CSCul50910

  Symptom: After a random reload of chassis or SPA Gig on SPA-5X1GE-V2 loses L3 connectivity and ARP protocol failing.

  Conditions: This symptom is observed in the Cisco 7600 router with SPA-5X1GE-V2.

  Workaround: Reload SIP with SPA loaded in it.

- CSCul52239

  Symptom: Multicast traffic might get affected after an interface delete and reconfiguration. This is more likely to happen in dot1q sub-interfaces in ES+ and specifically only if the delete and reconfiguration of the interface is done within 30 seconds.

  Conditions: This symptom occurs in Cisco IOS Release 12.2SREx and Cisco IOS 15S based releases.

  Workaround: Perform interface delete and reconfiguration with a time gap of one minute.

  More Info: How to check whether the issue is hit:

  Note down the interface’s internal vlan:

  ```
  PE2#sh vlan int usage | i GigabitEthernet2/24.904 2000 GigabitEthernet2/24.904
  Get to SP console and do "sh fid start <internal vlan> end <internal vlan>
  PE2-sp#sh fid start 2000 end 2000 FID Id Protocol Bkt Enabled FE CAM Enabled Vlan
  Don't Learn Age group ------ ------------------- ------------- ---- -----------
  --------- 2000 no no 2000 yes 0x00
  ```

  The issue is hit if “FE CAM Enabled” bit is set to “no”.

- CSCul56207

  Symptom: A standby RP crashes.

  Conditions: This symptom is seen on a Cisco ASR 1000 router used for PPPoEoA-aggregation when configuring a range/pvc. It was seen together with the following error message:

```
asr(config-if-atm-range)pvc-in-range 10/45 %ERROR: Standby doesn't support this
command ^ % Invalid input detected at '^' marker.
```

Workaround: There is no workaround.

- CSCul65614

  Symptom: The FAN-MOD-6SHS module consumes more power than expected (should be around 180W).

  ```
  #sh power <SNIP> Fan Type Watts A @42V State ---- ----------------- ------- ------
  ----- 1 FAN-MOD-6SHS 427.14 10.17 OK
  ```

  Conditions: This symptom occurs when the ES+ Combo card is placed in slot-1 of 7600 chassis.

  Workaround: Place ES+ Combo cards in any other slot other than slot-1 of 7600 chassis.

- CSCul72121

  Symptom: Continuous trace backs on the PTF console is observed and PTF crashes during a soak.

  Conditions: This symptom occurs under the following conditions:

  1. Create an MDS profile as attached.
  2. Leave the setup for soak for 12 hours.

  Workaround: Reload ACT and SBY PTF.

- CSCul86211

  Symptom: When LNS switches off while the sessions keep on establishing at LAC, LAC finds the l2tp db memory exhausted after sometime. Due to this, it fails to update the session in the database and during this period a crash is observed.

  Conditions: This symptom occurs when LAC tries to add l2tp session in the database and fails to do so. In order to handle this error condition, LAC frees the l2tp and l2x session twice. This double free is the reason for crash.

  Workaround: There is no workaround.

- CSCul87037

  Symptom: An “sg subrte conte” chunk leak occurs while roaming.

  Conditions: This symptom occurs after an account-logoff and if service permit is configured in control policy. In case of a service permit, the subscriber remains unauth and is redirected to the portal once again. Post successful second account logon and the subscriber session is cleared by timeout or cli, the leak is seen and the same client will not be able to create the session once again. The leak is seen after simulating for the second time account-logon. And if service permit is configured.

  In case of service disconnect configured under account-logoff, account-logon is not a practical scenario as the portal is not reachable for the client.

  Workaround: Use **service disconnect** for **event account-logoff**.

  ```
  class type control always event account-logoff
  1 service disconnect delay 10
  !
  ```

- CSCul92497

  Symptom: The Cisco 7600 router providing layer2 EoMPLS services may stop forwarding ingress and egress traffic for an xconnect for which a backup peer config has been applied.

Conditions: This symptom occurs in Cisco 7600 routers running Cisco IOS Release 15.2(4)S4a with ES+ cards (access/core facing) and xconnect configured under a service instance.

Workaround: Clear the xconnect on the Cisco 7600 router side. Clearing on the remote size does not have an effect.

- CSCul94087

  Symptom: Output Packet drops is observed on the ATM IMA interface even when there is no live traffic and only signaling exchange between non-Cisco devices. Although output drops in most cases means low bandwidth issues but in this case, an entire site was down due to these drops.

  Conditions: This symptom occurs under the following conditions:

  1. Layer 2 cross connect is configured on Cisco device and Non-Cisco device at other end.
  2. Only signaling traffic flows through the devices.
  3. IMA group is created for the ATM connectivity.
  4. SPA-24CHT1-CE-ATM card is to be used for the ATM connection.

  Workaround: Reload the SPA.

- CSCul99015

  Symptom: In VPLS using BGP signaling with Inter AS, when a PE on another AS is reachable through multiple ASBRs, the PW destination and the next hop PE address of some or all of the PWs in the standby RP remains as the non-preferred ASBR address instead of the preferred ASBR address.

  Conditions: This symptom occurs under the following conditions: 1. BGP L2VPN NLRIs received first from an ASBR becomes a less preferred ASBR on receiving NLRIs for the same VE-IDs from a more preferred ASBR. 2. NLRI received from the more preferred ASBR has the same values (VEID, VBO, VBS, Label Base, MTU and CW) as the ones received previously from the other ASBR.

  Workaround: Bring up the BGP session with the more preferred ASBR first. This would cause no updates to existing NLRIs even if received from other less preferred ASBRs.

- CSCum00056

  Symptom: ASR IOSd crash occurs with the following error:

  ```
  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = ISG CMD HANDLER
  ```

  Conditions: This symptom occurs when changes are made through RADIUS.

  Workaround: There is no workaround.

- CSCum04512

  Symptom: When an RP switchover is done (which is head end for 500 TE tunnel and tail end for 500 TE tunnels), the RSVP label is assigned to the TE tunnel change and this in turn causes a traffic loss of 45 seconds on the pseudowire which is directed through these tunnels.

  Conditions: This symptom occurs under the following conditions:

  – TE RID under the IGP is configured as a loopback other than the first one.

  – SSO is performed.

  Workaround: Configure the TE router ID under the IGP to be the first loopback interface.

- CSCum11118

  Symptom: A Cisco ISR router crashes due to stack overflow in the “ADJ background” process. The following syslog may be seen just before the crash:

```
000105: Dec 9 04:08:44.447 UTC: SYS-6-STACKLOW Stack for process ADJ background
running low, 20/6000
```

Conditions: The conditions to this symptom are unknown.

Workaround: There is no workaround.

- CSCum16315

  Symptom: Upon reload of a Cisco 7600 router configured with a CoPP policy containing IPv6 ACLs and DSCP matching, the CoPP is only applied to the active RSP as shown below.

  After reload:

```
lab-7609-rsp-02#sh mod power Mod Card Type Admin Status Oper Status ---
----------------------------------- ------------ ----------- 1 CEF720 48 port
10/100/1000mb Ethernet on on 5 Route Switch Processor 720 (Active) on on 6 Route
Switch Processor 720 (Hot) on on 7 CEF720 8 port 10GE with DFC on on 8 CEF720 8 port
10GE with DFC on on
```

  CoPP is applied to only the active RSP/SUP after reload:

```
lab-7609-rsp-02#sh policy-map control-plane in | inc class|Earl class-map:
COPPCLASS_MCAST (match-any) Earl in slot 5 : class-map: COPPCLASS_MGMT (match-any)
Earl in slot 5 : class-map: COPPCLASS_ALLOW_ICMP (match-any) Earl in slot 5 :
class-map: COPPCLASS_MONITORING (match-any) Earl in slot 5 : class-map:
COPPCLASS_FILEXFER (match-any) Earl in slot 5 : class-map: COPPCLASS_REMOTEACCESS
(match-any) Earl in slot 5 : class-map: COPPCLASS_OSPF (match-any) class-map:
COPPCLASS_LDP (match-any) Earl in slot 5 : class-map: COPPCLASS_BGP (match-any)
class-map: COPPCLASS_MISC (match-any) class-map: COPPCLASS_UNDESIRABLE (match-any)
Earl in slot 5 : class-map: COPPCLASS_IPV4_CATCHALL (match-any) Earl in slot 5 :
class-map: COPPCLASS_IPV6_CATCHALL (match-any) class-map: class-default (match-any)
Earl in slot 5 :
```

  When this issue is triggered, the following error will be seen in the logs:

```
*Dec 14 02:33:14.579: %QM-2-TCAM_BAD_LOU: Bad TCAM LOU operation in ACL
```

  This issue potentially exposes the device to a DoS vulnerability.

  Conditions: This symptom occurs under the following conditions:

  1. 7600 HA Environment.
  2. CoPP IPV6 ACL with DSCP match.
  3. Reload or Switchover.

  Workaround: There are two workarounds for this issue.

  1. Modify the CoPP Policy to remove IPV6 ACL/DSCP matching.
  2. Remove and reapply the CoPP configuration as shown below:

```
lab-7609-rsp-02(config)#control-plane
lab-7609-rsp-02(config-cp)#no service-policy in COPP
lab-7609-rsp-02(config-cp)#service-policy in COPP
lab-7609-rsp-02(config-cp)#end
```

  CoPP is applied to all modulues as required:

```
lab-7609-rsp-02#sh policy-map control-plane in | inc class|Earl class-map:
COPPCLASS_MCAST (match-any) Earl in slot 1 : Earl in slot 5 : Earl in slot 7 : Earl in
slot 8 : class-map: COPPCLASS_MGMT (match-any) Earl in slot 1 : Earl in slot 5 : Earl
in slot 7 : Earl in slot 8 : class-map: COPPCLASS_ALLOW_ICMP (match-any) Earl in slot
1 : Earl in slot 5 : Earl in slot 7 : Earl in slot 8 : class-map: COPPCLASS_MONITORING
(match-any) Earl in slot 1 : Earl in slot 5 : Earl in slot 7 : Earl in slot 8 :
class-map: COPPCLASS_FILEXFER (match-any) Earl in slot 1 : Earl in slot 5 : Earl in
```

```
slot 7 : Earl in slot 8 : class-map: COPPCLASS_REMOTEACCESS (match-any) Earl in slot 1
: Earl in slot 5 : Earl in slot 7 : Earl in slot 8 : class-map: COPPCLASS_OSPF
(match-any) Earl in slot 1 : Earl in slot 5 : Earl in slot 7 : Earl in slot 8 :
class-map: COPPCLASS_LDP (match-any) Earl in slot 1 : Earl in slot 5 : Earl in slot 7
: Earl in slot 8 : class-map: COPPCLASS_BGP (match-any) Earl in slot 1 : Earl in slot
5 : Earl in slot 7 : Earl in slot 8 : class-map: COPPCLASS_MISC (match-any) Earl in
slot 1 : Earl in slot 5 : Earl in slot 7 : Earl in slot 8 : class-map:
COPPCLASS_UNDESIRABLE (match-any) Earl in slot 1 : Earl in slot 5 : Earl in slot 7 :
Earl in slot 8 : class-map: COPPCLASS_IPV4_CATCHALL (match-any) Earl in slot 1 : Earl
in slot 5 : Earl in slot 7 : Earl in slot 8 : class-map: COPPCLASS_IPV6_CATCHALL
(match-any) Earl in slot 1 : Earl in slot 5 : Earl in slot 7 : Earl in slot 8 :
class-map: class-default (match-any) Earl in slot 1 : Earl in slot 5 : Earl in slot 7
: Earl in slot 8 :
```

- CSCum20242

  Symptom: The RSP720 image bootup fails with the following messages:

  ```
  rommon 2 > boot disk0:rsp72043-adventerprisek9-mz Initializing ATA monitor library...
  Self extracting the image... [OK] Error : memory requirements exceed available memory
  Memory required : 0x40286C44 *** System received a Software forced crash *** signal=
  0x17, code= 0x4, context= 0x0
  ```

  Conditions: This symptom could occur when the image size is very big (approximately greater than 220MB). This is not reported in any production images so far because their size is not big enough to hit this issue.

  Workaround: There is no workaround.

- CSCum24565

  Symptom:

  – MPLS is being processed by the CPU instead of HW switching

  – "rem com sw show mls vlan-ram" shows "0" value under vpn-num and netdr shows that mpls is being processed by the CPU:

  ```
  Example: 7600#rem comm sw sh mls vlan-ram 1906 1906
  TYCHO Vlan RAM Key: * => Set, - => Clear
  vlan eom nf-vpn mpls mc-base siteid stats rpf vpn-num bgp-grp l2-metro rpf-pbr-ovr
  ----+---+------+----+-------+------+-----+---+-------+-------+--------+-----------
  1906 * - * 0 0 - - 0 0 - * <<<=== vpn-num 0
  ```

  – There is a possibility of a high CPU due to interrupts.

  Conditions: The symptom may occur on 7600 Series Routers after SSO is performed on PE with L2VPN in PFC vlan mode is configured

  Workaround:

  1. Remove xconnect configuration from the subinterface and reconfigure it.
  2. shut/no shut the xconnect source interface.

- CSCum34830

  Symptom: A router crash is observed.

  Conditions: This symptom occurs while performing VRRP and VRRS-related configuration changes.

  Workaround: Unconfigure the **ip pim redundancy <>** command before deleting the subinterface or disabling PIM on an interface.

- CSCum42586

  Symptom: SLM does not work over the port-channel evc xconnect up mep.

Conditions: This symptom occurs when port-channel member links are on the same NP.

Workaround: There is no workaround.

- CSCum46850

  Symptom: Using LISP set tags on routes imported to the RIB when exporting LISP routes from the RIB to BGP fails.

  Conditions: This symptom occurs when redistribute list route-map is used under bgp with a route-map that contains match tag.

  Workaround: There is no workaround.

- CSCum62783

  Symptom: The following alignment errors are seen after a PPPoE session establishment for the first time after a reboot:

```
*Jan 14 07:24:40.591: %ALIGN-3-CORRECT: Alignment correction made at 0x32B2DFF4z
reading 0xE7790ED *Jan 14 07:24:40.591: %ALIGN-3-TRACE: -Traceback= 0x32B2DFF4z
0x32B1E274z 0x32B1EECCz 0x32B1EF90z 0x332E550Cz 0x332E54F0z 0xFFFF1A00z 0xFFFF1A00z
```

  Conditions: This symptom occurs when **pppoe-client ppp-max-payload** is configured under the Ethernet interface.

  Workaround: There is no workaround.

- CSCum65501

  Symptom: IPv6 CoPP ACL in PI matches traffic incorrectly for sw-switched paks. Packets are not hit against IPv6 ACE matching on L4 protocol. This causes traffic to be classified incorrectly.

  Conditions: This symptom occurs with recent Cisco IOS images. Results are as expected on Cisco IOS Release 12.2(33)SRE9a. However, it is broken in Cisco IOS Release 15.2(4)S4a onwards.

  Workaround: There is no workaround.

- CSCum67166

  Symptom: The router hangs after loading an image.

  Conditions: This symptom occurs with the latest whales-universal-mz mcp_dev image.

  Workaround: There is no workaround.

- CSCum85813

  Symptom: Shut primary static router and secondary static is not installed automatically.

  Conditions: This symptom is seen on the sites where the BFD state of the backup static route is marked as “U” in the output of “show ip static route bfd”.

  Workaround: Reinstall the default backup static route.

- CSCun38333

  Symptom: Locator ID Separation Protocol (LISP) local EID database locator configured through the "**database-mapping** <*eid-prefix*> **ipv6-interface** <*interface*> **priority** <*priority*> **weight** <*weight*>" command uses deprecated IPv6 address on specified interface.

  Conditions: Multiple IPv6 addresses available on an interface with the lexicographically first address being deprecated.

  Workaround: There is no workaround.

- CSCun57668

Symptom: LISP local EID database locator configured through the **database-mapping** <*eid-prefix*> **ipv6-interface** <*interface*> **priority** <*priority*> **weight** <*weight*> command can be a deprecated IPv6 address on a specified interface.

Conditions: This symptom is observed in multiple IPv6 addresses available on an interface with the lexicographically first address being deprecated.

Workaround: There is no workaround.

Open and Resolved Bugs - Cisco ASR 901 Series Routers in 15.4(2)S

For detailed information on Open and Resolved bugs on Cisco ASR 901 Series Routers in 15.4(2)S, see the following document:

https://www.cisco.com/c/en/us/td/docs/wireless/asr_901/Release/Notes/b-901-rn-15-4-2.html

Open and Resolved Bugs - Cisco ASR 901 S Series Routers in 15.4(2)S

For detailed information on Open and Resolved bugs on Cisco ASR 901 S Series Routers in 15.4(2)S, see the following document:

https://www.cisco.com/c/en/us/td/docs/wireless/asr_901s/scg/b_scg_for_asr901s.html

Open and Resolved Bugs - Cisco ME 3600x and ME 3800x Series Routers in 15.4(2)S

For detailed information on Open and Resolved bugs on Cisco ME 3600x and Cisco ME 3800x Series Routers in Cisco IOS Release 15.4(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

Bugs for Cisco IOS Release 15.4(1)S

Open and 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 and go to 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:

Open Bugs—Cisco IOS Release 15.4(1)S3

Table 1 Open Bugs—Cisco IOS Release 15.4(1)S3

Identifier	Description
CSCur32628	7600 mis-programming causing intermittent packet loss
CSCur70478	Software crash at ldpx_mem_reallocz_grow due to insufficient memory
CSCur77750	CSCtc51539 happening again on SRE6 onwards
CSCur53326	ASR crash at "IP Inband Session Initiator"

Identifier	Description
CSCuh92882	XE3.11 Seginfo->l2hw_cond_debug is set to "1" when there is no condition
CSCur68259	XE3.13 : Subscribers not pingable after 2nd "clear ip route vrf x *"
CSCua76379	%SYS-3-DUP_TIMER: Same tty1 in linewatch_timers errors in log.

Resolved Bugs—Cisco IOS Release 15.4(1)S3

Table 2 Resolved Bugs—Cisco IOS Release 15.4(1)T3

Identifier	Description
CSCup01885	ASR Reboots Once A week
CSCug18580	ASR1k crash: UNIX-EXT-SIGNAL SEGFAULT, Process = AAA ACCT Proc
CSCup42385	HA fails due to Bulk synch failure with encypted password
CSCup98776	ASR1K outbund SA creation failure & ESP not processing further requests
CSCup53658	ASR1k qinq subinterface stats do not work on Port Channel
CSCuo56871	ASR route server crashes due in BGP task
CSCun92095	asr1001x crashes when unconfiguring MPLS LDP scale config
CSCug08566	BGP does not advertize a global static route pointing to a vrf intf
CSCuo53561	BGP failed to apply inbound route-map on prefixes after switch over
CSCuo76187	BGP sends out VPN invalid update without label in MP_REACH
CSCuq24984	In rare high BGP update churn case, sh ip bgp x.x.x.x may crash
CSCup52988	InterAS OptionB ASBR does not allocate label for VPNv4 prefix
CSCun68542	invalid prefixes learned from RR with bgp add-path feature enabled
CSCun58072	ifOutOctets go backwards when output drop happens on FR subintf
CSCuq17550	ISRG2-GETVPN-IPv6 Egress IPv6 Interface ACL checked before encryption
CSCup70579	Malformed mDNS packet may cause a reload
CSCuj31290	Packet of Disconnect is Broke after upgrade from 15.1 to 15.2
CSCup89513	Router crash at dual_routeupdate
CSCul70788	Router crashes when calculating the best cost successor in EIGRP DUAL
CSCup06433	Selection of wrong LFA leads to crash during deletion of LFA
CSCul22914	ISR4451-X FIPS: Crypto Device power-up KAT selftests broken
CSCuq93406	IOSd crash on Ethernet CFM receiving a malformed CFM frame
CSCul11486	isrg2 reloaded while quering the objects of ieee8021CfmStackTable
CSCuo49923	c4mk13:Device crash with Unexpected exception to CPU after RV.
CSCun88267	need particle version of reg_invoke_fast_ipwrite() to avoid Q wedge

Identifier	Description
CSCuo84660	copy command yields DATACORRPUTION error
CSCuq96691	Utah crash during ezconfig installation.
CSCup22487	Multiple Vulnerabilities in BinOS OpenSSL - June 2014
CSCun75719	c4mk2: Device getting crashed after rpr and sso.
CSCuj96546	c4mk2:Packet drop with egress WCCP GRE red/L2 ret/Hash assign after sso
CSCuo48507	ISSU:XE310<->XE311 Packet drops seen with ikev2_dvti after switchover
CSCuh07579	IPSec fails to delete/create SAs due to IPSec background process stuck
CSCup51813	XR Control Packets and Data packets getting dropped on rekeying
CSCuq46955	IOS ISR AM IKEv1 doesnt work with rsa-sig
CSCup94123	ISSU:XE311->XE312 pseudo_wire VC status and LDP are down after RP SWO
CSCum45122	mvpnv6: ipv6 mfib stale entry on PE after toggling address-family
CSCum01661	MPLS Traffic drop after SSO, Label is NONE with IPFRR config
CSCuo97889	Traffic is getting drop after TE-SSO
CSCui85237	C3900 router crashed with MQC mode with mix of protocols
CSCuj40124	crash@stile_mtp_dp_post_cls_run when sending the specific pcap file
CSCum45864	MTP signatures failed due to addition on new custom MTP fields
CSCum66102	Router crashes @ stile_free_cnbar_protocols
CSCul05056	SYS-6-STACKLOW due to NBAR config
CSCup49206	Conditional Default route getting flushed on peer performing SSO on UUT.
CSCup04305	Router Crash seen @ __be_ospf_schedule_rtr_lsa
CSCuo83510	Stack overflow detected at ospfv3_router_process upon boot with NBMA cfg
CSCuo37123	PIM process sends out huge Hello bursts after SSO switchover on 7600
CSCuq64710	Large memory leak on RP SSS/SSM processes during pppoe churn
CSCui45885	NAT SIP ALG is translating SIP headers when the service is disabled.
CSCun52430	FFM: Queue-limit not getting updated during unconfig
CSCui23670	Even if show sup-bootdisk is executed, nothing is displayed.
CSCuc68034	IO Memory Leak on FlexWan WS-X6582-2PA exec 'sh cef interface internal'
CSCuo93711	ASR Standby RP - RSVP severely leaking memory
CSCup22590	Multiple Vulnerabilities in IOS/IOSd OpenSSL - June 2014
CSCup86552	Issue with qos service installation

Identifier	Description
CSCup52725	XE3.13: asr1k RP Crash while 72 hour longevity run
CSCup98776	ASR1K outbund SA creation failure & ESP not processing further requests
CSCuq17550	ISRG2-GETVPN-IPv6 Egress IPv6 Interface ACL checked before encryption
CSCul22914	ISR4451-X FIPS: Crypto Device power-up KAT selftests broken
CSCuj96546	c4mk2:Packet drop with egress WCCP GRE red/L2 ret/Hash assign after sso
CSCuo48507	ISSU:XE310<->XE311 Packet drops seen with ikev2_dvti after switchover
CSCuh07579	IPSec fails to delete/create SAs due to IPSec background process stuck
CSCup51813	XR Control Packets and Data packets getting dropped on rekeying
CSCuq46955	IOS ISR AM IKEv1 doesnt work with rsa-sig
CSCup22590	Multiple Vulnerabilities in IOS/IOSd OpenSSL - June 2014

Resolved Bugs—Cisco IOS Release 15.4(1)S2

- CSCee32792

  Symptom: A Cisco router reloads at snmp_free_variable_element while using SNMPv3 commands.

  Conditions: This symptom occurs while using SNMPv3 commands.

  Workaround: There is no workaround.

- CSCtq21722

  Symptom: A Cisco switch may reload when configured for SNMP.

  Conditions: This symptom is observed when SNMP inform hosts are configured.

  Workaround: Remove the SNMP host configurations for SNMP informs.

  ```
  Example: no snmp-server host x.x.x.x informs version 2c <removed>
  ```

- CSCtx82890

  Symptom: After removing the encapsulation on MFR member interface, tracebacks are observed.

  Conditions: This symptom is observed when serial interface is configured with FR MLP configuration.

  Workaround: There is no workaround.

- CSCtz45833

  Symptom: A Cisco router crashes with the following message:

  ```
  Router crash: UNIX-EXT-SIGNAL: Segmentation fault(11), Process = MPLS TE LM
  ```

  Conditions: This symptom occurs when a router acts as the mid point for MPLS-TE tunnels and performs an ERO expansion. In case the ERO expansion fails (due to IGP race conditions or inter-AS scenario) and backup tunnels are in use (for MPLS-TE FRR feature), the router may crash.

Workaround: Configure the head-ends to perform a full ERO computation to avoid mid points performing any ERO expansion. This can be done using the dynamic path option or by using the explicit path that specifies strict hops for each node along the desired LSP path (using “loose” hops or partial strict hops can lead to this issue).

- CSCtz97771

  Symptom: During regular operations, a Cisco router running Cisco IOS release 12.4(24)T and possibly other releases experiences a crash. The crash info will report the following:

  ```
  %SYS-2-FREEFREE: Attempted to free unassigned memory at 4A001C2C, alloc 4180794C, 
  dealloc 417616B0,
  %SYS-6-BLKINFO: Attempt to free a block that is in use blk 4A001BFC, words 134, alloc 
  4180794C, Free, dealloc 417616B0, rfcnt 0,
  ```

  Conditions: This symptom is not observed under any specific conditions.

  Workaround: There is no workaround.

- CSCuc21859

  Symptom: Memory leak is seen at ssf_owner_get_feature_sb.

  Conditions: This symptom occurs when the discriminator configuration is with logging, as given in the below examples:

  ```
  logging discriminator <NAME>
  logging host x.x.x.x discriminator DEBUG
  logging discriminator SysLog mnemonics drops NAME
  ```

  Workaround: Remove the discriminator configuration from the logging configuration.

- CSCuc60868

  Symptom: A router randomly crashes either due to memory corruption at bgp_timer_wheel or memory chunks near bgp_timer_wheel (for example, BFD event chunks if BFD is configured or AtoM Manager chunks if LDP is configured). A crash occurs right after an LDP neighbor is up in the L2VPN setup.

  Conditions: This symptom occurs when **vpls bgp signaling** is unconfigured and then reconfigured. Both L2VPN and BGP are unconfigured and reconfigured after all L2VPN and BGP data structures are fully deleted (about 3 minutes for 5 BGP VPLS prefixes). For the repro on file, OSPF (for IGP) is also unconfigured and reconfigured. Both LDP and BGP signaling are affected by this bug.

  Workaround: Avoid unconfiguring and reconfiguring BGP L2VPN.

- CSCue23898

  Symptom: A Cisco router running Cisco IOS Release 15.3(1)T may crash with a bus error immediately after issuing the **write memory** command.

  ```
  Example: 14:44:33 CST Thu Feb 14 2013: TLB (load or instruction fetch) exception, CPU 
  signal 10, PC = 0x228B2C70
  ```

  Conditions: This symptom occurs while updating the router’s running configuration with the **write memory** command.

  It has been seen while updating various different commands such as,

  those under “call-manager-fallback” ip route statements interface subcommands

  Workaround: There is no workaround.

- CSCuh45042

  Symptom: Traffic on some GIG subinterfaces are seen to be dropped at the SPA. The SPA TCAM is seen to have two entries sharing the same logical address as a result of which one entry is seen to overwrite the other.

  Conditions: This symptom was observed after a router/LC/SPA reload. The exact condition that triggers this symptom is not known.

  Workaround: There is no workaround.

- CSCuh87195

  Symptom: A crash is seen on a Cisco router.

  Conditions: The device crashes with gw-accounting and call-history configured. The exact conditions are still being investigated.

  Workaround: Perform the following workaround:

  1. Completely remove gw-accounting
  2. Disable call-history using the following commands:

  ```
  gw-accounting file
  no acct-template callhistory-detail
  ```

- CSCui05000

  Symptom: A Cisco router may crash upon importing a prefix into VRF after applying **no ipv4 multicast multitopology** under “vrf definition” for that VRF.

  Conditions: This symptom occurs while initially configuring the VRF. **address-family ipv4/6 multicast vrf** must be configured under “router bgp” mode before import route-targets are configured under “vrf definition” mode.

  Workaround: There is no workaround.

  More Info: If the crash does not occur, it is likely that importing of the prefix will not work.

- CSCui12822

  Symptom: The version of the GCC compiler (tool) used for builds in CEL 5.50 needs to be updated to a version that can work on CEL 5.50.

  Conditions: This symptom does not occur under specific conditions.

  Workaround: Update the version of the GCC compiler to a version that can work on CEL 5.50

- CSCui23099

  Symptom: A Cisco router with an etherswitch module installed may have the internal interface from the router to the switch become wedged. This will cause any traffic which needs to be process switched to not work. In addition further traffic will throttle the interface.

  This example is from a router in the lab. It is a 2811 with a NME-16ES-1G-P installed. This adds a new interface on the router which allows traffic from the etherswitch to the router. When specific traffic is send the interface becomes wedged. The telltale sign of the interface being wedged is having the input queue report more traffic than the size of the queue itself. For example:

  ```
  GigabitEthernet1/0 is up, line protocol is up
  Input queue: 76/75/585/0 (size/max/drops/flushes);
  Total output drops: 0 0 runts, 0 giants, 585 throttles
  ```

  Conditions: The exact conditions which cause this are unknown, but this has been seen with Wake On LAN (WOL) traffic being sent from a device connected to the etherswitch.

  Workaround: Currently there is no work around other than to block the traffic.

- CSCui29745

  Symptom: Member links under MLPPP go down as the LCP negotiation of those PPP links fails.

  Conditions: This symptom occurs after the router reloads and the traffic is flowing through the multilink.

  Workaround: Reload SPA/LC on the other end of the link.
- CSCui34165

  Symptom: Port-channel QoS features might fail to work after a router reload, followed by QoS configuration modification.

  Conditions: This symptom occurs when a VLAN load-balanced port-channel is used with policy aggregation configuration where the QoS policy is configured on member links and the port-channel subinterface, and after a system reload (configuration is from startup configuration).

  Workaround: Reload the router without port-channel QoS configuration, and add port-channel QoS configuration to the running configuration after the router boots up.
- CSCui64807

  Symptom: An active RP crashes during FIB sync because of memory overrun when the standby sup becomes unavailable.

  Conditions: This symptom occurs when redundant RPs are configured in SSO mode and the standby RP becomes unavailable (for instance because of crash or physical removal). The issue occurs only on Cisco 7600 RSP 720, Cisco 7600 Series Supervisor Engine 720, and Cisco 7600 platforms where the tableid “ISSU FOF LC” support is enabled. As of 03/17/2014, the tableid “ISSI FOF LC” feature is only supported on SY releases. This issue does not impact Cisco ASR 1000 Series platforms.

  Workaround: There is no workaround.
- CSCui83823

  Symptom: When CU executes “show tech” or any show commands which gives a long output using putty, the SSH2 putty closes prematurely.

  Conditions: This symptom is observed when “term length 0” is enabled. The putty session closes prematurely while executing “show tech show memory”.

  Workaround: Redirect the output to a file.
- CSCuj19201

  Symptom: Reregistration time is recalculated on GM nodes upon receiving a TBAR rekey, based on the remaining TEK lifetime at the time of the TBAR rekey.

  This effectively causes a much-shorter re-registration window compared to the one obtained at the GM registration, even if the original TEK lifetime was configured with a long value.

  Conditions: This symptom is observed when TBAR is configured and long TEK lifetime used (more than 7200 seconds).

  Workaround: There is no workaround.
- CSCuj27424

  Symptom: Licensing auto update process CPUHogs/Tracebacks seen while running regression suites.

  Conditions: The CPUHOG will occur when memory traceback CLI are configured, which is as expected. Also a warning is displayed when memory CLI configuration is applied.

  Workaround: There is no workaround.

- CSCuj82897

  Symptom: The “control-word” length is not set properly for small HDLC packets running over HDLC AToM VC with SIP-200.

  ```
  For example: SPA-8XCHT1/E1.
  ```

  Conditions: This symptom occurs when HDLC AToM VC with SIP-200 is deployed, for example, SPA-8XCHT1/E1, will result in a packet length mismatch issue or dropping by the remote PE router when HDLCoverMPLS runs over the Ethernet link adding an additional padding which cannot be classified at all.

  Workaround: Use SIP-400.

- CSCul01067

  Symptom: Memory leak occurs in process and I/O memory.

  Conditions: This symptom is observed when NTPv6 is configured, for example, “ntp server ipv6 2001::1”

  Workaround: Remove the NTPv6 configuration.

- CSCul18552

  Symptom: After a switchover, QoS policy map in standby is not synced as in the case of active.

  Conditions: This symptom occurs after a switchover.

  Workaround: There is no workaround.

- CSCul27924

  Symptom: Customer experienced crash on ASR-1001 during normal operation.

  Conditions: This symptom is not observed under any specific condition.

  Workaround: There is no workaround.

- CSCul32547

  Symptom: During NTT EFT customers performed COA with parent session id as key and when it was attempted the Cisco ASR 1000 router reloads with the following trace code:

  ```
  % 0x7fba0ee : __be___doprnt % 0x83e8bd4 : __be_vsnprintf % 0x83e8b7a : __be_snprintf %
  0x3429013 : __be_encode_cisco_vsa % 0x3428909 : __be_encode_rad_vsa % 0x342b79c :
  __be_attrib_op_encode % 0x34451d4 : __be_build_radius_packet_from_list % 0x3444b3b :
  __be_build_radius_packet % 0x34432fd : __be_send_radius_pkt % 0x6d629d :
  __be_process_response_req % 0x6da280 : __be_process_aaa_request % 0x6d48e6 :
  __be_aaa_acct_proc
  ```

  Conditions: This symptom occurs due to continuous printing.

  Workaround: There is no workaround.

- CSCul39964

  Symptom: Sessions do not get cleared. They get stuck in WT_ST state.

  Conditions: This symptom occurs when sessions are closed in bulk mode by shutting any trunk link or during a clear all session from DUT.

  Workaround: There is no workaround.

  More Info: The memory leak issue and WT_ST are related. Along with memory leak, sessions are not cleared on the active RP as they get stuck in WT_ST state.

  ```
  asr1k-1#sh clock
  07:18:07.045 CET Thu Nov 14 2013
  asr1k-1#su
  ```

```
PTA : Locally terminated sessions
FWDED: Forwarded sessions
TRANS: All other sessions (in transient state)
TOTAL PTA FWDED TRANS
TOTAL 14465 0 6557 7908
GigabitEthernet0/0/0 3024 0 0 3024
GigabitEthernet0/0/1 2587 0 0 2587
GigabitEthernet0/1/0 2297 0 0 2297
GigabitEthernet0/1/1 6557 0 6557 0
asr1k-1#
asr1k-1#
asr1k-1#
asr1k-1#sh clock
07:20:08.295 CET Thu Nov 14 2013
asr1k-1#su
PTA : Locally terminated sessions
FWDED: Forwarded sessions
TRANS: All other sessions (in transient state)
TOTAL PTA FWDED TRANS
TOTAL 14465 0 6557 7908
GigabitEthernet0/0/0 3024 0 0 3024
GigabitEthernet0/0/1 2587 0 0 2587
GigabitEthernet0/1/0 2297 0 0 2297
GigabitEthernet0/1/1 6557 0 6557 0
asr1k-1#
asr1k-1#
asr1k-1#sh clock
07:46:34.113 CET Thu Nov 14 2013
asr1k-1#su
PTA : Locally terminated sessions
FWDED: Forwarded sessions
TRANS: All other sessions (in transient state)
TOTAL PTA FWDED TRANS
TOTAL 14465 0 6557 7908
GigabitEthernet0/0/0 3024 0 0 3024
GigabitEthernet0/0/1 2587 0 0 2587
GigabitEthernet0/1/0 2297 0 0 2297
GigabitEthernet0/1/1 6557 0 6557 0
asr1k-1#
asr1k-1#s
6557 sessions in FORWARDED (FWDED) State
7908 sessions in WAITING_FOR_STATS (WT_ST) State
14465 sessions totalUniq ID PPPoE RemMAC Port VT
VA State
SID LocMAC VA-st Type
5978 5978 0000.6ca3.0116 Gi0/0/0.2940148 1 Vi2.3091 WT_ST
b414.8901.8e00 VLAN: 294/148 UP
5979 5979 0000.6ca3.0117 Gi0/0/0.2940149 1 Vi2.3092 WT_ST
b414.8901.8e00 VLAN: 294/149 UP
6460 6514 0000.6ca3.0134 Gi0/0/0.2940178 1 Vi2.3354 WT_ST
b414.8901.8e00 VLAN: 294/178 UP
6454 6508 0000.6ca3.0135 Gi0/0/0.2940179 1 Vi2.3350 WT_ST
b414.8901.8e00 VLAN: 294/179 UP
6453 6507 0000.6ca3.0136 Gi0/0/0.2940180 1 Vi2.3349 WT_ST
b414.8901.8e00 VLAN: 294/180 UP
6518 6572 0000.6ca3.0137 Gi0/0/0.2940181 1 Vi2.3395 WT_ST
b414.8901.8e00 VLAN: 294/181 UP
6514 6568 0000.6ca3.0138 Gi0/0/0.2940182 1 Vi2.3393 WT_ST
b414.8901.8e00 VLAN: 294/182 UP
6516 6570 0000.6ca3.0139 Gi0/0/0.2940183 1 Vi2.3394 WT_ST
b414.8901.8e00 VLAN: 294/183 UP
6560 6614 0000.6ca3.013a Gi0/0/0.2940184 1 Vi2.3413 WT_ST
```

- CSCul41442

  Symptom: In the M train of IOS and the S train of IOS-XE the “media anti-trombone” feature added in Cisco IOS Release 15.1(3)T, CUBE does not appear as an option when configuring “voice class media” groups. It is not present as an option at the dial-peer level as well.

  Conditions: This symptom is observed in any non “T” train of IOS and IOS-XE.

  IOS Tested 15.2(3)T - Available as media option Tested 15.3(3)M - not there

  IOS-XE Tested 15.1(3)T - Available as media option Tested 15.3(3)S1 - not there

  Workaround: Customer has to have a “T” train IOS of Cisco IOS Release 15.1(3)T or higher.

  More Info: Impacts customers ability to deploy Cube Enterprise solutions.

- CSCul49375

  Symptom: The Cisco ASR 1000 router displays the following messages in the logs:

  ```
  %IDMGR-3-INVALID_ID: bad id in id_get (Out of IDs!) (id: 0x0) -Traceback=
  1#cb40dca901558e45a65b881a8695af4f :400000+8653B3 :400000+893696 :400000+DF330C
  :400000+DED89B :400000+DF8643 :400000+1F57F36 :400000+1F4BBFB :400000+1F33BA7
  :400000+1F336C1 :400000+1F34FF9 :400000+1F27763 :400000+1F29B16 :400000+2546FF3
  :400000+2546EDD :400000+1F2930B
  ```

  No new PPPoE sessions can be established anymore.

  Conditions: The conditions to this symptom are unknown.

  Workaround: Reload the device.

- CSCul49852

  Symptom: A router might see PPPoE-sessions in the WAITING_FOR_STATS (or WT_ST) status.

  Conditions: This symptom was observed by specific users or because of using a specific profile or service like ShellMaps and Radius. The system is configured as BRAS aggregating PPPoEoA or -oE-sessions.

  Workaround: There is no workaround.

- CSCul50910

  Symptom: After a random reload of chassis or SPA Gig on SPA-5X1GE-V2 loses L3 connectivity and ARP protocol failing.

  Conditions: This symptom is observed in the Cisco 7600 router with SPA-5X1GE-V2.

  Workaround: Reload SIP with SPA loaded in it.

- CSCul59525

  Symptom: A Cisco ASR 1000 cube running Cisco IOS Release XE3.8S, many hung calls are seen over a period of one week. There are three different symptoms of hung call legs.

  ```
  Example 1: One of the call leg is in stuck state
  Example 2: Both the call legs are active and connected and stuck for more than week
  Example 3: Both call legs are stuck in disconnect state but one of the call is
  connecting and other leg is in active state.
  Topology:
  VzB ---sip----CUBE------sip------SME Cluster-----sip------Admin04 cluster---------IP
  Phones | | | ----------------sip trunk to fax server | | ------------------SIP trunk
  to Unity connection vm
  ```

  Conditions: Though the reason for this issue is unknown, it is very random in nature. Hung calls are seen for a normal sip to sip calls going to IP phone, or calls that routes to unity connection voicemail and also stuck fax calls.

Workaround: There is no workaround. However, reboot the box to clear the stuck calls.

More Info: Examples of single leg stuck calls:

```
---------------------------------------- 1E95 : 82689 40831920ms.1 (11:56:22.410 EST
Tue Nov 12 2013) +4130 pid:200 Answer 14178002600 active dur 1w2d tx:0/0 rx:0/0 dscp:0
media:0 audio tos:0xB8 video tos:0x0 IP 172.31.133.132:23322 SRTP: off rtt:0ms
pl:0/0ms lost:0/0/0 delay:0/0/0ms g729r8 TextRelay: off Transcoded: No media inactive
detected:n media contrl rcvd:n/a timestamp:n/a long duration call detected:n long
duration call duration:n/a timestamp:n/a
```

Example of two leg stuck calls:

```
------------------------------------------ 1E : 288165 141617380ms.1 (15:56:07.871
EST Wed Nov 13 2013) +-1 pid:220 Answer 8039058000 connected dur 00:00:00 tx:0/0
rx:0/0 dscp:0 media:0 audio tos:0xB8 video tos:0x0 IP 10.190.204.107:22476 SRTP: off
rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g729r8 TextRelay: off Transcoded: Yes media
inactive detected:n media contrl rcvd:n/a timestamp:n/a long duration call detected:n
long duration call duration:n/a timestamp:n/a
1E : 288177 141625940ms.1 (15:56:16.431 EST Wed Nov 13 2013) +3060 pid:245 Originate
8778074646 active dur 1w0d tx:0/0 rx:1/160 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 172.31.122.164:23688 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw
TextRelay: off Transcoded: Yes media inactive detected:n media contrl rcvd:n/a
timestamp:n/a long duration call detected:n long duration call duration:n/a
timestamp:n/a
```

Examples of two leg stuck calls and one leg

```
-------------------------------------------------------------- 3D41 : 447386
220196650ms.1 (13:45:47.147 EST Thu Nov 14 2013) +-1 pid:200 Answer 3186810693
connecting dur 00:00:00 tx:0/0 rx:0/0 dscp:0 media:0 audio tos:0xB8 video tos:0x0 IP
172.31.133.132:25856 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw
TextRelay: off Transcoded: No media inactive detected:n media contrl rcvd:n/a
timestamp:n/a long duration call detected:n long duration call duration:n/a
timestamp:n/a
3D41 : 447387 220196650ms.2 (13:45:47.147 EST Thu Nov 14 2013) +20380 pid:20003
Originate 9724445770 active dur 6d23h tx:0/0 rx:0/0 dscp:0 media:0 audio tos:0xB8
video tos:0x0 IP 10.144.132.72:20062 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0
delay:0/0/0ms g711ulaw TextRelay: off Transcoded: No media inactive detected:n media
contrl rcvd:n/a timestamp:n/a long duration call detected:n long duration call
duration:n/a timestamp:n/a
```

- CSCul73789

  Symptom: In an IPv6 IPSec scenario, code crashes occur with traffic flowing. This is seen even with a single tunnel with traffic flowing.

  Conditions: This symptom does not occur under specific conditions.

  Workaround: There is no workaround.

  More Info: The crash is seen because a structure that may not be available is accessed.

- CSCul81353

  Symptom: Cisco ASR 1006 with RP2 running ES version based of Cisco IOS Release 15.3(1)S crash with Segmentation Fault.

```
---snip-- UNIX-EXT-SIGNAL: Segmentation fault(11), Process = CCSIP_SPI_CONTROL
-Traceback= 1#9821b08208133f5124c039ddebb8173b :400000+347A664 :400000+7B14A0F
:400000+7B0F5E7 :400000+8F6C8A :400000+9A8C4C :400000+9B6951 :400000+95F2A4
:400000+962772 :400000+BE9018 :400000+BE8E4F ---snip--
```

  After the RP Switch over all the new calls were rejected with the following errors as well, which may be unrelated to the crash:

```
--snip-- Dec 2 15:11:47: %VOICE_IEC-3-GW: SIP: Internal Error (INVITE, codec
mismatch): IEC=1.1.278.7.110.0 on callID 17334189 Dec 2 15:11:49: %VOICE_IEC-3-GW:
SIP: Internal Error (INVITE, codec mismatch): IEC=1.1.278.7.110.0 on callID 17334212
Dec 2 15:11:49: %VOICE_IEC-3-GW: SIP: Internal Error (INVITE, codec mismatch):
IEC=1.1.278.7.110.0 on callID 17334218 ---snip---
```

Conditions: This symptom is observed after two weeks of uptime and during normal load condition.

Workaround: Workaround is to reboot the box to recover from the situation.

More Info: The core file writing is incomplete as TEMP_IN_PROGRESS

```
---- show stby-harddisk: all-----
142 2406627691 Dec 02 2013 14:11:14 +00:00
/harddisk/core/kernel.rp_20131202191114.core.gz
149 79237120 Dec 02 2013 14:03:52 +00:00
/harddisk/core/nyorbgdnesbc-dr_RP_0_linux_iosd-imag_6335.core.gz.TEMP_IN_PROGRESS
--------
```

- CSCul87037

  Symptom: An “sg subrte conte” chunk leak occurs while roaming.

  Conditions: This symptom occurs after an account-logoff and if service permit is configured in control policy. In case of a service permit, the subscriber remains unauth and is redirected to the portal once again. Post successful second account logon and the subscriber session is cleared by timeout or cli, the leak is seen and the same client will not be able to create the session once again. The leak is seen after simulating for the second time account-logon. And if service permit is configured.

  In case of service disconnect configured under account-logoff, account-logon is not a practical scenario as the portal is not reachable for the client.

  Workaround: Use **service disconnect** for **event account-logoff**.

  ```
  class type control always event account-logoff
     1 service disconnect delay 10
  !
  ```

- CSCul90667

  Symptom: Error messages and tracebacks are printed to the console.

  Conditions: This symptom occurs when IGP times out while Standby RP becomes NSR Active.

  Workaround: Enable NSR under IGP to ensure no timeout occurs.

- CSCul94087

  Symptom: Output Packet drops is observed on the ATM IMA interface even when there is no live traffic and only signalling exchange between non-Cisco devices. Although output drops in most cases means low bandwidth issues but in this case, an entire site was down due to these drops.

  Conditions: This symptom occurs under the following conditions:

  1. Layer 2 cross connect is configured on Cisco device and Non - Cisco device at other end
  2. Only signalling traffic flows through the devices
  3. IMA group is created for the ATM connectivity
  4. SPA-24CHT1-CE-ATM card is to be used for the ATM connection.

  Workaround: Reload the SPA.

- CSCul96421

  Symptom: Outbound calls over SIP trunk to provider fails.

Conditions: SIP IP phone (99xx) ------> CME ---------> SIP Trunk --------> ITSP

Cisco IOS Release 15.3(3)M and Cisco IOS Release15.4(1)T

Workaround: Downgrade Cisco IOS version to 15.2(4)M.

More Info: Outbound calls fail due to CME sending an INVITE with two authorization headers, one for SIP-UA credentials and other for digest user credentials of SIP phone:

```
Voice register pool 1 Type 9951 Id mac xxxx.xxxx.xxxx Username xxxx password xxxx
Number 1 dn 1
Sip-ua authentication username xxxxxx password 7 xxxxxxxxxx realm example.com
when the ITSP sends a 401 Unauthorized, we reply with 2 authentication headers.
```

- CSCum08918

Symptom: After an interface flap or device reload, a BFD neighbor fails to establish. Protocols registered to BFD like ISIS may also fail to establish.

Conditions: This symptom occurs with Cisco ME3600-cx platforms running ISIS with BFD. The issue can be seen with the **show platform ho-fpga tx-buffer-table detail** <*local discriminator (LD)*>command. With this command you can see the packet header of the BFD packet. The second line will show all 0s. The <*local discriminator (LD)*> value of the BFD session can be obtained from **show bfd neighbors** command output and

LD value should be between 1- 512 for the hardware offload BFD session.

```
me3600-cx# show bfd neighbors ipv4 10.1.1.1 details

IPv4 Sessions
NeighAddr                              LD/RD         RH/RS     State     Int
10.1.1.1                             258/0          Down      Down      Gi0/5   << LD
info >>
Session Host: Hardware
OurAddr: 10.1.1.2
Handle: 258
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 0, Received Multiplier: 0
Holddown (hits): 0(0), Hello (hits): 1000(0)
Rx Count: 0
Tx Count: 1660045
Elapsed time watermarks: 0 0 (last: 0)
Registered protocols: ISIS CEF
Last packet: Version: 1                  - Diagnostic: 0
             State bit: AdminDown        - Demand bit: 0
             Poll bit: 0                 - Final bit: 0
             C bit: 0
             Multiplier: 0               - Length: 0
             My Discr.: 0                - Your Discr.: 0
             Min tx interval: 0          - Min rx interval: 0
             Min Echo interval: 0


====================== me3600-cx#show platform ho-fpga tx-buffer-table detail 258 Tx
Buffer Table Entry: 258 --------------------------
Type: BFD_IPv4 Overload Ptr: 0x0000002A Length: 72 CFE Header: 0x004C Packet Header:
0x0000002A004C0000 0x0000000000000000 <<<<<<<<<<<<<<<<<<<<<<<< 0x0000080045C00034
0x00000000FF11A4F4 0x0A0101020A010101 0x0EC80EC800205FC9 0x2048031800000101
0x00000000000F4240 0x000F42400000C350 0x0000000000000000 0x0000000000000000
0x0000000000000000 0x0000000000000000 0x0000000000000000 0x0000000000000000
0x0000002A005BD0C2 ======================
```

Workaround: Flap the interface (shut/no shut) or remove and reapply BFD.

More Info: While running ISIS it is possible for BFD to attempt to register before IP ARP has completed (but the ISIS CLNS neighbor has been established). When this happens, BFD may send packets with source MAC and destination MAC addresses of all 0s. This causes the neighbor to ignore them and a BFD neighbor never establishes. This is a rare condition within the ISIS, ARP and BFD components and may not always be encountered.

- CSCum14438

  Symptom: "nh_l2m_handle_t" memory leaks are observed while configuring service instances on an access interface of the Cisco ME 3600 platform.

  Conditions: This symptom occurs when a new service instance is created on an access interface.

  Workaround: There is no workaround.

- CSCum14830

  Symptom: Leaking IPv6 routes is observed from a VRF table into the global table using BGP. These routes consist of the following:

  1. BGP routes learned from the VRF IPv6 BGP peer.
  2. Redistributed static and connected routes.

  The BGP routes leak fine, but the redistributed static and connected routes have an issue. After the redistributed routes leak, the exit interface shows "null0". Sometimes instead of showing the exit interface as "null0", it shows a random interface which is a part of VRF and has IPv6 enabled on it.

  Conditions: This symptom occurs with IPv6 redistributed connected and static routes into BGP VRF (could also be redistributed from other protocols as well but have not been tested).

  Workaround: There is no workaround.

- CSCum15232

  Symptom: A Cisco IOS router may crash using LDAP while performing TLS operations.

  Conditions: This symptom was observed in Cisco IOS Release 15.3(3)M1.4. Other versions can be affected as well.

  Workaround: There is no workaround.

  More Info: LDAP is used in IOS SSLVPN deployment to authenticate users.

- CSCum16315

  Symptom: Upon reload of a Cisco 7600 router configured with a CoPP policy containing IPv6 ACLs and DSCP matching, the CoPP is only applied to the active RSP as shown below.

  After reload:

```
lab-7609-rsp-02#sh mod power
Mod Card Type Admin Status Oper Status --- -------------------------------------
----------- ----------- 1 CEF720 48 port 10/100/1000mb Ethernet on on
5 Route Switch Processor 720 (Active) on on
6 Route Switch Processor 720 (Hot) on on
7 CEF720 8 port 10GE with DFC on on
8 CEF720 8 port 10GE with DFC on on
CoPP is applied to only the active RSP/SUP after reload:
lab-7609-rsp-02#sh policy-map control-plane in | inc class|Earl
class-map: COPPCLASS_MCAST (match-any)
Earl in slot 5 :
class-map: COPPCLASS_MGMT (match-any)
Earl in slot 5 :
class-map: COPPCLASS_ALLOW_ICMP (match-any)
Earl in slot 5 :
class-map: COPPCLASS_MONITORING (match-any)
```

```
Earl in slot 5 :
class-map: COPPCLASS_FILEXFER (match-any)
Earl in slot 5 :
class-map: COPPCLASS_REMOTEACCESS (match-any)
Earl in slot 5 :
class-map: COPPCLASS_OSPF (match-any)
class-map: COPPCLASS_LDP (match-any)
Earl in slot 5 :
class-map: COPPCLASS_BGP (match-any)
class-map: COPPCLASS_MISC (match-any)
class-map: COPPCLASS_UNDESIRABLE (match-any)
Earl in slot 5 :
class-map: COPPCLASS_IPV4_CATCHALL (match-any)
Earl in slot 5 :
class-map: COPPCLASS_IPV6_CATCHALL (match-any)
class-map: class-default (match-any)
Earl in slot 5 :
```

When this issue is triggered, the following error will be seen in the logs:

```
*Dec 14 02:33:14.579: %QM-2-TCAM_BAD_LOU: Bad TCAM LOU operation in ACL
```

This issue potentially exposes the device to a DoS vulnerability.

Conditions: This symptom occurs under the following conditions:

- 7600 HA Environment.
- CoPP IPV6 ACL with DSCP match.
- Reload or Switchover.

Workaround: There are two workarounds for this issue.

Modify the CoPP Policy to remove IPV6 ACL/DSCP matching.

Remove and reapply the CoPP configuration as shown below:

```
lab-7609-rsp-02(config)#control-plane
lab-7609-rsp-02(config-cp)#no service-policy in COPP
lab-7609-rsp-02(config-cp)#service-policy in COPP
lab-7609-rsp-02(config-cp)#end
```

CoPP is applied to all modulues as required:

```
lab-7609-rsp-02#sh policy-map control-plane in | inc class|Earl
class-map: COPPCLASS_MCAST (match-any)
Earl in slot 1 :
Earl in slot 5 :
Earl in slot 7 :
Earl in slot 8 :
class-map: COPPCLASS_MGMT (match-any)
Earl in slot 1 :
Earl in slot 5 :
Earl in slot 7 :
Earl in slot 8 :
class-map: COPPCLASS_ALLOW_ICMP (match-any)
Earl in slot 1 :
Earl in slot 5 :
Earl in slot 7 :
Earl in slot 8 :
class-map: COPPCLASS_MONITORING (match-any)
Earl in slot 1 :
Earl in slot 5 :
Earl in slot 7 :
Earl in slot 8 :
class-map: COPPCLASS_FILEXFER (match-any)
```

```
Earl in slot 1 :
Earl in slot 5 :
Earl in slot 7 :
Earl in slot 8 :
class-map: COPPCLASS_REMOTEACCESS (match-any)
Earl in slot 1 :
Earl in slot 5 :
Earl in slot 7 :
Earl in slot 8 :
class-map: COPPCLASS_OSPF (match-any)
Earl in slot 1 :
Earl in slot 5 :
Earl in slot 7 :
Earl in slot 8 :
class-map: COPPCLASS_LDP (match-any)
Earl in slot 1 :
Earl in slot 5 :
Earl in slot 7 :
Earl in slot 8 :
class-map: COPPCLASS_BGP (match-any)
Earl in slot 1 :
Earl in slot 5 :
Earl in slot 7 :
Earl in slot 8 :
class-map: COPPCLASS_MISC (match-any)
Earl in slot 1 :
Earl in slot 5 :
Earl in slot 7 :
Earl in slot 8 :
class-map: COPPCLASS_UNDESIRABLE (match-any)
Earl in slot 1 :
Earl in slot 5 :
Earl in slot 7 :
Earl in slot 8 :
class-map: COPPCLASS_IPV4_CATCHALL (match-any)
Earl in slot 1 :
Earl in slot 5 :
Earl in slot 7 :
Earl in slot 8 :
class-map: COPPCLASS_IPV6_CATCHALL (match-any)
Earl in slot 1 :
Earl in slot 5 :
Earl in slot 7 :
Earl in slot 8 :
class-map: class-default (match-any)
Earl in slot 1 :
Earl in slot 5 :
Earl in slot 7 :
Earl in slot 8 :
```

PSIRT Evaluation: The Cisco PSIRT has evaluated this issue and does not meet the criteria for PSIRT ownership or involvement. This issue will be addressed via normal resolution channels.

If you believe that there is new information that would cause a change in the severity of this issue, please contact psirt@cisco.com for another evaluation.

Additional information on Cisco's security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCum18012

  Symptom: System crashes on defaulting an interface with 64 EFPs.

Conditions: This symptom occurs under the following conditions:

1. Configure 64 EFPs on an interface in the same VLAN.
2. Default the interface.

The system will crash.

Workaround: There is no workaround.

More Info: This issue was fixed in Cisco IOS XE Release 3.10.3 and Cisco IOS Release 3.11.2.

- CSCum24565

  Symptom: - MPLS is being processed by the CPU instead of HW switching. - **rem com sw show mls vlan-ram** shows "0" value under vpn-num and netdr shows that mpls is being processed by the CPU:

  ```
  Example: 7600# rem comm sw sh mls vlan-ram 1906 1906
  TYCHO Vlan RAM Key: * => Set, - => Clear
  vlan eom nf-vpn mpls mc-base siteid stats rpf vpn-num bgp-grp l2-metro rpf-pbr-ovr
  ----+---+------+----+-------+------+-----+---+-------+-------+--------+-----------
  1906 * - * 0 0 - - 0 0 - * <<<=== vpn-num 0
  ```

  There is a possibility of a high CPU due to interrupts.

  Conditions: The symptom may occur on the Cisco 7600 Series Routers after an SSO is performed on PE with L2VPN in PFC VLAN mode.

  Workaround:

  1. Remove xconnect configuration from the subinterface and reconfigure it.
  2. Shut/no shut the xconnect source interface.

- CSCum29064

  Symptom: Syncing dual-stack iWAG session to STANDBY does not occur.

  Conditions: This symptom occurs when IPv4 and IPv6 FSOL is received from same client at ISG together (or very less time gap) for a dual-stack session. In this case, the session does not sync to STANDBY for the previous IPv6 FSOL and ISG gets a new IPv4 FSOL.

  Workaround: There is no workaround.

- CSCum40043

  Symptom: Crypto sessions get stuck in UP-IDLE state in scale scenario on a Cisco CSR platform.

  Conditions: This symptom occurs on a Cisco CSR platform in Cisco IOS XE Release 3.11.

  Workaround: Bring the sessions up in very small increments, for example, 40 sessions at a time initially and keep monitoring. When the sessions stop coming up for 40 sessions at a time, switch to a smaller number like 20.

- CSCum40306

  Symptom: Router crashes during call transfer in SRST mode.

  Conditions: This symptom is observed during call transfer in SRST mode, including SCCP phones.

  Workaround: There is no workaround.

- CSCum48166

  Symptom:

```
000175: Oct 30 11:05:09.413 KSA: ASSERTION FAILED : ../voip/ccvtsp/vtsp.c:
vtsp_cdb_assert: 1518: unkn -Traceback= 000176: Oct 30 11:05:09.481 KSA: ASSERTION
FAILED : ../voip/ccvtsp/vtsp.c: vtsp_cdb_assert: 1518: unkn -Traceback= 000177: Oct 30
11:05:09.485 KSA: %SYS-3-MGDTIMER: Uninitialized timer, timer stop, timer = 49595828.
-Process= "DSMP", ipl= 0, pid= 304, -Traceback=
11:05:09 KSA Wed Oct 30 2013: TLB (load or instruction fetch) exception, CPU signal
10, PC = 0x4110CA2C
```

Conditions: Cisco IOS VoIP gateway experiences an unexpected reload while processing voice calls. This happens when the caller Id is enabled on the FXO port with the voice-port subcommand **caller-id alerting dsp-pre-allocate** enabled.

Workaround:

1. Disable the **caller-id alerting dsp-pre-allocate** command. This will, however, not support caller Id on Old FXO cards where the Caller Id Type is set to Type I (i.e. caller Id reception before connect).
2. Disable the **caller-id enable** command. This again will not provide the Caller Id feature, but prevent the router from unexpected reloads.

- CSCum52216

  Symptom: After a reload, **ip pim sparse-mode** is gone on interface lisp 0.x (x denoted the LSIP interface number).

  Conditions: This symptom occurs after a reload.

  Workaround: There is no workaround.

- CSCum55357

  Symptom: CUBE crashes for SIP-H323 Transcoding call.

  Conditions: The issue is seen while running regression for Cisco IOS Release 15.3(3)M1.9.

  Workaround: There is no workaround.

- CSCum60848

  Symptom: Under certain conditions, a DSP will hang in certain call scenarios including REFER passthrough.

  Conditions: This symptom is observed under heavy load.

  Workaround: There is no workaround.

- CSCum61595

  Symptom: Alignment errors are observed after upgrading to Cisco IOS Release 15.2(4)M5.

  ```
  Jan 9 19:42:59.623 GMT: %ALIGN-3-CORRECT: Alignment correction made at 0x6477F81Cz
  reading 0x6BE87495 Jan 9 19:42:59.623 GMT: %ALIGN-3-TRACE: -Traceback= 0x6477F81Cz
  0x647805D0z 0x6478FE70z 0x64751088z 0x64B99F4Cz 0x64B99FD4z 0x64752 284z 0x647525ACz
  ```

  Conditions: This symptom does not occur under specific conditions.

  Workaround: There is no workaround.

- CSCum62783

  Symptom: The following alignment errors are seen after a PPPoE session establishment for the first time after a reboot:

  ```
  *Jan 14 07:24:40.591: %ALIGN-3-CORRECT: Alignment correction made at 0x32B2DFF4z
  reading 0xE7790ED *Jan 14 07:24:40.591: %ALIGN-3-TRACE: -Traceback= 0x32B2DFF4z
  0x32B1E274z 0x32B1EECCz 0x32B1EF90z 0x332E550Cz 0x332E54F0z 0xFFFF1A00z 0xFFFF1A00z
  ```

Conditions: This symptom occurs when **pppoe-client ppp-max-payload** is configured under the Ethernet interface.

Workaround: There is no workaround.

- CSCum65451

  Symptom: A crash occurs due to multicast stack overflow memory corruption.

  Conditions: This symptom may occur when PIM is enabled on a LISP interface and Auto-RP is also enabled.

  Workaround: Configure **no ip pim autorp** before any other PIM or LISP configuration.

- CSCum67229

  Symptom: Entitymib does not respond for OC3/OC12/T3/E3 controller ports on the Cisco ME3600x-24CX-M platform.

  Conditions: This symptom occurs with the Cisco ME 3600X-24CX-M platform running Cisco IOS XE Release 3.10.

  Workaround: There is no workaround.

- CSCum70579

  Symptom: CISCO-EVC-MIB is not available with MetroIPAccess license on Cisco ME 3600X platforms.

  Conditions: This symptom is observed only with MetroIPAccess license.

  Workaround: Upgrade the license to AdvancedMetroIP license.

- CSCum71701

  Symptom: This bug can stop traffic from being forwarded by an upstream router when the **ip pim join-prune-interval** command is configured on the downstream router's upstream LISP interface.

  Conditions: This symptom occurs when the **ip pim join-prune-interval** command is configured with a value greater than the default on a LISP interface.

  Workaround: There is no workaround.

- CSCum78613

  Symptom: A crash is observed with QoS Egress classification policies in trunk mode configuration.

  Conditions: This symptom occurs with a random sequence of steps involving changing of interface configurations by attaching the policy beforehand.

  Workaround: Reload with the final configurations needed.

- CSCum81041

  Symptom: One way audio incoming calls redirected through CVP.

  ```
  Conditions: Call flow: ------------
  Caller----G711----TDM GW----SIP-----ASR1K----SIP-----CUSP----SIP----CVP(Vz0)----IP-IVR
  | | -----SIP---CVP (BAMS) | |--------SIP---CUCM---Agent Phone (G729 only)
  ```

  Initially the caller is connected to IP-IVR, both ingress and egress leg of the CUBE is doing G711. Call is connected to the IP-IVR, then CVP sends a refer to the VXML GW for playing prompts and ringback tone etc. When the call is transferred to the agent, CUBE negotiated G729 at the sip level with the CVP, but because of mid-call signalling block on the ingress side, continue with the G711. Hence xcoder is invoked on the CUBE to handle G729 to G711 and vise versa, but CUBE is still sending G711 media to the agent phone side while the agent phone is sending G729 media to the CUBE.

Workaround: There is no workaround.

- CSCum83829

  Symptom: Cisco ME 3600 and ME 3800 platforms crash when shut and no shut is performed on an interface.

  Conditions: This symptom occurs prior to shut and no shut when the VLAN of the that particular port is removed and added back. The VLAN must have static configurations like static join or static mrouter.

  Workaround: There is no workaround.

- CSCum84999

  Symptom: SUBSCRIBE received from CVP after BYE and NOTIFY with subscription-state: terminates is send by CUBE.

  Conditions: This symptom is observed when SUBSCRIBE IS recieved after call is terminated with BYE.

  Workaround: There is no workaround.

- CSCum85813

  Symptom: Shut primary static router and secondary static is not installed automatically.

  Conditions: This symptom is seen on the sites where the BFD state of the backup static route is marked as “U” in the output of **show ip static route bfd**.

  Workaround: Reinstall the default backup static route.

- CSCum95330

  Symptom: Removing an Ethernet service instance which is a member of a bridge domain may cause the router to reload.

  Conditions: This symptom is observed when the last service instance is removed from the bridge domain and there are still members of the bridge domain which are not service instances (such as VFIs).

  Workaround: Completely unconfigure the bridge domain and reconfigure it.

- CSCun07772

  Symptom: A Cisco router crashes.

  Conditions: This symptom occurs on deleting a subcriber’s session in attempting state by a COA script as shown below:

```
#!/bin/sh CISCO=$1 # bras SessionID=$2 CoaSecret='secret'
#clear ISG session on BRAS /bin/echo
"User-Name="undef",Acct-Session-Id="$SessionID",cisco-avpair="subscriber:command=accou
nt-logoff"" | /usr/bin/radclient -x $CISCO:1700 coa $CoaSecret
```

  Workaround: Do not use the COA script for deleting the subscriber’s session.

- CSCun10381

  Symptom: A traffic drop was observed because labels do not get programmed.

  Conditions: This symptom occurs when scalable EoMPLS with L3VPN is configured. When notifications on atom-imps arrive, they have to get programmed.

  Workaround: Clear ip route.

  More Info: Traffic was seen to be dropped as the atom-imps could not be programmed because label entry could not be found for the atom-imps.

- CSCun11782

  Symptom: Rtfilter prefixes are sent with incorrect next-hop equal to next-hop of the default static route in GRT instead of BGP router-id.

  Conditions: This symptom occurs with a default static route present in GRT pointing, for example, to the next-hop known behind the connected interface.

  Workaround: Replace the default static route with a more specific static route or remove static and clear BGP.

- CSCun13688

  Symptom: The Cisco Catalyst 6500 Supervisor Engine 2T with CLNS routing configured crashes after **show clnbs route**.

  Conditions: This symptom occurs when CLNS routing is configured.

  Workaround: There is no workaround.

- CSCun18738

  Symptom: A “aspdma_rx_n_pkt_handler” memory leak is observed in Cisco ME 3600 and ME 3800 platforms.

  Conditions: This symptom occurs randomly with the Cisco Discovery Protocol configured in the device.

  Workaround: There is no workaround.

- CSCun20187

  Symptom: HSRP communication fails between two PEs (Cisco 7600 Series router) right after removing a neighbor from VFI.

  Conditions: Assume that a VPLS circuit is running between more than two PEs say A,B, and C and HSRP is running between A and B. Removing VPLS peer C on either A or B would cause HSRP communication failure between A and B. This failure is not expected as data path is still available between A and B.

  Workaround: Perform shut/no shut on the SVI.

- CSCun21602

  Symptom: Traffic is not forwarded by the router out of any interface.

  Conditions: This symptom occurs on toggling of the **ip routing** command in global configuration mode.

  Workaround: Perform shut and no shut of the interface which is involved in forwarding or reload the device with **ip routing** enabled.

- CSCun25316

  Symptom: Cisco ME 3600 packets in routing protocol queue results in an ISIS Flap.

  Conditions: This symptom occurs when more than 1000 packets get punted to the routing protocol queue.

  Workaround: Increase the queue size.

  platform qos policer cpu queue <qid><rate>

- CSCun30040

  Symptom: AN neighbor ship goes down after enabling SD.

  Conditions: This symptom occurs when IPv6 packets get dropped because interface input queue is full after enabling mDNS.

Workaround: There is no workaround.

- CSCun31021

  Symptom: A vulnerability in IKE module of Cisco IOS and Cisco IOS XE could allow an unauthenticated, remote attacker to affect already established Security Associations (SA)..

  The vulnerability is due to a wrong handling of rogue IKE Main Mode packets. An attacker could exploit this vulnerability by sending a crafted Main Mode packet to an affected device. An exploit could allow the attacker to cause dropping of valid, established IKE Security Associations on an affected device.

  Conditions: Device configured to process IKE request that already has a number of established security associations.

  Workaround: There is no workaround.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4.3/3.6: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:N/A:P/E:F/RL:OF/RC:C

  CVE ID CVE-2014-2143 has been assigned to document this issue.

  Additional details about the vulnerability described here can be found at: http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-2143

  Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCun41292

  Symptom: On a Cisco ASR 1001 router running Cisco IOS Release 15.3(1)S, a crash occurs when the "show ip ei vrf X topo X.X.X.X/X" command is executed. The X.X.X.X/X must be in "FD is infinity" status in EIGRP as CSCtz01338.

  ```
  asr1001_bew_03# show ip ei vrf * to all | i Infinity P 174.162.XX.XX/24, 0 successors,
  FD is Infinity, U, serno 37, refcount 1 snip P 174.180.XX.XX/29, 0 successors, FD is
  Infinity, U, serno 46, refcount 1 asr1001_bew_03# asr1001_bew_03# asr1001_bew_03#
  asr1001_bew_03# asr1001_bew_03# asr1001_bew_03#show ip ei vrf 1 to 174.162.XX.XX/24
  Exception to IOS Thread: Frame pointer 0x7F63DF6602D0, PC = 0x1956C8D
  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = Exec -Traceback=
  1#980611ad3b9665cd80fe5178bcd6036a :400000+1556C8D :400000+1556B09 :400000+15569D1
  :400000+157DE39 :400000+15197A2 :400000+1518659 :400000+156BA5E :400000+15591D1
  :400000+1189768 :400000+1188E6D :400000+1186E15 :400000+484F270 :400000+11A1CA0
  Fastpath Thread backtrace: -Traceback= 1#980611ad3b9665cd80fe5178bcd6036a
  c:7F64154A4000+BE002
  Auxiliary Thread backtrace: -Traceback= 1#980611ad3b9665cd80fe5178bcd6036a
  pthread:7F640ED43000+A7C9
  ```

  Conditions: This symptom occurs when X.X.X.X/X is in "FD is infinity" status in EIGRP.

  Workaround: There is no workaround.

- CSCun45272

  Symptom:

  1. Standby RP will have out-of-sync entries. With MPLS-TE NSR enabled, the standby RP will have out-of-sync entries which will result in flapping of the path-protected LSP of the tunnel after an SSO.
  2. Leaking an LSP. A third LSP will be signaled and leaked (there is no management of the LSP). There are supposed to be two LSPs at steady state (primary and path protected), but with this defect, there will be primary, path protected, and leaked LSP.

Conditions: This symptom occurs with a reoptimization of a tunnel that has failed with path protection enabled.

Workaround: There is no workaround.

- CSCun45299

  Symptom: IPv6 traffic is dropped for packets with extension headers.

  Conditions: This symptom occurs when extension header packets are punted to the CPU.

  Workaround: There is no workaround.

- CSCun46486

  Symptom: A Cisco device crashes every 2-3 days when the SNMPSET operation is used to create guest users.

  Conditions: This symptom occurs when guest users are created through SNMPSET operations at a very high rate.

  Workaround: There is no workaround.

- CSCun48344

  Symptom: A config-sync failure occurs due to the **address-family ipv6 unicast vrf** command during the immediate unconfiguration and reconfiguration of VRF definition.

  Conditions: This symptom occurs with attached running configurations.

  Workaround: There is no workaround.

- CSCun58030

  Symptom: A Cisco ME-3600X platform does not display time source information while running the PTP dataset time properties show command. Functional issues are not noticed with PTP time sync. The time source field says “Unknown”.

  Conditions: This symptom does not occur under specific conditions. A simple Ordinary Clock(OC) Slave- Master connectivity would make the Slave show up as “Time Source Unknown”.

  Workaround: There is no workaround.

- CSCun65000

  Symptom: Traffic loss of about 200-500 ms is observed.

  Conditions: This symptom is observed on an RLFA cutover.

  Workaround: There is no workaround.

- CSCun68723

  Symptom: Incorrect information is present on the E1/T1 ports on the Cisco ME 3600X 24CX platform in the IfTable of IF-MIB.

  The incorrect information includes the following:

  1. ifType of the interface is 0 which is not a valid ifType.
  2. ifAdminStatus value is always testing, and does not reflect the actual state.
  3. ifOperStatus value is always unknown and does not reflect the actual state.
  4. ifSpeed value is 0 which is incorrect.

  Conditions: This symptom occurs on any Cisco ME 3600X 24CX device running Cisco IOS Release 15.3(3)S.

  Workaround: The correct information on the E1/T1 ports is available in CLI.

- CSCun72459

  Symptom: High traffic loss is observed with setups having BGP and microloop avoidance combination.

  Conditions: This symptom occurs with the following combination:

  1. IP FRR is turned on.
  2. Cisco IOS XE Release 3.11 code (or newer) that enables microloop avoidance by default.
  3. BGP configurations.

  Workaround: Disable the microloop avoidance feature. For example, in ISIS, execute the following commands:

  ```
  router isis <process name>
  microloop avoidance disable
  !
  ```

  However, there will be some traffic loss due to the lack of microloop avoidance.

- CSCun73463

  Symptom: A Cisco ME 3600 device crashes.

  Conditions: This symptom occurs on configuring a card type t1/e1 without a t1/e1 license on the device.

  Workaround: Configure the card type after obtaining a t1/e1 license.

- CSCun73515

  Symptom: A router crashes due to RMON.

  Conditions: This symptom occurs on activation of an RMON event.

  Workaround: There is no workaround.

- CSCun73782

  Symptom: A vulnerability in LISP control messages processing on Cisco IOS and Cisco IOS XE could allow an unauthenticated, remote attacker to cause a vulnerable device to disable CEF forwarding and eventually drop traffic passing through.

  The vulnerability is due to insufficient checking of certain parameters in LISP control messages on ITR. An attacker could exploit this vulnerability by sending malformed LISP control messages to ITR. An exploit could allow the attacker to cause a vulnerable device to disable CEF forwarding and eventually drop traffic passing through.

  Conditions: Malformed messages can only be generated by a device that is already registered to a LISP system: a valid ETR or ALT.

  Workaround: There is no workaround.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4.3/3.6: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:N/A:P/E:F/RL:OF/RC:C

  CVE ID CVE-2014-3262 has been assigned to document this issue.

  Additional details about the vulnerability described here can be found at: http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-3262

  Additional information on Cisco’s security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCun76733

  Symptom: BFD goes down and remains in admindown state.

  Conditions: This symptom occurs after applying ACL chaining and flapping of the interface.

  Workaround: There is no workaround.

  More Info: An IPv4 BFD neighbor remains in admindown state on the PE. The ACE configured in ACL for BFD is matched and the receive counters on BFD neighbors are incremented but the BFD is still down.

  This issue occurs only after ACL chaining is applied.

- CSCun77010

  Symptom: A router may crash after or during the execution of the **show ipv6 ospf rib** command.

  Conditions: This symptom occurs when many routes or route paths are present in the OSPFv3 rib. The OSPFv3 rib is significantly recomputed during execution of commands.

  Workaround: Limit the use of the **show ipv6 ospf rib** command.

- CSCun85501

  Symptom: IPv6 traffic is not forwarded by the device for templates other than the default (like VPNv4-only, VPNv4-v6). However, IPv4 traffic works fine.

  Conditions: This symptom occurs when the template is changed to anything other than the default.

  Workaround: There is no workaround.

- CSCun86087

  Symptom: In a VPLS environment, packets of some VCs are blocked in an imposition direction.

  Conditions: This symptom occurs with port channels and LAG as MPLS core-facing interface on ES+.

  Workaround: There is no workaround.

- CSCun91720

  Symptom: IPv6 mcast traffic is punted to the host queue (inl3idc_vlan.bridgeBasedMcastIp=1).

  Conditions: This symptom occurs on a Layer 2 device with no multicast configurations.

  Workaround: There is no workaround.

  More Info: Instead of bridging the IPv6 traffic, the switch punts it to the CPU.

- CSCuo08759

  Symptom: With IP-FRR, VPLS traffic is dropped on a core-facing port-channel after a link flap.

  Conditions: This symptom occurs when a core-facing interface is a portchannel configured on a Cisco 7600 ES+ card.

  Workaround: Perform shut and no shut on the port channel interface.

- CSCuo11703

  Symptom: The **show network-clock synchronization** command flaps between different QL values on the same interface. Depending on the values with which the interface flaps, this could lead to triggering of network-clock selection algorithm and subsequent selection of primary reference clock for the system.

  Conditions: This symptom could occur when the network-clock synchronization mode is unprovisioned from automatic selection, and then the monitor interfaces are removed and a new set of interfaces are added for network-clock monitoring with automatic selection reprovisioned.

Workaround: Adding back the older set of interfaces and removing them would resolve the issue.

- CSCuo16717

  Symptom: PPPoX brings up sessions failure with IPv6 configurations.

  Conditions: This symptom occurs when “vpdn authen-before-forward” is configured.

  Workaround: Do not configure “vpdn authen-before-forward”.

- CSCuo19730

  Symptom: Cisco IOS XE includes a version of OpenSSL that is affected by the vulnerability identified by the Common Vulnerability and Exposures (CVE) ID CVE-2014-0160.

  This bug has been opened to address the potential impact on this product.

  Conditions: Cisco IOS XE devices running release 3.11.0S, 3.11.1S or 3.12.0S and with the WebUI interface over HTTPs enabled. No other versions of Cisco IOS XE are affected.

  Devices with the WebUI interface enabled and using HTTPs as transport protocol will include the following configuration:

  transport-map type persistent webui http-webui secure-server ip http secure-server transport type persistent webui input http-webui

  Devices running IOS XE release 3.11.0S, 3.11.1S or 3.12.0S but WITHOUT the WebUI interface enabled, or with the WebUI interface enabled but NOT using HTTPs as transport protocol are NOT AFFECTED by this vulnerability.

  Devices running IOS XE release 3.11.0S, 3.11.1S or 3.12.0S and with the HTTPs server enabled (by including in their configuration the line “ip http secure-server”) are NOT affected. Both the HTTPs server and the WebUI interface need to be enabled for a device to be vulnerable.

  The WebUI configuration guide is available at http://www.cisco.com/c/en/us/td/docs/routers/asr1000/configuration/guide/chassis/asrswcfg/webui.html

  Workaround: There is no workaround.

  Further Problem Description: Additional details about this vulnerability can be found at http://cve.mitre.org/cve/cve.html

  Software version and Fixes

  The first column is the Cisco IOS XE Software Release The second column is the First Fixed Release.

  2.x.x Not Vulnerable 3.1.xS Not Vulnerable 3.1.xSG Not Vulnerable 3.2.xS Not Vulnerable 3.2xSE Not Vulnerable 3.2.xSG Not Vulnerable 3.2.xXO Not Vulnerable 3.2.xSQ Not Vulnerable 3.3.xS Not Vulnerable 3.3.xSE Not Vulnerable 3.3xSG Not Vulnerable 3.3xXO Not Vulnerable 3.3xSQ Not Vulnerable 3.4.xS Not Vulnerable 3.4.xSG Not Vulnerable 3.5.xS Not Vulnerable 3.5.xE Not Vulnerable 3.6.xS Not Vulnerable 3.6.xE Not Vulnerable 3.7.xS Not Vulnerable 3.8.xS Not Vulnerable 3.9.xS Not Vulnerable 3.10.xS Not Vulnerable 3.11.xS Vulnerable 3.12.xS Vulnerable 3.12.0aS Not Vulnerable

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4.3/4.3:

  https://intellishield.cisco.com/security/alertmanager/cvss?target=new&version=2.0&vector=AV:N/AC:M/Au:N/C:P/I:N/A:N/E:H/RL:U/RC:C

  The Cisco PSIRT has assigned this score based on information obtained from multiple sources. This includes the CVSS score assigned by the third-party vendor when available. The CVSS score assigned may not reflect the actual impact on the Cisco Product.

CVE-2014-0160 has been assigned to document this issue.

Additional information on Cisco's security vulnerability policy can be found at the following URL:

http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

- CSCuo22184

  Symptom: The VPLS bit is not set in the flood VLAN LTL index which causes a traffic drop.

  Conditions: This symptom occurs under the following conditions:

  – Have a port-channel with member links on different NP (say NP2 and NP1) and a physical interface on the same LC and NP (say NP2) to different neighbors, say PE1 and PE2 respectively.

  – Shut down the member link of NP1.

  – Remote shut the VLAN or access interface on PE2 (reached by physical interface).

  – The V-bit is not set and this affects the traffic towards PE1 (reached by port-channel interface).

  Workaround:

  – Either no-shut the remote VLAN or AC on PE2.

  – Perform shut and no-shut the port-channel.

- CSCuo35867

  Symptom:

  1. CPOS-based PPP serial interface is UP/DOWN; but HDLC is UP/UP; loopback local for PPP is also UP/DOWN.
  2. From debug, the following output is seen:

```
*Apr 16 20:46:50.330: AAA/ID(00100066): PPP allocated .... *Apr 16 20:46:50.831: CCM:
Failed to create session, session already exists <<<<<<<<<<<< *Apr 16 20:46:50.831:
AAA/ID(NA): PPP allocating *Apr 16 20:46:50.831: CCM GROUP:ERROR group not found with
shdb 0 *Apr 16 20:46:50.831: AAA/ID(NA): propagate hw:Se1/0/0.1/1/6/1:0,0x42352E64
sw:Se1/0/0.1/1/6/1:0,0x42353C48 other:nil base:nil unit:0/1 slot:1 shelf:0 tty:nil
*Apr 16 20:46:50.831: aaa_uid_propogate grabbed_id = 1048678 *Apr 16 20:46:50.831:
AAA/ID(00100066): PPP allocated *Apr 16 20:46:52.847: Se1/0/0.1/1/6/1:0 PPP: Missed a
Link-Up transition, starting PPP <<<<<<<<<<<<<
```

  Conditions: This symptom occurs with PPP serial interface flapping.

  Workaround: Chassis reload can temporarily make PPP interface UP/UP, but the problem will reoccur after a few days.

- CSCuo47685

  Symptom: While evaluating the Cisco IOS Release 15.3(3)S3 early release image, the following error message was observed when using the CoPP configuration given below which matches based on precedence only as shown:

```
class-map match-any coppclass-protocol match precedence 6 7
```

  "Match precedence in IPv4/IPv6 packets is not supported for this interface error: failed to install policy map CoPP"

  Upon occurrence, the entire CoPP policy map is not loaded. There is a concern that some field devices on the current release (Cisco IOS Release 15.0(1)S6) may have the above configuration and as such is prone to this error (CoPP installation failure during upgrade).

  Conditions: This symptom occurs while evaluating the Cisco IOS Release 15.3(3)S3 early release image.

Workaround: There is no workaround.

Resolved Bugs—Cisco IOS Release 15.4(1)S1

- CSCte77398

  Symptom: A Cisco ATM router configured with ATM PVC Range commands report the following error when attempting to configure a PVC Range:

  ```
  Unable to configure PVC Range. Possibly multiple users configuring IOS simultaneously.
  ```

  Conditions: This problem occurs randomly and even if there are no multiple sessions accessing the pvc-range at the same time.

  Workaround: There is no workaround.

- CSCtz73473

  Symptom: In a rare multipath import configuration on IOS router, the following traceback is seen:

  ```
  SW0: *May 4 12:08:40.175 PDT: %IPRT-3-INVALID_NEXTHOP: Duplicate ID 0x3 113.1.1.0/24
  from bgp decode: 0x6770760 ---> ip_route_update+37C 0x59F7B20 --->
  bgp_ipv4_rib_install+578 0x59F87C8 ---> bgp_ipv4_rib_update+108 0x5A8C524 --->
  bgp_vpnv4_update_iprib+2C 0x59F8C24 ---> bgp_v4class_update_fwdtable_walker+60 ...
  ```

  Though there is no operational impact, it disturbs the console with the above traceback.

  Conditions: This symptom is observed when you configure the following in the VRF address family:

  ```
  router bgp 200000
  !
  address-family ipv4 vrf 5
  import path selection multipaths
  maximum-paths eibgp 8
  ```

  Workaround: Do not log output on console but make it buffered to keep console clean.

- CSCuc53853

  Symptom: A vulnerability exists in Cisco IOS switches where the remote, non-authenticated attacker can cause Denial of Service (DoS) by reloading an affected device. An attacker can exploit this vulnerability by sending a special combination of crafted packets.

  Conditions: This symptom occurs when the HTTP server is enabled on the affected device.

  Workaround: There is no workaround.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5.4/4.2:

  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:H/Au:N/C:N/I:N/A:C/E:POC/RL:OF/RC:C

  CVE ID CVE-2013-1100 has been assigned to document this issue.

  Additional details about the vulnerability described here can be found at: http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2013-1100

  Additional information on Cisco’s security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCue68714

  Symptom: Newer released IOS-XE BGP, post Cisco IOS Release 15.2(4)S/XE3.7 not forming BFD session with the older implementations. This happens when using eBGP multi-hop to peer between two loopback interfaces on directly connected routers.

  Conditions: This ddts adds a couple of options "[single-hop | multi-hop]" to the existing BGP-BFD knob "neighbor x.x.x.x fall-over [bfd] [check-control-plane-failure]".

  So, after the change the knob would be: "neighbor x.x.x.x fall-over [bfd] [single-hop | multi-hop] [check-control-plane-failure]"

  **Note: Existing: "neighbor x.x.x.x fall-over [bfd]" --- This behavior would not be disturbed; so that we do not change the behavior that has been released as part of all the releases for more than three years now.

  Add-on in this ddts:

  1) "neighbor x.x.x.x fall-over [bfd] [single-hop] -- NEW-option "single-hop"; would force BGP to open a single-hop bfd session. Even in case of back-to-back ebgp update-source loopback with 2 hop BGP peering.

  2) "neighbor x.x.x.x fall-over [bfd] [multi-hop] -- NEW-option "multi-hop"; would force BGP to open a multi-hop bfd session.

  Workaround: There is no work around. ISR G2 should support BFD multi-hop feature.

  More Info: ISR-G2 does not support multi-hop BFD, while ISR4400 supports multi-hop BFD. BFD multi-hop support for ISR-G2 needs to be provided, so that they can interop with ISR4400 and ASRs.

- CSCuh15049

  Symptom: EIGRP internal error log message appears along with tracebacks when EIGRP neighbors go down. The device might crash during the peer cleanup.

  Conditions: This symptom is not observed under any specific conditions.

  Workaround: There is no workaround.

- CSCuh69292

  Symptom: LDAP moves in the stuck state.

  Conditions: This issue is seen if the LDAP server becomes unavailable during LDAP transactions.

  Workaround: There is no workaround.

- CSCui17084

  Symptom: Delay between VPN convergence and BGP-based MDT tunnel creation after router reload may cause multicast traffic loss.

  Conditions: In a BGP MVPN setup utilizing MDT SAFI, problem is seen upon BGP exiting read-only mode. VPN prefixes will be advertised immediately, whereas MDT prefixes are advertised after a BGP scanner run.

  Workaround: There is no workaround.

- CSCui51363

  Symptom: The multilink does not pass traffic even though it is in an up/up state.

  Conditions: This symptom occurs when the auto DNR status is set and the sip400 ucode crashes.

  Workaround: Perform a shut/no shut in the multilink.

- CSCui53428

  Symptom: Forwarding state is not preserved on the Cisco ASR 9000 series router after an SSO in the Cisco ASR 903 router.

  Conditions: This symptom occurs when an SSO is performed on the Cisco ASR 903 router.

  Workaround: There is no workaround.

- CSCui59185

  Symptom: ASR901 crashes while booting up with memory lite disabled.

  Conditions: This symptom is observed when RFLA is enabled with memory lite disabled.

  Workaround: Enable memory lite.

- CSCui63462

  Symptom: High CPU usage is observed in an mDNS process with redistribution enabled.

  Conditions: This symptom occurs when redistribution is enabled in a loop scenario.

  Workaround: Enable redistribution accurately. This CLI should not be enabled when the setup contains loops.

- CSCui82519

  Symptom: The receiver has a remote alarm after configuring “framing no-crc4” on the controller.

  Conditions: This symptom occurs after configuring “framing no-crc4” on the controller.

  Workaround: There is no workaround.

- CSCui82817

  Symptom: A tunnel with lower absolute metric is not advertised properly.

  Conditions: This symptom occurs under the following conditions:

  1. When there are multiple tunnels to a destination.
  2. The tunnel with a better metric comes up.
  3. When ISIS is used as IGP and both L1 and L2 are present and configured for TE.

  Workaround: Clear the ISIS sessions.

- CSCuj11232

  Symptom: Changing the local label on an existing static (no signaling) Any Transport over MPLS (AToM) pseudowire, or changing the static pseudowire to a dynamic one (with LDP signaling) may cause traffic to fail to traverse the pseudowire.

  Conditions: This symptom is observed when either the configured value of the static local label is changed, or if the pseudowire is changed to a dynamic one.

  Workaround: Completely unconfigure the existing xconnect or pseudowire before entering the new configuration.

- CSCuj30572

  Symptom: With EIGRP and PFR configured, a router crashes after giving the following EIGRP messages.

  ```
  000111: Sep 17 09:08:33.331: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.50.2.1
  (Tunnel502) is down: Peer Termination received 000112: Sep 17 09:08:33.347:
  %DUAL-3-INTERNAL: EIGRP-IPv4 1: Internal Error -Traceback= 319D4CB4z 319EC5E4z
  319EC7C8z 319E4950z 319EA760z 31A25008z 32C23084z 32C23068z
  ```

  Conditions: This symptom occurs when PFR, OER and EIGRP are configured.

Say RouterUnderTest has two EIGRP Peers HUB1 and HUB2. (Given metrics are only for illustration) When EIGRP has a Prefix with 3 different Paths installed in following Order DRDB1 NH - HUB1, Metric 36571392 / 0 (Installed by PFR) DRDB2 NH - HUB2, Metric 58322432 / 409600 (x Hops away learnt from RouterX) DRDB3 NH - HUB1, Metric 538004992/500409600 (y Hops away learnt from Router Y)

With these initial conditions, if Neighbor ship with Router Y goes down, Both PFR and EIGRP try to delete DRDB3 Which results in inconsistent data structures with Memory corruption. Any further access to memory will result in crash.

Workaround: Use other load sharing methods instead of PFR.

More Info: The crash is usually seen during execution of an EIGRP Route lookup function similar to the following:

```
0x33841E10:eigrp_pfr_get_drdb(0x33841ddc)+0x34
0x33842014:eigrp_pfr_route_lookup(0x33841e88)+0x18c
```

- CSCuj39400

  Symptom: A Cisco 3945 series router running Cisco IOS Release 15.2(2)T2 may crash with a bus error. This relates to VOIP_RTCP.

  Conditions: Initial assessment shows that this appears to happen most often while running sip debugs. However at least one identical crash happened after SIP debugs were disabled three days before.

  Workaround: There is no known workaround.

- CSCuj41494

  Symptom: Memory leak is observed when the Cloud Web Security (formerly know as Scansafe) functionality is used on IOS versions containing the fix for CSCuh33843. Versions prior to 15.3(3)M are unaffected since they did not get the fix for CSCuh33843.

  Conditions: This symptom occurs when Scansafe traffic is handled by TCP.

  Workaround: Disable Scansafe.

- CSCuj42031

  Symptom: Router may crash due to bus error - voip_rtp_dispose_media_service_pak

  This new bug is similar to CSCtx54882 and is impacting the IOS image : c3900-universalk9_npe-mz .SPA.152-4.M2.bin.

  Conditions: This symptom has been observed on a Cisco router running Cisco IOS Release 152-4.M2.

  Workaround: There is no workaround.

- CSCuj44818

  Symptom: A warning message is displayed.

  Conditions: This issue occurs while unconfiguring video monitoring.

  Workaround: There is no workaround.

- CSCuj50396

  Symptom: The flow exporter status becomes inactive.

  Conditions: This symptom occurs after an RP switchover while checking flow monitor information.

  Workaround: There is no workaround.

- CSCuj52396

  Symptom: In a VPLS Inter-Autonomous System Option B configuration, the virtual circuits between the Autonomous System Border Router (ASBR) and the PE may fail to come up.

  Conditions: This symptom is observed while initially establishing VCs after the ASBR has reloaded.

  Workaround: The **clear xconnect** exec command can be used to clear the VCs that are down.

- CSCuj52699

  Symptom: A Cisco router crashes.

  Conditions: This symptom is observed in a load or stress condition.

  Workaround: There is no workaround.

- CSCuj54036

  Symptom: A Cisco c3900e router crashes during stress conditions.

  Conditions: This symptom is observed when content-scan is enabled and the router is at stress conditions.

  Workaround: There is no workaround.

- CSCuj55540

  Symptom: An exception is seen on a Cisco ISR 3945E router with whitelisted scansafe traffic.

  Conditions: This symptom is observed when there is a lot of whitelisted traffic going through the ISR box.

  Workaround: Disable whitelisting.

- CSCuj58950

  Symptom: A Cisco Catalyst 6500 Series switch may leak memory in the I/O pool due to mDNS traffic. The pool in which the leak is seen is dependent on the size of the incoming packet.

  Conditions: This symptom occurs when mDNS traffic is sent to the switch.

  Workaround: Apply an ACL to the inbound interface. This will drop the traffic and buffers will not leak.

- CSCuj64691

  Symptom: When configuring redistribute connected under eigrp, a host route/32 on SVI is installed unexpectedly.

  Conditions: This symptom is observed under the following conditions:

  – Configure a prefix to be in the routing table with EIGRP as the owner.

  – Redistribute connected interface to EIGRP so that the local entry is same as the prefix.

  Workaround: Disable STP for the VLAN of SVI (in this particular case).

- CSCuj64806

  Symptom: VRRPv2 priority may be incorrectly calculated when tracking tunnel interfaces. After reloading the router, the track decrement value is decremented twice. As a result, VRRPv2 with tracking does not work as expected.

  Conditions: This symptom is observed when you use tracking tunnel for VRRP priority.

  Workaround: Use VRRPv3.

- CSCuj65057

  Symptom: The **ip vrf forwarding** command under "aaa" is deleted after reloading the stack master.

Conditions: This symptom occurs after reloading the stack master switch.

```
--------- aaa new-model ! aaa group server tacacs+ TACACS+ ip vrf forwarding VRF01 !
ip vrf VRF01 rd x.x.x.x ---------
```

Workaround: Use the **vrf definition** command instead of the **ip vrf command to define vrf. (This command is supported on Cisco IOS Release 12.2(58)SE or later releases.)**

- CSCuj65601

  Symptom: Logging into a Cisco router through SSH and telnet with AAA fails.

  Conditions: This symptom occurs when the TACACS server group contains IPv6 source interface. The IPv6 source interface needs to be removed and added. After this process the SSH and telnet stops working.

  Workaround 1: On entering the **no ipv6 tacacs source-interface GigabitEthernet0/0/0** command, enter **end** and wait for around 2 minutes. Enter the **ipv6 tacacs source-interface GigabitEthernet0/0/0** command and wait for around 5 minutes. Login to the router through SSH or telnet.

  Workaround 2. Enter the above commands in succession and then wait for 7 to 9 minutes to login into the router.

- CSCuj66067

  Symptom: Router running out of memory after an upgrade to Cisco IOS Releases 15.3(1)S, 15.3(3)S, and 15.4(1)S.

  Conditions: This symptom is observed when huge number of route server (approximately more than 700) contexts configures in the router.

  Workaround: Perform the following workaround:

  1. Reduce the number of Route server contexts
  2. Downgrade the IOS version to 15.2(4)S or lower release

- CSCuj72553

  Symptom: The OSPF router may stay without a router LSA after NSF restarts which means that routing in the OSPF domain is seriously affected.

  Conditions: This symptom occurs under the following conditions: -OSPF NSF is terminated for some reason. -**mpls traffic-eng nsr** is configured.

  Workaround: Remove **mpls traffic-eng nsr**.

  More Info: Example of **show ip ospf nsf** after a failed NSF:

```
Router#sh ip ospf 1 nsf
Routing Process "ospf 1" IETF Non-Stop Forwarding enabled restart-interval limit: 120
sec Last IETF NSF restart 03:33:06 ago terminated after 5 secs, reason: Event nbr
1-way IETF NSF helper support enabled Cisco NSF helper support enabled Restart resync
LSA state: TE has requested data Restart resync Adj state: TE has requested data OSPF
restart state is NO_RESTART Handle 140515696469576, Router ID 10.1.1.1, checkpoint
Router ID 0.0.0.0 Config wait timer interval 10, timer not running Dbase wait timer
interval 120, timer not running
Router#
Router LSA generation is prevented by flag described on lines:
Restart resync LSA state: TE has requested data Restart resync Adj state: TE has
requested data
```

  Note: TE resync is not completed, although NSF is completed.

- CSCuj72631

  Symptom: The Cisco Catalyst 6500 Series Switch crashes due to mdns configuration running Cisco IOS Release 15.1(2)SY.

  Conditions: This symptom occurs while configuring the following:

  ```
  CMD: "service-routing mdns-sd" 09:05:29 EDT Thu Sep 26 2013
  CMD: "service-policy permit-all in" 09:05:52 EDT Thu Sep 26 2013
  CMD: "service-policy permit-all out" 09:06:14 EDT Thu Sep 26 2013
  Early Notification of crash condition..
  09:06:18 EDT Thu Sep 26 2013: Floating Point exception, CPU signal 8, PC = 0x406F71BC
  ```

  Workaround: There is no workaround.

- CSCuj75952

  Symptom: The Cisco ASR 1000 route processor reloads.

  Conditions: This symptom occurs during PPPoA session establishment if CAC determines that resources are low and HW-assisted CAC needs to be enabled. The router is used to terminate PPPoA sessions and Call Admission Control (CAC) is enabled.

  Workaround: Disable Call Admission Control.

- CSCuj78636

  Symptom: A memory leak is observed in the IP Switching segment.

  Conditions: This symptom occurs if a subscriber roams with the same MAC address but a different IP address. This happens only for L2 roaming and not for L3 roaming.

  Workaround: There is no workaround.

- CSCuj81681

  Symptom: Mediamon fails working after the number of records pushed from the producers exceeds the cache entries set.

  Conditions: This symptom is observed when the number of records or the flows generated by the traffic has to be more than the number of cache entries.

  Workaround: There is no workaround.

- CSCuj83764

  Symptom: Router crashes when a two-level ZBFW policy with attribute configured is attached to the zone pair.

  Conditions: This symptom is observed when the ZBFW policy has two levels and the attribute is used in the policy.

  Workaround: There is no workaround.

- CSCuj87667

  Symptom: When the value "xxx" of MPLS exp bits is copied to the outer IP/GRE header TOS, the new TOS value should be "xxx00000". Instead, it shows "00000xxx", and the QoS information is broken.

  Conditions: This symptom is observed in MPLS over GRE case.

  Workaround: There is no workaround.

- CSCuj94571

  Symptom: To run the BERT test, remove **keepalive** from the interface. After completing the BERT test, adding **keepalive** causes the standby RSP to reset.

Conditions: This symptom is consistent and affects Cisco IOS Release 15.1(3)S1.

Workaround: After the completion of the BERT test, remove the BERT test with **no bert pattern qrss interval** *interval* and then add **keepalive**. This will avoid standby RSP reset.

- CSCuj94804

  Symptom: On selecting a new clock source with the same QL value as the previous clock source, the clock class will not be updated.

  Conditions: This symptom occurs under the following conditions:

  1. Configure a PTP ordinary clock as master. The unit will select the internal clock source (QL-SEC) and will send clock class 58.
  2. Configure a network source with the same QL as the internal clock (that is, QL-sec). The new clock source will be selected, but the clock class does not change accordingly. The same issue does not occur when the network source is configured with a different QL value.

  Workaround: Reload the router.

- CSCuj99819

  Symptom: MVPN GRE tunnels are not established.

  Conditions: BGP has a VPN peer configured using an update-source that does not have PIM enabled.

  Workaround: There is no workaround.

- CSCul04692

  Symptom: A T1 controller flaps in CHT1/ET1 SPA.

  Conditions: This symptom is seen in T1 mode with “cablelength short 100ft” or “cablelength long 0db” when connected with a PURA box.

  Workaround: Configure “cablelength long -7.5db”.

- CSCul10573

  Symptom: On receiving a BGP update from a neighbor, the router will send an illegal network notification and flap the session.

  Conditions: This symptom occurs when the prefix received is a Leaf A-D route (RFC 6514) with an S-PMSI route serving as the Route Key.

  Workaround: There is no workaround.

- CSCul11961

  Symptom: While performing an ISSU super-pkg downgrade with broadband IP-based session features from Cisco IOS XE Release 3.12.0 to Cisco IOS XE Release 3.11.0, standby FP gets stuck in an "init" state after run version. There are Standby FP pending issues.

  Conditions: This symptom occurs while performing an ISSU super-pkg downgrade with broadband IP-based session features from Cisco IOS XE Release 3.12.0 to Cisco IOS XE Release 3.11.0.

  Workaround: There is no workaround.

  More Info: The issue will not occurs in the following cases:

  1. ISSU sub-pkg upgrade or downgrade between XE311 and XE312.
  2. ISSU sup-pkg upgrade from XE311 to XE312.
  3. PPP-session features in ISSU super-pkg upgrade or downgrade between XE311 and XE312.

  The upgrade from 3.11.0(without the fix for CSCul11961) to 3.12(with the fix of CSCul11961) works fine.

The downgrade from 3.12(with the fix of CSCul11961) to 3.11.0(without the fix for CSCul11961) fails with IP-based sessions. With this downgrade bug for 3.11.0, the fix will go out in 3.11.1 and 3.12.0.

- CSCul12583

  Symptom: L4R is not removed after an account logon when DRL is present.

  Conditions: This symptom occurs if per user merge is present.

  Workaround: There is no workaround.

- CSCul14571

  Symptom: Cisco router can crash after OSPFv3 is unconfigured from an interface.

  Conditions: This symptom is observed when NSR is enabled.

  Workaround: Unconfigure NSR before unconfiguring OSPFv3 from an interface.

  More Info: This is extremely rare issue; the OSPFv3 should be in a process of checkpointing LSA from primary RP to standby while an interface from which the LSA was received is unconfigured.

- CSCul19814

  ```
  Symptom: After collecting "raw netflow" data, the active switch crashes. The show flow
  monitor v4 cache command causes the reboot of the switch with the following message:
  %SCHED-3-TRASHING: Process thrashing on watched message event.
  ```

  Conditions: This symptom occurs due to the **show flow monitor** command.

  Workaround: There is no workaround.

- CSCul19906

  Symptom: A crash is seen on the Cisco ASR router with crashinfo and core with following messages:

  ```
  Exception to IOS Thread:
  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = EIGRP-IPv4
  ```

  Conditions: This symptom occurs with a Cisco ASR router routing EIGRP.

  Workaround: There is no workaround.

- CSCul24682

  Symptom: L2TP LNS puts a non-negotiated magic number to LCP packets. The PPPoE client may terminate the session prematurely due to the unknown magic number.

  Conditions: This symptom occurs when L2TP LAC does not negotiate the magic number with the PPPoE client and L2TP LNS does not renegotiate options with the PPPoE client.

  Workaround: Configure **lcp renegotiation always** on L2TP LNS.

- CSCul31953

  Symptom: Wrong value is fetched for plaintext mtu of IPSec SA.

  Conditions: Configuring Cisco Group Encrypted Transport VPN(GETVPN) within LISP network.

  Workaround: There is no workaround.

- CSCul38081

  Symptom: In a scaled environment, when a preferred path configuration is removed and is followed by a RP switchover the pseudowire interfaces goes down. The psudowire interface comes up if we add the preferred path or just remove and add the neighbor statement.

  Conditions: This symptom is not observed under any specific conditions.

Workaround: There is no workaround.

- CSCul40898

  Symptom: After reloading the router or fresh service-instance configuration, traffic received from the access is sent to the core without a dummy VLAN header. This traffic is received by a remote PE2 and sent to switch with a missing VLAN header. Therefore CE2 drops received packets. When the issue is removed, captured traffic in the core contains a dummy VLAN header.

  Conditions: This symptom is occasionally observed when the router is reloaded and is consistently observed when a new service instance is configured as an xconnect member.

  Workaround: Perform **shutdown** followed by **no shutdown** on the service instance.

- CSCul43968

  Symptom: Mroute states never expire on egress PE without any active downstream receivers.

  Conditions: This symptom occurs in an IPv6 multicast running in a VRF scenario and during unconfiguration of such a loopback interface that has MLD joins on it.

  Workaround: There is no workaround.

- CSCul47135

  Symptom: On Cisco ASR 1000 routers, services are not removed or applied from the active subscriber sessions when CoA is sent from the radius server. The router sends wrong values in response to the CoA request packet.

  Conditions: This symptom occurs when 15.2(20130918:081157) is run.

  Workaround: There is no workaround.

- CSCul54254

  Symptom: Invalid LSAs are not flushed by the router which has their Advertising Router ID. Specifically, Router LSAs which do not have LSID of 0 will not be flushed if the router does not re-originate them, and any LSA with a type that the router does not recognize.

  Lingering LSAs could lead to incorrect routing in some very obscure instances. For example, stale Router LSA fragments from two neighboring routers would need to remain in the network. There would not be a routing problem if only one router's stale Router LSA fragment was allowed to linger.

  Conditions: There are several possible scenarios that could lead to this symptom. One example is that a router is configured with many interfaces attached to an OSPFv3 instance such that it originates more than one Router LSA fragment. Then the router is reloaded before the configuration is saved, and after the reload it does not reoriginate some of the Router LSA fragments.

  Workaround: There is no workaround.

- CSCul55900

  Symptom: A FlexVPN Scale rate degradation occurs due to more CPU consumed by static processes.

  Conditions: This symptom occurs under the following conditions:

  1. Configure UUT to be the flexvpn server which can scale upto 10K sessions.
  2. Configure IKEv2 Authorization policy.
  3. Try to bring up the flexvpn 10K sessions and monitor the CPU usage.

  Workaround: Remove IKEv2 authorization policy. In such a case, IKEv2 routing and mode configuration cannot be verified.

- CSCul56207

  Symptom: A standby RP crashes.

  Conditions: This symptom is seen on a Cisco ASR 1000 router used for PPPoEoA-aggregation when configuring a range/pvc. It was seen together with the following error message:

  ```
  asr(config-if-atm-range)pvc-in-range 10/45 %ERROR: Standby doesn't support this
  command ^ % Invalid input detected at '^' marker.
  ```

  Workaround: There is no workaround.

- CSCul72121

  Symptom: Continuous trace backs on the PTF console is observed and PTF crashes during a soak.

  Conditions: This symptom occurs under the following conditions:

  1. Create an MDS profile as attached.
  2. Leave the setup for soak for 12 hours.

  Workaround: Reload ACT and SBY PTF.

- CSCul75876

  Symptom: A router may crash in an OSPF process during reconfiguration.

  Conditions: This symptom occurs under the following conditions:

  1. Configure the router with “ipfrr” in area 0.
  2. Connect router to area 0 through two links. For some route one interface is the primary path, and the second is the repair path.
  3. Configure router as ABR, that is, have a non-zero area with a neighbor. Do not configure “ipfrr” in the non-zero area. Quickly remove the IP address from both the interfaces in area 0 and router the may crash.

  Workaround: Changes to the reconfiguration procedure will avoid the crash.

  – Shutdown the interface before removing the IP

  – Remove the IP from one interface in area 0, wait for a few seconds and remove the IP address from the second interface in area 0.

- CSCul86211

  Symptom: When LNS switches off while the sessions keep on establishing at LAC, LAC finds the l2tp db memory exhausted after sometime. Due to this, it fails to update the session in the database and during this period a crash is observed.

  Conditions: This symptom occurs when LAC tries to add l2tp session in the database and fails to do so. In order to handle this error condition, LAC frees the l2tp and l2x session twice. This double free is the reason for crash.

  Workaround: There is no workaround.

- CSCul92497

  Symptom: The Cisco 7600 router providing layer2 EoMPLS services may stop forwarding ingress and egress traffic for an xconnect for which a backup peer config has been applied.

  Conditions: This symptom occurs in Cisco 7600 routers running Cisco IOS Release 15.2(4)S4a with ES+ cards (access/core facing) and xconnect configured under a service instance.

  Workaround: Clear the xconnect on the Cisco 7600 router side. Clearing on the remote size does not have an effect.

- CSCul96778

  Symptom: A router may crash and reload with BGP related traceback in an extremely rare timing condition while running “show ip bgp vpnv4 vrf XXXX nei A.A.A.A”.

  Conditions: This symptom occurs while making BGP-related changes such as moving the same neighbor with quick operation of “no neighbor x.x.x.x” and then “neighbor x.x.x.x across VRFs. Imediately after this if we type a “show ip bgp vpnv4 vrf XXXX nei A.A.A.A” - on a Cisco router running IOS and BGP, then in extremely rare timing condition the router may crash. The possibility of this to happen increases if there config and unconfig is done from one console and the show operation done from other console.

  Workaround: When doing configuration and unconfiguration and then show, it is better to serialize the operation rather than aggressively use multiple consoles to do all actions at the same time.

- CSCul99015

  Symptom: In VPLS using BGP Signaling with Inter AS, when a PE on another AS is reachable through multiple ASBRs, the PW destination & Next hop PE address of some or all of the PW’s in Standby RP remains as the non-preferred ASBR address instead of the preferred ASBR address.

  Conditions: This issue would be encountered when the following conditions occur:

  1. BGP L2VPN NLRI’s received first from a ASBR becomes a less preferred ASBR on receiving NLRI’s for the same VE-ID’s from a more preferred ASBR.
  2. NLRI received from the more preferred ASBR has the same values (VEID, VBO, VBS, Label Base, MTU & CW) as the ones received previously from the other ASBR.

  Workaround: Bring up BGP session with the more preferred ASBR first. This would cause no updates to existing NLRIs even if received from other less preferred ASBR.

- CSCum00056

  Symptom: ASR IOSd crash occurs with the following error:

  ```
  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = ISG CMD HANDLER
  ```

  Conditions: This symptom occurs when changes are made through RADIUS.

  Workaround: There is no workaround.

- CSCum02221

  Symptom: Memory Corruption crash: chunk from bgp_attrlist_chunks accessed past redzone. With BGP debug update turned on there will be messages about wrong attributes, etc. by BGP Error Handling shortly before the crash.

  Conditions: This symptom is observed while running BGPv4 codenomicon suite; BGP receives an update with repeating valid attributes with flag lengths bigger than data in the packet. Crash will happen every time with a generic BGP session if update as described above is received, however under normal working conditions crash will not occur as above update is not valid.

  Workaround: There is no workaround.

- CSCum04512

  Symptom: When an RP switchover is done (which is head end for 500 TE tunnel and tail end for 500 TE tunnels), the RSVP label is assigned to the TE tunnel change and this in turn causes a traffic loss of 45 seconds on the pseudowire which is directed through these tunnels.

  Conditions: This symptom occurs under the following conditions: -TE RID under the IGP is configured as a loopback other than the first one. -SSO is performed.

  Workaround: Configure the TE router ID under the IGP to be the first loopback interface.

- CSCum07119

  Symptom: A router generates tracebacks or crashes depending on platforms when **show application ip route** command is used concurrently with application route deletion.

  Conditions: This symptom is observed when the **show application ip route** command is issued when JAVA onePK SDK is handling route replace operations.

  Workaround:

  1. Use **show ip route** command to display the application routes and not **show application ip route** command.
  2. Use onePK GET ROUTE API to get the status of application added route.
  3. Use **show application ip route** only when there is no route delete is in progress.

- CSCum11118

  Symptom: A Cisco ISR router crashes due to stack overflow in the "ADJ background" process. The following syslog may be seen just before the crash:

  ```
  000105: Dec 9 04:08:44.447 UTC: SYS-6-STACKLOW Stack for process ADJ background
  running low, 20/6000
  ```

  Conditions: The conditions to this symptom are unknown.

  Workaround: There is no workaround.

- CSCum34830

  Symptom: A router crash is observed.

  Conditions: This symptom occurs while performing VRRP and VRRS-related configuration changes.

  Workaround: Unconfigure the **ip pim redundancy <>** command before deleting the subinterface or disabling PIM on an interface.

- CSCum42586

  Symptom: SLM does not work over the port-channel evc xconnect up mep.

  Conditions: This symptom occurs when port-channel member links are on the same NP.

  Workaround: There is no workaround.

- CSCum78363

  Symptom: Local circuit keeps DOWN state.

  Conditions: This symptom is observed when L2TPv3 session is configured.

  Workaround: There is no workaround.

- CSCum88382

  Symptom: BFD session not established upon RP Switchover and back.

  Conditions: This symptom is observed during RP switchover and switchback.

  Workaround: There is no workaround.

- CSCun00488

  Symptom: Duplicate records are exported from MMA.

  Conditions: This symptom occurs in the following topology:

  ```
  SRC --- UUT --DST | collector
  ```

Set the configuration at the UUT to export all the records to the collector. At the exporter, duplicate records are noticed.

Workaround: There is no workaround.

Open Bugs—Cisco IOS Release 15.4(1)S

This section describes possibly unexpected behavior by Cisco IOS Release 15.4(1)S. All the bugs listed in this section are open in Cisco IOS Release 15.4(1)S. This section describes only severity 1, severity 2, and select severity 3 bugs.

- CSCuh85588

  Symptoms: VRF-related CLIs are not executed under “view nw-gp”.

  Conditions: This symptom occurs in VRF-related CLIs.

  Workaround: Include the definition in the view rather than using all for vrf.

```
MCP-1RU(config-view)#commands configure
MCP-1RU(config-view)#commands configure  incl
MCP-1RU(config-view)#commands configure  include ?
  LINE  Keywords of the command
  all   wild card support
MCP-1RU(config-view)#commands configure  include vrf def
MCP-1RU(config-view)#commands configure  include vrf definition
```

Resolved Bugs—Cisco IOS Release 15.4(1)S

- CSCtb34814

  Symptoms: The following error message is reported just before a crash:

```
%DATACORRUPTION-1-DATAINCONSISTENCY: copy error
```

  There may not be any tracebacks given for the crash.

  Conditions: This symptom is observed under normal conditions.

  Workaround: There is no workaround.

- CSCtd45679

  Symptom: The standby supervisor reloads after removing an IPSLA probe via CLI:

```
R7600(config)#no ip sla 1
R7600(config)# 06:53:31: Config Sync: Line-by-Line sync verifying failure on command:
no ip sla 1 due to parser return error
06:53:31: rf_reload_peer_stub: RP sending reload request to Standby. User:
Config-Sync, Reason: Configuration mismatch
R7600(config)# 06:53:31: %RF-SP-5-RF_RELOAD: Peer reload. Reason: Proxy request to
reload peer
R7600(config)# 06:53:31: %OIR-SP-3-PWRCYCLE: Card in module 6, is being power-cycled
(RF request)
R7600(config)# 06:53:32: %PFREDUN-SP-6-ACTIVE: Standby processor removed or reloaded,
changing to Simplex mode
```

  Conditions: This symptom only occurs if the probe is configured via SNMP.

  Workaround: Remove the probe via SNMP.

More Info: This issue is applicable to a Cisco Catalyst 6500 platform running Cisco IOS 12.2SX releases. It may also affect other high availability (HA) platforms running Cisco IOS 12.2 or 15.X releases.

- CSCtq23960

  Symptoms: A Cisco ISRG2 3900 series platform using PPC architecture crashes and generates empty crashinfo files:

  ```
  show flash: all
  -#- --length-- -----date/time------ path <<snip>> 2 0 Mar 13 2011 09:40:36
  crashinfo_<date> 3 0 Mar 13 2011 12:35:56 crashinfo_<date> 4 0 Mar 17 2011 16:14:04
  crashinfo_<date> 5 0 Mar 21 2011 05:50:58 crashinfo_<date>
  ```

  Conditions: The symptom is observed with a Cisco ISRG2 3900 series platform using PPC architecture.

  Workaround: There is no workaround.

- CSCtx20903

  Symptom: TACACS authentication fallback does not work.

  Conditions: This symptom occurs in single connection TACACS host.

  Workaround: Disable the single connection.

- CSCty13747

  Symptoms: Cisco Network Based Application Recognition (NBAR) applications with “engine-id=13” not shown or exported.

  Conditions: This symptom is observed while executing the **show flow exporter option application table** command.

  Workaround: The issue has been fixed.

- CSCty57970

  Symptoms: A crash occurs when “content-scan out” is unconfigured from the egress interface.

  Conditions: This symptom occurs when “content-scan out” is unconfigured after router runs continuously for around two days.

  Workaround: There is no known workaround.

- CSCtz19192

  Symptom: Router crashes with the following message:

  Unexpected exception to CPU: vector 120.

  Conditions: This symptom occurs due to a change in the bandwidth or policing rate of the dialer interface.

  Workaround: Downgrade to Cisco IOS Release 15.1(4)M4.

- CSCtz66347

  Symptom: Router crashes on executing **show tech-support** from the linux client to the IOS server over an SSH session with the rekey enabled.

  Conditions: This symptom occurs when the rekey value “ip ssh rekey volume 400” is configured.

  Workaround: Disable the rekey feature by configuring the **no ip ssh rekey** command.

- CSCtz98228

  Symptom: On the Cisco 3900e platform, a crash and router reload occurs without generating any crashinfo and traceback.

Conditions: This symptom could be seen with HTTP traffic intercepted by the content-scan feature. It is mostly seen during the content-scan session creation.

Workaround: Disable the content-scan feature.

- CSCua64100

  Symptom: SCTP receive message fails when the socktest tool is used.

  Conditions: This symptom is seen only when the socktest tool is used.

  Workaround: Another test tool can be used.

- CSCub95285

  Symptoms: No logging messages are seen when configuring the syslog server in CLI mode until configuration mode is exited. However when unconfiguring the syslog server, syslog messages will appear within configuration mode.

  Conditions: The symptom is observed when, in CLI configuration mode, you enter the following command:

  ```
  Router(config)#logging host 1.2.3.4 transport tcp
  ```

  Workaround: There is no workaround.

- CSCuc11958

  Symptom: 7600-SIP-400 linecard crash seen with SPA reload.

  Conditions: The symptom is observed with a SPA reload.

  Workaround: There is no workaround.

- CSCuc41531

  Symptoms: Forwarding loop is observed for some PfR-controlled traffic.

  Conditions: This symptom is observed with the following conditions:

  - Traffic Classes (TCs) are controlled via PBR.
  - The parent route is withdrawn on selected BR/exit.

  Workaround: This issue does not affect configured or statically defined applications, but only affects learned applications so this can be used as one workaround. Another option is to issue shut/no shut on PfR master or clear the related TCs with the **clear pfr master traffic-class ...** command (this fixes the issue until the next occurrence).

- CSCuc49364

  Symptoms: A discrepancy is seen between show profile flow and show metadata table.

  Conditions: This symptom is observed on SIP Re-invite.

  Workaround: There is no workaround.

- CSCuc51879

  Symptom: Traffic loss occurs on the Cisco ASR 1000 Series Routers during an RP SSO switchover.

  Conditions: This symptom occurs during an RP SSO switchover on the Cisco ASR 1000 Series Routers.

  Workaround: There is no workaround.

- CSCuc57360

  Symptom: Adjacencies in the stats region get exhausted.

Conditions: This symptom occurs while reloading the router with mldp inband v4 and v6 data. When the control traffic ison and when other features are configured (scaled configuration), the adjacency leak happens. Adjacency allocation failure happens for the adjacencies allocated during this time.

Workaround: There is no workaround.

- CSCuc65662

  Symptom: Router crashes while configuring xconnect after traffic over SAToP over UDP.

  Conditions: The symptom is observed when you send traffic using SAToP over UDP. After that try to configure SAToP over MPLS and router crashes.

  Workaround: There is no workaround.

- CSCuc83061

  Symptoms: In a SAF setup with EIGRP, the EIGRP peers are seen flapping continuously when there are mixed TLV version neighbors on a single interface.

  Conditions: This symptom occurs when EIGRP Service-family neighbor-ship flaps are seen at random intervals. There is no definite pattern to these flaps, and they are not restricted to any one peer in the network. This issue is seen when there are two different TLV versions and they are on the same interface, and if service data is greater than 8KB.

  Workaround: There is no workaround. If one of the mixed peers is removed from the interface, the issue will not be seen.

- CSCuc85638

  Symptom: Ethernet CFM and ELMI interworking. If CFM is configured on xconnect and interworking with ELMI, incorrect EVC state may be reported to ELMI on MPLS configuration changes.

  Conditions: The symptom is observed with the following conditions:

  – CFM configured on xconnect EFP.

  – ELMI configured on same interface.

  – CFM-ELMI interworking enabled.

  Workaround: There is no workaround.

- CSCud32155

  Symptom: When the **license revoke** command is used, the license count does not reduce or change on the Cisco uBR10012 router with the Cisco uBR-MC3GX60V line card running Cisco IOS Release 12.2(33)SCF4.

  Conditions: This symptom occurs when the license is revoked without installing the actual license file.

  Workaround: A notification message will be displayed to user stating that the evaluation license will be installed on the device on revoke success.

- CSCud49546

  Symptom: The Cisco ASR 1000 Router Processor crashes with punted fragment-bit set multicast packets.

  Conditions: This symptom occurs when the fragment bit is set in the multicast packets and when the same fragment gets punted to the Router Processor more than once.

  Workaround: There is no workaround.

- CSCud58457

  Symptom: Standby interface stays UP/UP after a reload:

  ```
  BGL.S.15-ASR1004-1#sh int des Interface Status Protocol Description Te0/0/0 down down
  Te0/1/0 up up Te0/2/0 down down Te0/3/0 up up Gi0 admin down down
  ```

  It should be like this :

  ```
  BGL.S.15-ASR1004-1#sh int des
  Interface Status Protocol Description
  Te0/0/0 down down
  Te0/1/0 up up
  Te0/2/0 down down
  Te0/3/0 standby mode down
  Gi0 admin down down
  ```

  Conditions: The symptom is observed when “backup interface” and “carrier-delay” are configured under the interface:

  ```
  interface TenGigabitEthernet0/1/0
  backup interface TenGigabitEthernet0/3/0
  ip address 10.163.137.29 255.255.255.224
  logging event link-status
  carrier-delay up 1
  carrier-delay down msec 0
  cdp enable
  hold-queue 4096 in
  hold-queue 4096 out
  !
  interface TenGigabitEthernet0/3/0
  mac-address d867.d9dd.ff10
  no ip address
  logging event link-status
  carrier-delay up 1
  carrier-delay down msec 0
  cdp enable
  hold-queue 4096 in
  hold-queue 4096 out
  !
  ```

  Workaround: Flap the standby interface.

- CSCud86954

  Symptom: Some flows are not added to the Flexible Netflow cache, as indicated by the “Flows not added” counter increasing in the **show flow monitor statistics** command output. “Debug flow monitor packets” shows “FNF_BUILD: Lost cache entry” messages, and after some time, all cache entries are lost. At that moment, debug starts showing “FLOW MON: ip input feature builder failed on interface couldn’t get free cache entry”, and no new entries are created and exported (“Current entries” counter remains at 0).

  The following is sample output when all cache entries are lost:

  ```
  Router#sh flow monitor
  FNF-MON stat Cache type: Normal Cache size: 4096 Current entries: 0 High Watermark:
  882
  Flows added: 15969 Flows not added: 32668 Flows aged: 15969 - Active timeout ( 1800
  secs) 0 - Inactive timeout ( 15 secs) 15969 - Event aged 0 - Watermark aged 0 -
  Emergency aged 0
  ```

  Conditions: This symptom occurs when all of the following are true:

  – Flexible Netflow is enabled on a DMVPN tunnel interface.

  – Local policy-based routing is also enabled on the router.

  - Local PBR references an ACL that does not exist or an ACL that matches IPsec packets.

  Workaround:

  1. Make sure that the ACL used in the local PBR route-map exists and does not match IPsec packets sent over the DMVPN tunnel interface.
  2. Disabling encryption on the tunnel interface, or changing tunnel mode from mGRE to GRE also removes this bug.
  3. The issue will not be seen if FNF is not configured, or if FNF is configured but is not monitoring VPN traffic.

- CSCud96854

  Symptom: Standby RSP crashes while unconfiguring interfaces on ACR controller.

  Conditions: The symptom is observed when using a TCLSH script to teardown 450 CEM CKTs.

  Workaround: There is no workaround.

- CSCue05186

  Symptom: FRR LFA will wrongly switch to the alternate path if BFD is unconfigured on the peer router.

  Conditions: The symptom is observed if BFD is unconfigured on the peer router.

  Workaround: Shut the interfaces with BFD configured, remove the BFD configuration on both routers, then re-enable the interfaces.

- CSCue09385

  Symptom: Active RP crash during sessions bring up after clearing PDP.

  Conditions: The symptom is observed after clearing PDP.

  Workaround: There is no workaround.

  More Info: This is a negative test where DHCP IP under APN on IWAG is the access interface IP. In real world, we do not configure access interface IP as a DHCP IP for an APN.

- CSCue14596

  Symptom: The mib cfmFlowMetadataAppName value in the SNMP query should not include vendor information.

  Conditions: This symptom occurs when the SNMP query is run for mib cfmFlowMetadataAppName and the following value is obtained:

  ```
  cfmFlowMetadataAppName.2.1 = cisco telepresence-control
  ```

  The vendor information “cisco” should be removed. The expected mib value should be as following:

  ```
  cfmFlowMetadataAppName.2.1 = telepresence-control
  ```

  Workaround: There is no workaround.

- CSCue18999

  Symptom: The CEF adjacency becomes incomplete after the subinterface is up in the Cisco ASR 1000 series router.

  ```
  Router#show ip cef vrf <vrf_name> detail | include incomplete
  Adj source: IP adj out of <subinterface>, addr <IP Address> (incomplete)
  ```

  Conditions: This symptom occurs when too many subinterfaces are used and a shut/no shut is performed using an interface range on the physical interface.

Workaround 1. Execute shutdown/no shutdown on subinterfaces.

Workaround 2. Configure **no ip arp incomplete enable**.

- CSCue25754

  Symptom: During reconvergence after flapping of an MVPNv6 PE/CE interface in upstream PE, SG and SG RPT Prune state for the same source, a group will be created in the Upstream PE. SG RPT Prune state will be deleted after about 60 seconds. The outgoing MVPN tunnel interface will exist in both the SG state (with OIF state as Joined) and SG RPT Prune state (with OIF state as Pruned).

  Conditions: This symptom occurs only when data MDT configuration for the VRF containing the affected flow is deleted and then reconfigured while the PE/CE link is in "shutdown" state. The path to the source for the affected flow and also the Rendezvous Point for the affected flow are via the CE router attached to the link that has flapped.

  Workaround: The **clear ipv6 pim topology** command will clear the states, after which only the SG state will be recreated.

- CSCue50101

  Symptom: ATM OAM packets are not being sent on the L2TPv3 tunnel when configured in transparent mode.

  Conditions: This symptom is observed when you enable oam-pvc manage on the CE.

  Workaround: There is no workaround.

- CSCue68714

  Symptom: Newer released IOS-XE BGP, post Cisco IOS Release 15.2(4)S/XE3.7 not forming BFD session with the older implementations. This happens when using eBGP multi-hop to peer between two loopback interfaces on directly connected routers.

  Conditions: This ddts adds a couple of options "[single-hop | multi-hop]" to the existing BGP-BFD knob "neighbor x.x.x.x fall-over [bfd] [check-control-plane-failure]".

  So, after the change the knob would be: "neighbor x.x.x.x fall-over [bfd] [single-hop | multi-hop] [check-control-plane-failure]"

  **Note: Existing: "neighbor x.x.x.x fall-over [bfd]" --- This behavior would not be disturbed; so that we do not change the behavior that has been released as part of all the releases for more than three years now.

  Add-on in this ddts:

  1) neighbor x.x.x.x fall-over [bfd] [single-hop] -- NEW-option "single-hop"; would force BGP to open a single-hop bfd session. Even in case of back-to-back ebgp update-source loopback with 2 hop BGP peering.

  2) neighbor x.x.x.x fall-over [bfd] [multi-hop] -- NEW-option "multi-hop"; would force BGP to open a multi-hop bfd session.

  Workaround: There is no work around. ISR G2 should support BFD multi-hop feature.

  More Info: ISR-G2 does not support multi-hop BFD, while ISR4400 supports multi-hop BFD. BFD multi-hop support for ISR-G2 needs to be provided, so that they can interop with ISR4400 and ASRs.

- CSCue68761

  Symptom: A leak in small buffer is seen at ip_mforward in Cisco IOS Release 15.1(4)M3.

```
Device: Cisco 2911 Cisco IOS: c2900-universalk9-mz .SPA.151-4.M3.bin
----------------- show buffers ------------------
```

```
Buffer elements: 156 in free list (500 max allowed) 11839912 hits, 0 misses, 617
created
Public buffer pools: Small buffers, 104 bytes (total 45187, permanent 50, peak 45187 @
10:04:00): 0 in free list (20 min, 150 max allowed) 7968057 hits, 202704 misses, 2128
trims, 47265 created 71869 failures (680277 no memory)
----------------- show buffers usage ------------------
Statistics for the Small pool Input IDB : Mu1 count: 45180 Caller pc : 0x22CF95C4
count: 45180 Resource User: IP Input count: 45180 Caller pc : 0x22381654 count: 2
Resource User: Init count: 2 Output IDB : Mu1 count: 4 Caller pc : 0x2380114C count: 4
Resource User: PIM regist count: 4 Number of Buffers used by packets generated by
system: 45187 Number of Buffers used by incoming packets:
+++++++++++++++++++++++++++small buffer packet+++++++++++++++++++++++++++++++
<snip>
Buffer information for Small buffer at 0x2A815220 data_area 0xD9DEB04, refcount 1,
next 0x0, flags 0x2080 linktype 7 (IP), enctype 16 (PPP), encsize 2, rxtype 1 if_input
0x30F21520 (Multilink1), if_output 0x0 (None) inputtime 00:02:46.212 (elapsed
05:55:11.464) outputtime 00:01:22.632 (elapsed 05:56:35.044), oqnumber 65535
datagramstart 0xD9DEB56, datagramsize 38, maximum size 260 mac_start 0xD9DEB56,
addr_start 0x0, info_start 0xD9DEB58 network_start 0xD9DEB58, transport_start
0xD9DEB6C, caller_pc 0x22CF0044
source: 10.131.124.33, destination: 224.0.1.40, id: 0x55F0, ttl: 11, TOS: 192 prot:
17, source port 496, destination port 496
Enter hex value: 0x22CF95C4 0x22CF95C4:ip_mforward(0x22ce9448)+0x51c Enter hex value:
0x22CF0044 0x22CF0044:ip_mforward(0x22ce9448)+0x51c
```

Conditions: This symptom is observed with the Cisco 2911 running Cisco IOS Release 15.1(4)M3. When IP Multicast is used with NAT, in certain scenarios when NAT functionality returns error, multicast code does not free duplicate packet buffers eventually leading to exhaustion of packet buffer pool in the router.

Workaround: There is no real workaround except to disable NAT.

- CSCue76057

  Symptom: On a SIP 400 with gigeV2 SPA, when EVC is configured with “encap default”, it is seen that sometimes the FUGU TCAM is not programmed with correct VVID for the EVC. This results in incoming traffic reaching the linecard with wrong VVID. This can impact traffic incoming on the EVC.

  Conditions: The symptom is observed with an “encap default” configuration under EVC, or removal and re-application of “encap default” under EVC.

  Workaround: There is no workaround.

- CSCue85804

  Symptom: A memory allocation error occurs in the standby log after a switchover.

  Conditions: This symptom occurs after an RP switchover on a router configured with the Locator ID Separation Protocol (LISP).

  Workaround: There is no workaround.

- CSCue91919

  Symptom: When “ip mtu 17892” or “ipv6 mtu 17892” is configured on tunnel interfaces, a Config-Sync failure is seen after a Stateful Switch Over (SSO) and the CLI is rejected on reload.

  Conditions: The tunnel modes affected are “tunnel mode ipsec ipv4” or “tunnel mode mpls traffic-engineering”. The CLI “ip mtu 17892” is accepted for the “ipsec ipv4” tunnel mode or the “mpls traffic- engineering” tunnel mode , but is nvgenned in a different order causing a Config-Sync failure on SSO.

  Workaround: There is no workaround.

More Info: Since the CLI (ipv4 /ipv6 mtu 17892) is rejected on every reload, it has to be reentered to take effect.

- CSCue92027

  Symptom: The RP crashes due to redzone corruption.

  Conditions: This symptom occurs due to improper memory management

  Workaround: There is no workaround.

- CSCue92733

  Symptom: An open routing application cannot install a route into the router.

  Conditions: This symptom is observed when the application sets up the route with Null0 as a next-hop interface.

  Workaround: There is no workaround.

- CSCue95644

  A limited number of Cisco IOS and Cisco IOS XE releases based on theCisco IOS 15 code base include support for a new algorithm to hashuser-provided plaintext passwords. This algorithm is called Type 4,and a password hashed using this algorithm is referred to as a Type 4password. The Type 4 algorithm was designed to be a strongeralternative to the existing Type 5 and Type 7 algorithms to increasethe resiliency of passwords used for the “enable secret password” and’username username secret password’ commands against brute-forceattacks.

  For additional information please see the full Cisco Security Response at the link below.

  This Cisco Security Response is available at:

  http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20130318-type4

- CSCuf06108

  Symptom: Memory leaks from “IPC RTTYC Message Handler” might be detected by the “show memory debug leak” tool.

  Conditions: This symptom occurs when commands which involve remote TTY interactions and which are filter-specified (include or search) are executed. The memory leaks will occur on the RTTY client side.

  For example: Execute this command on PRE B (Active RP):

  ```
  sh licen all sub 0/0 | i Activeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
  ```

  The memory leak will be detected on PRE A (Standby RP): Address Size Alloc_pc PID Alloc-Proc Name 87252944 272 10F1E858 22 IPC RTTYC Messa IPC RTTYC Message Handler

  Workaround: There is no workaround.

- CSCuf09198

  Symptom: After deleting a VRF, you are unable to reconfigure the VRF.

  Conditions: The symptom is observed when BGP SAFI 129 address-family is not configured, but unicast routes are installed into multicast RIB to serve as upstream multicast hop, as described in RFC 6513. This applies to VRFs configured before BGP is configured.

  Workaround: Beyond unconfiguring BGP, there is no workaround once the issue occurs. Configuring a dummy VRF multicast address-family under BGP before the issue occurs can prevent the problem from occurring.

- CSCuf53543

  Symptom: MPLS-TP L2 VCs are down after an SIP reload and RP switchover.

Conditions: This symptom occurs when VCs are configured through an MPLS-TP tunnel in a hardware redundant platform.

Workaround: There is no workaround.

- CSCuf56776

  Symptom: After a linecard is removed and reinserted (OIR), traffic may fail to pass through some virtual circuits which have been configured for pseudowire redundancy.

  Conditions: This symptom is observed when the first segment ID in the redundancy group is numerically greater than the second segment.

  ```
  PE1#show ssm id | inc 1st 1stMem: 16394 2ndMem: 12301 ActMem: 12301 1stMem: 16394
  2ndMem: 12301 ActMem: 12301
  ```

  After the OIR is performed, it can be seen that the segments are reversed on the linecard.

  ```
  ESM-20G-12#sh ssm id | inc 1st 1stMem: 12301 2ndMem: 16394 ActMem: 12301 1stMem: 12301
  2ndMem: 16394 ActMem: 12301
  ```

  Workaround: There is no workaround.

- CSCuf56842

  Symptom: A reload may occur while using **show oer** and **show pfr** commands via SSH.

  Conditions: This symptom is observed when the **show pfr master application detail** command is used via SSH.

  Workaround: There is no workaround.

- CSCuf60830

  Symptom: The standby-RP occasionally crashes on the process SSS Manager after an RP failover when the new standby-RP attempts to sync.

  Conditions: This symptom occurs during an RP Failover, at high scale, with a high churn of sessions and ISG services.

  Workaround: In case the standby-RP does not recover itself after the crash, manually reload the router.

- CSCuf62756

  Symptom: If **bandwidth qos-reference** *value* is configured on an interface which bandwidth can change, then the actual interface bandwidth will be used for QoS service-policy validation when the interface bandwidth changes. This can result in a service-policy being removed if the interface bandwidth is insufficient to meet the requirements of the service-policy, such as bandwidth guarantees.

  Conditions: Affects variable-bandwidth interfaces such as EFM interfaces or PPP multilink bundles.

  Workaround 1: Use proportional actions in the QoS service-policy, such as “police rate percent....”, “bandwidth remaining ratio...”, “bandwidth remaining percent...”, and “priority percent”.

  Workaround 2: You can configure **bandwidth qos-reference** with maximum bandwidth of the interface:

  ```
  interface Ethernet0 bandwidth qos-reference <max bandwidth of interface>
  ```

  This can prevent policy-map detached due to interface bandwidth change.

- CSCuf65255

  Symptom: A CPU hog is caused by unnecessary requests to calculate the dynamic MPLS label range for each of the service instances configured (especially for L3VPN services).

Conditions: This symptom will occur if there is any MPLS ip-propagate-ttl, label range, or per-interface MPLS MTU configuration on the switch/router. When this configuration is present, and there are a large number of interfaces, any operation that involves generating the configuration will be slow (for example, show run, copy run, write mem, etc).

This can result in the copy operation taking more than 300 seconds (for an average configuration size of 1000kB). Note that it will complete in due course, and the generated configuration will be correct (it takes longer than it should).

Workaround: Reducing the number of BGP routes injected for L3VPN sessions causes the CPU hog to last for a smaller duration as it reduces the number of MPLS labels assigned and thus the amount of unnecessary work being done.

- CSCuf65371

  Symptom: On LAC, with "l2tp hidden" configured under VPDN template, L2TP sessions are failing to establish on existing L2TP tunnels after RP failover.

  Conditions: The symptom is observed with "l2tp hidden" configured under VPDN template.

  Workaround: Tear down L2TP tunnels after RP failover, or unconfigure "l2tp hidden". Disabling L2TP redundancy with "no l2tp sso enable" will fix issue as well.

- CSCuf68995

  Symptom: Ping failures are observed and traffic gets dropped.

  Conditions: The symptom is observed when you configure MPLSoMGRE tunnel on PE1 and PE2. Initiate ping from CE1 to CE2. Packets reach the CE2 and replay is coming back but these packets are getting dropped on PE2. After PE2 switchover, ping fails from CE1 to CE2. PE2 is configured with MPLSoMGRE on an HA system. Topology:

  ```
  CE1---- PE1 ----PE2----CE2
  ```

  Workaround: There is no workaround.

- CSCuf73798

  Symptom: Tracebacks are seen when Lc/Sp is comes up.

  ```
  May 15 10:14:22.145 IST: %MFIB_PLTF-SP-3-ENTRY_HANDLE_BAD: Space. 0x291E5D04 -Process=
  "mfib-const-lc Process", ipl= 0, pid= 303 -Traceback= 81D35D8z 8B13630z 8B0C434z
  8A86784z 8A3F588z 8A434A8z 8A65C64z 8A68ED0z 8A86EA8z 83ECFF0z 83E82D0
  ```

  Conditions: This symptom occurs in Cisco IOS Release 15.3(3)S.

  Workaround: There is no workaround.

  More Info: This issue was not reproducible. So a code walk-through and some safe checks and code strengthening was done to avoid such an error.

- CSCuf81275

  Symptom: Some ISG sessions do not pass traffic.

  Conditions: This symptom is observed when you have more than one Line Card for the ISG sessions.

  Workaround: There is no workaround.

- CSCuf86171

  Symptom: The DHCP snooping database agent can get stuck while using FTP as the transfer protocol.

  The following is the output of "show ip dhcp snooping database":

  ```
  Agent URL : <FTP URL> Write delay Timer : 300 seconds Abort Timer : 300 seconds
  ```

```
Agent Running : Yes Delay Timer Expiry : 0 (00:00:00) <<<<< Delay timer is at zero,
but process will never re-start Abort Timer Expiry : Not Running
Last Succeded Time : 02:09:53 PDT Thu Jun 6 2013 <<<<< Time will never update Last
Failed Time : None Last Failed Reason : No failure recorded.
Total Attempts : 12 Startup Failures : 0 Successful Transfers : 11 Failed Transfers :
0 Successful Reads : 1 Failed Reads : 0 Successful Writes : 10 Failed Writes : 0 Media
Failures : 0
```

Conditions: This symptom occurs while using FTP as the protocol to transfer the DHCP snooping binding database to an external server.

Workaround: Use another file transport mechanism like SCP or TFTP. Once the issue occurs, the only known workaround is to reload the affected device.

- CSCug04187

  Symptom: A build breakage is observed.

  Conditions: This symptom occurs due to CSCuf62756.

  Workaround: There is no workaround.

- CSCug08561

  Symptom: After a web-logon, users do not get the web-logon response page sent by the portal. If the web-logon is successful, users are not redirected to the web address which they have entered initially but are redirected to the portal for authentication.

  Conditions: This symptom occurs under the following conditions:

  1. Walkby feature is enabled with L4R & PBHK features applied to the lite session.
  2. User initiated the web-logon request.

  Workaround: There is no workaround.

  More Info: When a user does a web-logon, an account-logon coa request is triggered from the portal to ISG. In ISG, the account-logon request triggers a lite session conversion to a dedicated session. During the conversion, lite session and its associated resources (L4R and PBHK mappings) are removed from PD and a dedicated session gets provisioned. Once the conversion is done, ISG replies back with COA ACK/NACK to the portal. Based on the response from ISG, the portal generates a weblogon response (SUCCESS/FAILURE) page and sends it back to the client. But when it reaches ISG, the response packet does not get classified to session in the downstream direction and gets dropped in ISG because PBHK & L4R maping are deleted.

- CSCug08663

  Symptom: Traffic drops on the edge device and traffic looping may occur after a shut and no shut of the overlay interface.

  Conditions: This symptom may occur in an OTV multihoming setup when the overlay interface on one of the edge devices is shut and no shut in quick succession.

  Workaround: There is no workaround.

- CSCug15952

  Symptom: %QOS-3-INDEX_EXISTS error message is shown and router crashes.

  Conditions: The symptom is observed when sessions are bought up and the collision IDs with dynamic policy names are synced to standby from active. When the sessions time out and restart, the same dynamic policy names are synced to HA tree on standby again without cleaning up the tree earlier and the crash will happen.

  Workaround: Avoid the same session reestablishment before rebooting the router.

- CSCug17724

  Symptom: When using session protection and graceful restart for LDP, LDP neighbor goes down immediately after filtering LDP hello between routers. The LDP neighbor should go down after 10 minutes (default value of forwarding state holding time for GR).

  Conditions: The symptom is observed when you enable session protection and graceful restart for LDP

  Workaround: There is no workaround.

- CSCug17808

  Symptom: In certain scenarios, EIGRP routes are advertised only to stub peers and are not advertised to non-stub peers.

  EIGRP routes are routes in the EIGRP Topo table. They can be routes learnt by EIGRP peer or can be redistributed.

  Conditions: This symptom is observed when a Cisco ASR router is rebooted or the route is cleared via the **clear ip route** command and the route disappears from the spokes. This bug is not restricted to Cisco ASR routers. It can happen to any kind of routers if the following conditions are met:

  1. Peers must be a mixture of stubs and non-stubs.
  2. When a route is lost, send a query to non-stubs and wait for a reply from non-stubs about the query.
  3. A new update needs to be sent to all peers.

  Workaround: Upgrade to an image with the fix for this bug. Clearing the EIGRP neighborship restores the route on the spokes.

  Further Problem Description: In an ideal scenario, the sequence is as follows:

  1. When a route is lost, a query to non-stubs is sent.
  2. After receiving a reply from non-stubs, infinite metric to stub peers is sent.
  3. The route is learnt again.
  4. The route is advertised to both stub and non-stub peers properly.

  In a defective scenario (for example clear route), as a new route is learnt before getting a reply from non stubs, especially when non-stub neighbors or networks beyond non-stubs are more, sequence (3) comes before (2). In such cases routes are sent only to stubs.

- CSCug17820

  Symptoms: Random crashes are seen pointing to managed timer in L4F component.

  Conditions: The symptom is observed during scansafe traffic.

  Workaround: Disable the scansafe feature.

- CSCug18797

  Symptom: Router crashes when it checks whether the interface is configured as DHCP SIP session initiator.

  Conditions: The symptom is observed DHCP and ISG are configured.

  Workaround: There is no workaround.

- CSCug21879

  Symptom: After a link flap, ATM PVC does not come up due to PPP negotiation failure.

Conditions: This symptom occurs due to LCP timeout. The output queue of the Virtual Access Interface mapped to the dialer interface will be stuck or will be full with continual increment of output drops under the Virtual Access Interface.

Workaround: The two possible ways to recover from the Virtual Access Interface being stuck are:

1. Reconfiguring the ATM PVC.
2. Unbinding and rebinding the sialer to the ATM PVC using **no dialer pool-member <>** & **dialer pool-member <>** commands under the interface configuration mode.

- CSCug24114

  Symptom: CTS environment-data download fails from ISE.

  Conditions: The symptom is observed if there is less PAC and environment-data refresh timer is configured in ISE. After multiple refreshes of PAC and environment data and the switch is reloaded, sometimes a CTS environment-data download fails from ISE on the switch.

  Workaround: Unconfigure **pac key CLI** and configure it again as below:

  ```
  no pac key pac key <key-id>
  ```

- CSCug25258

  Symptom: Router crashes while running the **show interface rate-limit** command. When entries down the list of the output disappear for reasons such as interfaces going down or PPPoE clients disconnecting, the router may crash when you hit the space bar to get to these invalid entries.

  Conditions: This symptom occurs when rate limiting is configured.

  Workaround: Configure **term length 0** before running the show output.

- CSCug31561

  A vulnerability in the DHCP implementation of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

  The vulnerability occurs during the parsing of crafted DHCP packets. An attacker could exploit this vulnerability by sending crafted DHCP packets to an affected device that has the DHCP server or DHCP relay feature enabled. An exploit could allow the attacker to cause a reload of an affected device.

  Cisco has released free software updates that address this vulnerability. There are no workarounds to this vulnerability.

  This advisory is available at the following link:
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130925-dhcp

  Note: The September 25, 2013, Cisco IOS Software Security Advisory bundled publication includes eight Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the September 2013 bundled publication.

  Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep13.html

- CSCug31579

  Symptom: In an OTV scenario, when a multicast source (site) is connected via dual OTV routers and if the AED node's L3 interface flaps and comes up within around 30 seconds, the multicast stream stops flowing due to an RPF failure on the data group.

Conditions: This symptom occurs only when an AED node's L3 interface (join interface) flaps and comes up within around 30-50 seconds.

Workaround: Clear the mroute table on an AED using **clear ip mroute <data-group>**. This issue is not seen if the flapped interface comes up after around 150 seconds.

- CSCug33084

  Symptom: An SP/DFC crash is seen when a churn on the multicast is done either through provisioning/unprovisioning or through other network events.

  Conditions: This symptom occurs when a pointer to an already freed hal_context is still present in a replicate queue. Later during the churn the same pointer is accessed which leads to the crash.

  Workaround: There is no workaround.

- CSCug34485

  Multiple Cisco products are affected by a vulnerability involving the Open Shortest Path First (OSPF) Routing Protocol Link State Advertisement (LSA) database. This vulnerability could allow an unauthenticated attacker to take full control of the OSPF Autonomous System (AS) domain routing table, blackhole traffic, and intercept traffic.

  The attacker could trigger this vulnerability by injecting crafted OSPF packets. Successful exploitation could cause flushing of the routing table on a targeted router, as well as propagation of the crafted OSPF LSA type 1 update throughout the OSPF AS domain.

  To exploit this vulnerability, an attacker must accurately determine certain parameters within the LSA database on the target router. This vulnerability can only be triggered by sending crafted unicast or multicast LSA type 1 packets. No other LSA type packets can trigger this vulnerability.

  OSPFv3 is not affected by this vulnerability. Fabric Shortest Path First (FSPF) protocol is not affected by this vulnerability.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available. This advisory is available at the following link: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130801-lsaospf.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5.8/5.8: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:P/A:P/E:H/RL:U/RC:C

  CVE ID CVE-2013-0149 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCug34503

  Symptom: LLDP packets with destination MAC: 01:80:C2:00:00:0E are dropped.

  Conditions: This symptom occurs with the fix of CSCue41216.

  Workaround: There is no workaround.

  More Info: Regression because of CSCue41216 causes LLDP packets which have a MAC address of 01.80.c2.00.00.0e to get dropped according to MEF standard. But the packets should get dropped for SUNI and NNI port, while for CUNI they should get passed.

- CSCug34877

  Symptom: Switch crashes with the following message:

  ```
  %SYS-2-LINKED: Bad enqueue of 901E0D40 in queue 1AABE690 -Process= "SSH Process", ipl=
  0, pid= 392
  ```

Conditions: This symptom occurs during an SSH connection to a remote device from the switch while having multiple SSH connections to the same switch.

Workaround: There is no workaround.

- CSCug37196

  Symptom: Execution of "no bfd interval" under an interface results in a router crash.

  Conditions: Basic usage of the BFD template on an interface followed by the execution of the "no bfd interval" results in a router crash.

  Workaround: There is no workaround.

- CSCug37333

  Symptom: An error occurs while attaching a non-queue based service policy in the input direction.

  Conditions: This symptom occurs while attaching a service policy map in the input direction.

  Workaround: There is no workaround.

- CSCug38011

  Symptom: Device crashes with CPU hog messages.

  Conditions: The symptom is observed when the device is reloaded after configuring NTP peer:

  ```
  ntp server pool.ntp.org source cell0
  ```

  Workaround: There is no workaround.

- CSCug38248

  Symptom: Watchdog crash is observed on "Common Flow Table" timer process. For example:

  ```
  %SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = CFT Timer Process.
  ```

  Conditions: Error is raised due to a CPU loop while attempting to unbind and delete a child flow in the "CFT Timer" process.

  Workaround: There is no workaround.

- CSCug39278

  Symptom: L3 QoS policy not working in EVC L3 VPN.

  Conditions: The symptom is observed when CFM is enabled globally.

  Workaround: Disable CFM.

- CSCug41888

  This is by design currently. Logging persistent uses the software forced crash unexpected restart reason to handle various errors including misconfigurations and running out of space on the flash device in certain circumstances. CSCts03251 addressed one circumstance where running out of space on a flash device would lead to a software forced crash unexpected restart when trying to write to the persistent log, but if the flash is out of space and the oldest file is being deleted, the same issue can occur still.

  One known misconfiguration to lead to a software forced crash is to configure the protected option with a url that points to a file rather than a directory. When the next logging message is attempted to be written to the persistent log, the persistent logging feature determines that it can not write to the url provided and invokes a software forced crash. To avoid this, ensure that the url provided in the logging persistent command points to a directory or do not use the protected option.

  PSIRT Evaluation:

The Cisco PSIRT has evaluated this issue and does not meet the criteria for PSIRT ownership or involvement. This issue will be addressed via normal resolution channels.

If you believe that there is new information that would cause a change in the severity of this issue, please contact psirt@cisco.com for another evaluation.

Additional information on Cisco's security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCug44641

  Symptom: The **clear xconnect all** command causes xconnect related CFM configuration to be removed permanently.

  Conditions: This symptom is observed only when using xconnect related CFM configuration.

  Workaround: Avoid issuing the **clear xconnect all** command.

- CSCug48702

  Symptom: When no **ipv6 unicast-routing** is configured, a crash occurs in the router in the ART code.

  Conditions: This symptom occurs under the following conditions:

  1. Configure **ipv6 unicast-routing**.
  2. Add a few application routes.
  3. Configure **no ipv6 unicast-routing**.

  Workaround: There is no workaround.

- CSCug50208

  Symptom: A crash is seen due to double free of memory.

  Conditions: The symptom is seen when the accept interface VLAN goes down.

  Workaround: There is no workaround.

- CSCug50340

  Symptom: PW traffic is not flowing after SSO/card reset the active PTF card.

  Conditions: The symptom is observed with the following conditions:

  1. Create a unprotected tunnel between the active PTF card and create a PW.
  2. Apply the table map. Bi-directional traffic is flowing fine.
  3. SSO/reset the active PTF card in node 106 (4/1).
  4. Now tunnel core port is in standby card.
  5. Observed bi-directional traffic is not flowing once the card becomes up.
  6. Again reset the active PTF card (5/4).
  7. Observe uni-directional traffic only is flowing.

  Workaround: Delete the PW and recreate it again. However, note that if you do an SSO/card reset, the issue reappears.

- CSCug50606

  Symptom: Sometimes, IPCP assigns an different address for clients from wrong address pool.

  Conditions: This symptom is observed under the following conditions:

  – **peer default ip address** command is configured on dialers.

  - There are some dialers on the Cisco router.
  - The issue could happen on Cisco IOS Release 15.2(4)M3.

  Workaround: There is no workaround.

- CSCug52119

  Symptom: A RIB route is present for a prefix, but the router continues to LISP encapsulate.

  Conditions: The symptom is observed when a LISP map-cache existed for a prefix and then the RIB route was added later.

  Workaround: Use the following command:

  ```
  clear ip/ipv6 lisp map-cache <prefix>
  ```

- CSCug58977

  Symptom: 2.6Gbp/s traffic is observed on both of the VPN SPA interfaces. Traffic direction: Rx on outside interface, Tx on inside interface.

  Conditions: This symptom occurs when fragmented IPSec packet arrives on clear side. The issue is observed only in VRF mode.

  Workaround: Reload the IPSec card.

- CSCug59746

  Symptom: A crash is seen on the RP in the SS manager process:

  ```
  Exception to IOS Thread: Frame pointer 0x7F58BB22FE80, PC = 0x7C505FB
  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = SSS Manager -Traceback=
  1#980611ad3b9665cd80fe5178bcd6036a :400000+78505FB :400000+7C68774 :400000+7C6871A
  :400000+1C13522 :400000+7852194 :400000+78512C8 :400000+7C68774 :400000+7C6871A
  :400000+33A8AC1 :400000+77DD92F :400000+33C3E4C :400000+33AFE89 :400000+33B2564
  :400000+7824301 :400000+7823F37 :400000+77FA27F
  ```

  Conditions: The issue appears to be related to NAS port. It looks like a key is being set when the issue occurred. The exact conditions are still being investigated.

  Workaround: Possibly remove radius or more specifically, NAS port configurations. This still needs to be verified.

- CSCug61252

  Symptoms: The potential exists for an unauthenticated user to read the contents of an uninitialized memory of a WebEx node.

  Conditions: This symptom occurs in the fefault installation of an affected version of the WebEx node software.

  Workaround: There is no workaround.

  Additional details about the vulnerability described here can be found at:
  http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2013-1232

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5/5:
  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:N/C:P/I:N/A:N/E:H/RL:U/RC:C

  CVE ID CVE-2013-1232 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL:
  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCug61485

  Symptom: The Cisco ASR 1000 RP crashes in RSVP.

Conditions: This symptom occurs when “mpls traffic-eng tunnels” is configured on an interface and “ip rsvp bandwidth” is not configured and the bandwidth on the physical interface is changed.

Workaround: There is no workaround.

- CSCug62154

  Symptom: CPU shoots to 100% with TACACS configuration. VTY to the device does not work due to this.

  Conditions: This symptom is observed when the router or switch is booted up with TACACS configurations and the CPU shoots up to 100%. Telnet to the router is not possible. Any command issued on the console would take lot of time.

  Workaround: Remove the TACACS configurations and then reboot the router.

- CSCug64059

  Symptom: In a rare case when the VPN core RR advertises paths that contain the ibgp-CE attribute ATTR_SET to the PE and does a graceful start, the PE router crashes.

  Conditions: This symptom occurs in a rare case when the VPN core RR advertises paths that contain the ibgp-CE attribute ATTR_SET to the PE and the peering RR to PE does a graceful restart. In case the RR switches over then the stale paths in the PE containing ATTR_SET cause the PE to crash.

  Workaround: This problem will not occur if the RR that sends paths to the PE with ATTR_SET does not enable graceful restart.

- CSCug64957

  Symptom: An error occurs on changing the grandchild class rate.

  Conditions: This symptom occurs when 1x1000x8 policy maps are configured.

  Workaround: There is no workaround.

- CSCug68193

  Symptom: Multicast traffic across ES+ cards stop flowing across subinterfaces.

  Conditions: The symptom is observed after a linecard OIR. After the linecard comes up, multicast traffic stops flowing across subinterfaces.

  Workaround: Shut/no shut the subinterface.

- CSCug70151

  Symptom: The box crashes on removing the oneP datapath transport CLI configuration.

  Conditions: This symptom occurs only on Cisco c3945e, Cisco c3925e and Cisco IOL platforms.

  Workaround: There is no workaround.

- CSCug71297

  Symptom: An SP crash is observed at the below RPC call block during an ISSU upgrade after commit version.

  ```
  SP: Frames of RPC pf_issu_sp2rp process (pid 579) on 16 (proc|slot) after blocking rpc
  call failed: 42342B84
  ```

  Conditions: This symptom occurs during ISSU commit version while saving the configuration.

  Workaround: There is no workaround.

- CSCug72891

  Symptom: EIGRP neighbor flaps due to EIGRP SIA. Troubleshooting shows that a race condition causes EIGRP successor loop first and it leads to EIGRP QUERY loop resulting in the neighbor flaps.

  Conditions: The issue is observed when a worse metric update is received from the successor, once the route is already in active state, in a partially peered multiaccess network.

  Workaround: There is no workaround.

- CSCug75194

  Symptom: A latency issue is observed. The order of packets changes.

  Conditions: This symptom occurs on EVC xconnect for MACsec packets and data packets.

  Workaround: Stop the control traffic from the peer side and send only data traffic.

- CSCug77784

  Symptom: When **wr mem** is executed, the following error message is seen:

  ```
  private-config file open failed (File table overflow)
  ```

  Conditions: This symptom occurs when the standby is reloaded continuously. Due to this, the client, that is, the active side is not able to reach the standby side and while returning an error, the FD is not released and exhausts FDs. The maximum number of open FDs allowed is 128. Once this limit is reached, no more files can be opened.

  Workaround: Reload is a possible workaround to free the FDs.

- CSCug78098

  Symptom: Supervisor engine crashes and the Cisco IOS software is forced to reload due to the PIM process.

  Conditions: This symptom is observed when using the **show ip pim rp-hash** command right after the BSR RP times out and causes the crash.

  Workaround: Perform these steps in the following order:

  1. Wait for a minute after BSR RP times out before using this command.
  2. Configuring **no ip domain lookup** will make the time taken to execute **show ip pim rp-hash** to a few milliseconds. This will prevent the crash from being reproduced manually.

- CSCug78929

  Symptom: Packets of a certain protocol are dropped due to v6 PACL applied on a switch port.

  Conditions: This symptom occurs when v6 PACL contains explicit protocol entries such as “permit 89 any any”.

  Workaround: There is no workaround.

- CSCug79199

  Symptom: When the Gigbit Ethernet SPA interface configured with vlan0, that is, “encapulation priority-tagged native tx-tagged” undergoes MDR, MDR will fail with a “:%ETH_SPA_GILA_FUGU-3-HW_SW_MISMATCH” message. MDR will be aborted and the SPA will undergo a reboot thereby causing interface flaps and traffic loss.

  Conditions: This symptom occurs when the Gigabit Ethernet interface is configured with vlan0 configuration as follows:

  ```
  interface GigabitEthernet0/1/0.9
  encapsulation priority-tagged native tx-tagged
  ```

```
ip address 21.0.0.1 255.255.255.0 !
```

Workaround: There is no workaround.

- CSCug79561

  Symptom: Memory leaks are observed when accessing certain parts of the PTP MIB.

  Conditions: This symptom occurs when the following OIDs are accessed:

  ```
  cPtpClockInput1ppsInterface : 1.3.6.1.4.1.9.9.760.1.1.3.1.11
  cPtpClockOutput1ppsInterface : 1.3.6.1.4.1.9.9.760.1.1.3.1.12 cPtpClockTODInterface :
  1.3.6.1.4.1.9.9.760.1.1.3.1.13 cPtpClockCurrentDSOffsetFromMaster :
  1.3.6.1.4.1.9.9.760.1.2.1.1.5 cPtpClockCurrentDSMeanPathDelay :
  1.3.6.1.4.1.9.9.760.1.2.1.1.6 cPtpClockParentDSParentPortIdentity :
  1.3.6.1.4.1.9.9.760.1.2.2.1.4 cPtpClockParentDSGMClockIdentity :
  1.3.6.1.4.1.9.9.760.1.2.2.1.8 cPtpClockDefaultDSClockIdentity :
  1.3.6.1.4.1.9.9.760.1.2.3.1.5 cPtpClockTransDefaultDSClockIdentity :
  1.3.6.1.4.1.9.9.760.1.2.6.1.3 cPtpClockPortName : 1.3.6.1.4.1.9.9.760.1.2.7.1.5
  cPtpClockPortCurrentPeerAddress : 1.3.6.1.4.1.9.9.760.1.2.7.1.9 cPtpClockPortDSName :
  1.3.6.1.4.1.9.9.760.1.2.8.1.5 cPtpClockPortDSPortIdentity :
  1.3.6.1.4.1.9.9.760.1.2.8.1.6 cPtpClockPortDSPeerMeanPathDelay :
  1.3.6.1.4.1.9.9.760.1.2.8.1.13 cPtpClockPortRunningName :
  1.3.6.1.4.1.9.9.760.1.2.9.1.5 cPtpClockPortTransDSPortIdentity :
  1.3.6.1.4.1.9.9.760.1.2.10.1.4 cPtpClockPortTransDSPeerMeanPathDelay :
  1.3.6.1.4.1.9.9.760.1.2.10.1.7 cPtpClockPortAssociateAddress :
  1.3.6.1.4.1.9.9.760.1.2.11.1.7
  ```

  Workaround: Exclude the above OIDs.

- CSCug79857

  Symptom: Router crash is seen.

  Conditions: The symptom is observed when you issue the following command:

  show ip subscriber mac e01d.3b70.108e

  Workaround: Do **show ip subscriber mac** *e01d.3b70.108e* only for the sessions in connected state, that is, sessions should not be in “Attempting” state in **sh sss sess | i** *mac address*.

- CSCug83238

  Symptom: TE Tunnel constantly performs signalling attempts instead of holding down the path option, which causes CPU to become very busy.

  Conditions: The symptom is observed with the following conditions:

  – Configuration of multiple verbatim explicit path options.

  – Path error during LSP signalling.

  Workaround: There is no workaround.

- CSCug85947

  Symptom: OSPFv3 routes go missing after an NSR switchover.

  Conditions: This symptom occurs after an SSO.

  Workaround: Clear the IPv6 OSPF process.

- CSCug86298

  Symptom: The “l4f mgt task” process takes up memory and does not release it.

  Conditions: This symptom occurs with scansafe configuration.

  Workaround: There is no workaround.

- CSCug87772

  Symptom: On a receiver PE router with a scaled recevier MVRF, stale entries are left behind in the MFIB table after a shut/unshut of the subinterfaces.

  Conditions: This symptom occurs when 200 receiver MVRFs are configured on the receiver PE router and the subinterfaces are shut/unshut.

  Workaround: There is no workaround.

- CSCug92091

  Symptom: When an IPv6 host is performing DAD and it is not yet present in the binding table it might log the following message:

  ```
  %SISF-4-PAK_DROP: Message dropped A=:: G=FE80::84D2:B20F:7041:433D V=7 I=Gi1/0/13
  P=NDP::NS Reason=Advertise while TENTATIVE
  ```

  This packet is seen on other ports in the same VLAN without an impact to DAD. Hence the message is misleading.

  Conditions: This symptom occurs when DAD packets are received on the switch and they can be logged as drops.

  Workaround: There is no workaround.

- CSCug92748

  Symptom: Pathtrace (Mediatrace) Service Set APIs can crash the network element when the source-ip or destination-ip in the path specifier is null.

  Conditions: This symptom occurs when Pathtrace (Mediatrace) Service Set APIs is used with a path-specifier with a destination ip or source ip set to null.

  Workaround: Do not use source ip and destination ip as null for path specifier while using the Pathtrace (Mediatrace) Service Set APIs.

- CSCug94275

  Symptom: ES+ card crashes with an unexpected exception to CPU: vector 200, PC = 0x0.

  Conditions: The symptom is observed on the ES+ series linecards on a Cisco 7600 series router. Symptom is reported on the ES+ console and in the crashinfo file on the ES+ flash disk. It is not reported in the syslog.

  Workaround: There is no workaround.

- CSCug97383

  Symptom: Switch crashes with EOAM and IP SLA Ethernet-monitor configurations.

  Conditions: This issue occurs infrequently when EOAM configuration include VLANs. Does not occur if all EOAM configurations are configured with only Ethernet Virtual Circuits (EVC).

  Workaround: There is no workaround.

- CSCug99771

  Symptom: OSPF N2 default route missing from Spoke upon reloading Hub. Hub has a static default route configured and sends that route over DMVPN tunnel running OSPF to spoke. When hub is reloaded, the default route is missing on Spoke. NSSA-External LSA is there on Spoke after reload, but the routing bit is not set. Hence, it is not installed in RIB on Spoke.

  Conditions: Default originated using command **area X nssa default-information-originate**.

  Workaround: Removing & re adding **area X nssa default-information-originate** on Hub resolves the issue.

- CSCuh01533

  Symptom: Memory leaks are seen at SADB index list.

  Conditions: This symptom is observed in ISR-G2 and ASR platforms when the configurations are loaded.

  Workaround: There is no workaround.
- CSCuh03718

  Symptom: When configuring a fail-close policy for GETVPN, an exemption for locally terminated VPN on the GM (deny esp any any) does not work. The traffic will still be blocked until the GETVPN policy is downloaded via a registration to the KS.

  One scenario is where the GM is terminating a GETVPN domain as well as GRE/IPSEC tunnels encrypted by tunnel-protection.

  Conditions: This symptom is observed under no specific conditions.

  Workaround: There is no workaround.
- CSCuh06821

  Symptom: Traffic drop occurs after the SSO.

  Conditions: This symptom is observed with RSP10g.

  Workaround: There is no workaround.
- CSCuh07349

  Symptom: A Cisco 7600 Sup may crash due to SP memory corruption.

  Conditions: This issue is observed on an REP enabled router, which is part of an REP segment. The exact trigger for this issue is not clear.

  Workaround: There is no workaround.
- CSCuh07404

  Symptom: VFI and PWs remain down.

  Conditions: This symptom is observed after removing and re-adding VLAN.

  Workaround: Configure **member vfi <>** command again under VLAN configuration.
- CSCuh07657

  Symptom: VRF Aggregate label is not re-originated after a directly connected CE facing interface (in VRF) is shut down.

  Conditions: This symptom occurs in an MPLS VPN set-up with Cisco 7600(PE) Router running on Cisco IOS Release 12.2(33)SRE4 with per VRF aggregation.

  For example:

  ```
  mpls label mode vrf TEST protocol all-afs per-vrf
  ```

  Workaround: Downgrade to Cisco IOS Release 12.2(33)SRE3 or earlier.
- CSCuh09412

  Symptom: A Cisco ASR 1000 running ISG with "radius-proxy session-restart" crashes when WiFi clients are roaming between hotspots.

  Conditions: The symptom is observed if a client roams between WiFi access points and the accounting-stop message from the initial access point does not reach the ISG where the subscriber session is active as can sometimes be the case of roaming between access points on a wireless LAN controller.

Workaround: Disable “radius-proxy session-restart” and reload the chassis to clear the session-cache.

- CSCuh16115

  Symptom: With VPLS configuration with IP-FRR, on doing multiple churns SP/LC may crash.

  Conditions: The issue occurs when xconnect internal data structre is to be freed up and IP FRR is still pointing to it.

  Workaround: Remove IP-FRR configuration before unprovisioning xconnect.

- CSCuh16927

  Symptom: Mac entries learned on a trunk link are flushed after removing VLANs.

  Conditions: The symptom is observed when some allowed VLANs are removed on a trunk link, all mac address entries learned on this link are flushed. This is issue is specific to extended VLAN IDs.

  Workaround: Executing ping to destination IP after removing VLANs will recover this condition.

- CSCuh20027

  Symptom: Cisco router configured with Locator ID Separation Protocol (LISP) configuration may crash when LISP debug is enabled.

  Conditions: This symptom is observed when LISP debug output is enabled through “debug lisp control ...”.

  Workaround: Disable LISP debugging.

- CSCuh21740

  Symptom: There is a deletion and addition of VRFs with MVPNV6 configurations.

  Conditions: This symptom occurs when PIM VRF neighbors are not up.

  Workaround: Reload the router.

- CSCuh24040

  Symptom: BGP routes are not marked Stale and considered best routes even though the BGP session with the peer is torn down. A hard or soft reset of the BGP peering session does not help.

  For BFD-related triggering, the following messages are normally produced with the BGP-5-ADJCHANGE message first, and the BGP_SESSION-5-ADJCHANGE message second. Under normal conditions, the two messages will have identical timestamps. When this problem is seen, the order of the messages will be reversed, with the BGP_SESSION-5-ADJCHANGE message appearing first, and with a slightly different timestamp from the BGP-5-ADJCHANGE message. In the problem case, the BGP_SESSION-5-ADJCHANGE message will also include the string “NSF peer closed the session”

  For example when encountering this bug, you would see:

  ```
  May 29 18:16:24.414: %BGP_SESSION-5-ADJCHANGE: neighbor x.x.x.x IPv4 Unicast vpn vrf
  VRFNAME topology base removed from session NSF peer closed the session May 29
  18:16:24.526: %BGP-5-ADJCHANGE: neighbor x.x.x.x vpn vrf VRFNAME Down BFD adjacency
  down
  Instead of: May 29 18:16:24.354: %BGP-5-ADJCHANGE: neighbor x.x.x.x vpn vrf VRFNAME
  Down BFD adjacency down May 29 18:16:24.354: %BGP_SESSION-5-ADJCHANGE: neighbor
  x.x.x.x IPv4 Unicast vpn vrf VRFNAME topology base removed from session BFD adjacency
  down
  ```

  Log messages associated for non-BFD triggers are not documented.

Conditions: This symptom is observed when BGP graceful restart is used in conjunction with BFD, but it is possible (but very low probability) for it to happen when BGP graceful restart processing happens when any other type of BGP reset (Example: clear command) is in progress.

Affected configurations all include:

```
router bgp ASN
...
bgp graceful-restart
...
```

The trigger is that BGP exceeds its CPU quantum during the processing of a reset, and gives up the CPU, and then BGP Graceful Restart processing runs before BGP can complete its reset processing. This is a very low probability event, and triggering it is going to be highly dependent on the configuration of the router, and on BGP's CPU requirements.

It is not possible to trigger this bug unless BGP graceful-restart is configured.

Workaround: If you are engaged in active monitoring of router logs, and the bug is being triggered by a BFD-induced reset, you can detect this situation by watching for the reversal of log message order described in the Symptoms section, and then take manual steps to remedy this problem when it occurs.

On the problematic router, issue **no neighbor <xxx> activate** command under the proper address-family will clear the stale routes.

The other option is to manually shutdown the outgoing interface which marks the routes as "inaccessible" and hence not been used anymore. This prevents the traffic blackhole but the routes will stay in the BGP table.

More Info: This bug affects all releases where CSCsk79641 or CSCtn58128 is integrated. Releases where neither of those fixes is integrated are not affected.

- CSCuh27770

  Symptom: On a dual-RP system which is configured for stateful switchover (SSO), some VPLS virtual circuits may fail to be provisioned on the standby route processor.

  Conditions: This symptom is observed when the VFI consists of VLAN interfaces that are also configured for IP.

  Workaround: Reload the standby RP.

- CSCuh32177

  Symptom: The "no passive-interface <if-name>" command will be added automatically after configuring the "ipv6 enable" command on the interface even though the "passive-interface default" command is configured for OSPFv3.

  ```
  (config)#interface FastEthernet0/2/0
  (config-if)#ipv6 enable
  (config-if)#end
  #sh run | sec ipv6 router ospf
  ipv6 router ospf 100 router-id 10.1.1.1
  passive-interface default
  no passive-interface FastEthernet0/2/0 <<< Added automatically. ---
  ```

  Conditions: This symptom occurs when the "passive-interface default" command is configured for OSPFv3.

  Workaround: Adjust the configuration manually. In this example it would be "passive-interface FastEthernet0/2/0".

- CSCuh32439

  Symptom: A linktrace targeted at the MAC address of a remote MIP fails with no response seen from the router with the target MIP despite the fact that a linktrace targeted at a MEP or MIP beyond that MIP fully succeeds (including recording the existence of the MIP that cannot be targeted directly).

  Conditions: This symptom is seen only when all of the following conditions are true:

  – The router on which the target MIP is on uses the 'Bridgeport' model of assigning MAC addresses to MPs (currently, this is just Cisco ASR 901 router).

  – The target MIP is on a port channel interface.

  – The target MIP is not on the port that the linktrace will ingress on.

  Workaround: Linktraces to MIPs or MEPs beyond the failing MIP will succeed and return the relevant information for the untargetable MIP.

- CSCuh36124

  Symptom: Service Routing/SAF in Cisco IOS Release 15.2 experiences HIGH cpu during a failover condition where the active SAF forwarder looses connection to the network causing the clients to switch to the secondary forwarder. This problem only happens if the forwarder that becomes active still has an active neighbor that it needs to send an updated registration data to (so more than 2 forwarders are required to observe this defect). Due to the high CPU condition during this failover, clients can experience longer registration times increasing the outage window.

  Conditions: This symptom ocurrs when more than 2 forwarders are involved and all the forwarders are peered to each other via direct configured peers or network-based EIGRP peers. The HIGH CPU is caused directly by the connection that exists between SAF forwarders to exchange data across the network, and not due to the client towards SAF forwarder data exchange.

  Workaround: There is no workaround.

- CSCuh37664

  Symptom: Prefixes and TCs stay "INPOLICY" although some configured resolvers are above the threshold.

  Conditions: This symptom occurs when a policy uses non-default resolvers.

  Workaround: Reload the MC.

  More Info: Non-default resolvers are not checked (only unreachable is checked).

  Output of "debug pfr master prefix detail" should normally show a similar line for each of the configured resolvers

  ```
  OER MC PFX 10.2.1.0/24: Check ACT ABS unreachable: unreachable 0, policy 400000,
  notify FALSE
  ```

  When the problem is seen, only this line is observed for the unreachable.

- CSCuh39624

  Symptom: PMIPV6 crashes when "no ipv6 mobile pmipv6-lma lma1" is configured.

  Conditions: This symptom occurs when "no ipv6 mobile pmipv6-lma lma1" is configured.

  Workaround: There is no workaround.

- CSCuh40275

  Symptom: SNMP occupies more than 90% of the CPU.

  Conditions: This symptom is observed when polling the cefFESelectionTable MIB.

  Workaround: Execute the following commands:

```
snmp-server view cutdown iso included
snmp-server view cutdown cefFESelectionEntry excluded
snmp-server community public view cutdown ro
snmp-server community private view cutdown rw
```

- CSCuh40329

  Symptom: OSPFV3 runs as PE-CE, but used to learn IPv4 prefixes. Core facing interface is GRE tunnel where OSPF and LDP runs. OSPV3 based Shamlinks are created between PEs. When tunnel flaps , OSPF and LDP recovers, but in a few seconds tunnel locks up. In locked up condition, all traffic fails on the tunnel, even directly connected pings. The only way to recover is to reconfigure the tunnel from scratch. It happens fairly consistently after every re-convergence, not every time though.

  Conditions: This issue is seen only on ISRG2s that are configured as PEs. They are so far seen with 3925 running Cisco IOS Release 15.3(2)T and 2911 running Cisco IOS Release 15.2(4)M3.

  Workaround: Use OSPF V2 based shamlinks.

- CSCuh40617

  Symptom: Ping fails when “encap dot1q” is configured on an FE SPA inserted in bay 1 of flexwan.

  Conditions: This symptom is observed when FE SPA is inserted in bay 1 of flexwan.

  Workaround: Move the SPA to bay 0 of flexwan.

- CSCuh41290

  Symptom: After the unavailability of the LDAP CRL, no new CRL fetches can be done because LDAP waits for a reply infinitely and never times out.

  Conditions: This symptom was first seen on Cisco IOS Release 15.1(4)M6 but not exclusive to it.

  Workaround: Set “revocation-check none” under affected trustpoint. Reload router.

- CSCuh43027

  Symptom: Prefixes withdrawn from BGP are not removed from the RIB although they are removed from the BGP table.

  Conditions: A withdraw message contains more than one NLRI, one of which is for a route that is not chosen as best. If deterministic med is enabled, then the other NLRI in the withdraw message might not eventually be removed from the RIB.

  Workaround: Forcibly clear the RIB.

  Further Problem Description: This issue may also occur if BGP PIC is enabled and the withdraw message contains a route that is currently serving as a backup path.

- CSCuh43252

  Symptom: After upgrading to Cisco IOS Release 15.0(2)SE3, you can no longer authenticate using TACACS. The TPLUS process on the switch will be pushing the CPU up to 99%.

  Conditions: The symptom is observed when you use TACACS for authentication.

  Workaround: Downgrade the switch to a version prior to 15.0(2)SE3.

- CSCuh43255

  Symptom: The BGP task update-generation process may cause the router to reload, in a rare timing condition when there is prefix flap and there is high scale of prefixes going through update-generation, including the flapping prefix.

Conditions: The symptom is observed when the Cisco ASR router is acting as a route server for BGP along with having various route-server contexts. The router does not do any forwarding. It merely processes control plane traffic.

Workaround: There is no workaround.

More Info: The setup is the same as mentioned in this doc: http://www.cisco.com/en/US/docs/ios/ios_xe/iproute_bgp/configuration/guide/irg_route_server_xe.html.

- CSCuh44420

  Symptom: When a Cisco IOS router with one or more mpls ldp neighbors undergoes an mpls ldp router-id configuration change and non-stop routing had been previously enabled and disabled prior to the router-id configuration change, sessions fail to become NSR-ready once mpls ldp nsr is reconfigured.

  Conditions: This symptom occurs when the mpls ldp router-id is reconfigured after mpls ldp nsr has been enabled and then disabled. After the router-id change, mpls ldp nsr must be reconfigured in order to encounter this issue.

  Workaround: Reload the standby RP.

- CSCuh44476

  Symptom: After an SSO, some VCs are not displayed for certain neighbors.

  Conditions: This symptom occurs after an SSO on a box which has VFIs with autodiscovery BGP and BGP signalling with more than two remote PEs.

  Workaround: There is no workaround.

- CSCuh46849

  Symptom: A Cisco ASR 1000 router may display the following log with a traceback:

  ```
  SCHED-3-UNEXPECTEDEVENT Process received unknown event (maj 80, min 0).
  ```

  Conditions: The conditions are unknown.

  Workaround: Reload the router.

- CSCuh47183

  Symptom: This message will be seen followed by a “%Software forced reload”:

  ```
  %SYS-6-STACKLOW: Stack for process EEM Callback Thread running low, 0/9000
  ```

  Conditions: EEM (Embedded Event Manager) configuration necessary.

  Workaround: Avoid using EEM applet.

- CSCuh48666

  Symptom: Router crashes and reloads with dynamic EID scaling.

  Conditions: The symptom is observed with dynamic EID scaling.

  Workaround: There is no workaround.

- CSCuh48840

  Symptom: A Cisco router crashes.

  Conditions: This symptom is observed under the following conditions:

  a. The sup-bootdisk is formatted and copied with a big size file (example: copy a Cisco 7600 image file of an approximate size of 180M).

b. Reload the box and during bootup try to write the file onto the sup-bootdisk (SEA write sea_log.dat 32M bytes).

c. The issue is reproduced.

d. When the issue seen, check the sea_log.dat always with 0 byte

e. No matter where (disk0 or bootdisk) to load image.

f. No matter sea log disk to sup-bootdisk or disk0:. I reproduced the issue with "logg sys disk disk0:" configuration.

SEA is calling IFS API to create sea_log.dat, looks like IFS creating file hungs SP.

```
sea_log.c : sea_log_init_file() -> ifs_open() -> sea_zero_log() -> ifs_lseek() ->
ifs_write()
```

Workaround: There is no workaround.

- CSCuh51367

  Symptom: An alignment traceback is seen in the L4F code.

  Conditions: This symptom occurs when traffic from HTTP/HTTPS goes through Scansafe+l4f.

  Workaround: There is no workaround.

- CSCuh51897

  Symptom: LC crashes with following error messages:

```
Jun 11 03:55:05.641: %SYS-DFC2-2-NOBLOCK: printf with blocking disabled. -Process=
''NDE - IPV6'', ipl= 7, pid= 165 Jun 11 03:55:44.165: %CPU_MONITOR-SP-6-NOT_HEARD:
CPU_MONITOR messages have not been heard for 31 seconds [2/0] Jun 11 03:56:44.761:
%CPU_MONITOR-SP-6-NOT_HEARD: CPU_MONITOR messages have not been heard for 91 seconds
[2/0] Jun 11 03:57:02.441: %XDR-6-XDRIPCNOTIFY: Message not sent to slot 2/0 (2)
because of IPC error timeout. Disabling linecard. (Expected during linecard OIR) Jun
11 03:57:14.761: %CPU_MONITOR-SP-6-NOT_HEARD: CPU_MONITOR messages have not been heard
for 121 seconds [2/0] Jun 11 03:58:14.762: %CPU_MONITOR-SP-3-TIMED_OUT: CPU_MONITOR
messages have failed, resetting module [2/0] Jun 11 03:58:14.826:
%C7600_PWR-SP-4-DISABLED: power to module in slot 2 set off (Heartbeat Messages Not
Received From Module)
```

  Conditions: This symptom occurs when IPv6 NetFlow is enabled on the device.

  Workaround: Disable IPv6 NetFlow.

- CSCuh53544

  Symptom: OSPF ABR router does not flush type-4 ASBR summary LSA after NSR swithover if the connection to ASBR is lost during NSR switchover.

  Conditions: This symptom is occurs when the VSS system acts as ABR and loses connection to an ASBR during NSR switchover. This configuration is not recommended and Layer 3 topology should not change during the switchover.

  Workaround: Clear "ip ospf proc".

- CSCuh56327

  Symptom: IP SLA responder crash occurs on Cisco ASR 1002 router in Cisco IOS Release 15.2(4)S, Cisco IOS Release 15.2(4)S1, and Cisco IOS Release 15.2(4)S2.

  Conditions: This symptom occurs when ip sla udp jitter with precision microseconds, udp jitter with milliseconds and udp echo are configured on the sender device with the same destination port on Cisco ASR 1002 router.

Workaround: Use different destination ports for udp-echo and udp jitter with millisecond precision than udp jitter with microsecond and optimize timestamp.

- CSCuh56385

  Symptom: Very slow propagation of data across a network of SAF forwarders after a fail over condition is observed. More than two SAF forwarders are required to observe this defect.

  Conditions: This symptom occurs when there are more than two SAF forwarders in the network. After a fail over condition and the clients initiate advertising patterns into the standby forwarder, the propagation of these advertisements via update messages to the SAF peers can experience a 5 second inter-service advertisement delay.

  Workaround: There is no workaround. Once the forwarder that suffered the fail over condition returns and establishes its neighbor relationships with its peers, the forwarders will update quickly.

- CSCuh57839

  Symptom: Clock quality level stuck and QL-DNU and not synchronized with the quality level of the clock source.

  Conditions: This occurs when a synchronization interface that was previously down comes back up.

  Workaround: There is no workaround.

- CSCuh59070

  Symptom: Tunnel or Vtemplate interface type becomes P2P or Traffic Engineering type, so the class is different, so some of the operation can not be perform because of the wrong type.

  Conditions: This symptom is observed when Restful API uses Onep python SDK.

  Workaround: There is no workaround.

- CSCuh62266

  Symptom: During normal operation, the Cisco ASR 1000 router may crash after repeated SNMP related watchdog errors.

  ```
  Jun 15 2013 10:43:30.325: %SCHED-0-WATCHDOG: Scheduler running for a long time, more
  than the maximum configured (120) secs. -Traceback= 1#6d024ee43b83b4f5539a076aa2e8d467
  :10000000+56A5348 :10000000+20F7D54 :10000000+2513910 :10000000+20F807C
  :10000000+20EBE84 :10000000+2119BA8 :10000000+20EBE84 :10000000+2106C24
  :10000000+20EBE84 :10000000+213C9E8 :10000000+213CC34 :10000000+225B748
  :10000000+222941C :10000000+2214314 :10000000+224812C -Traceback=
  1#6d024ee43b83b4f5539a076aa2e8d467 :10000000+21416F0 :10000000+2513910
  :10000000+20F807C :10000000+20EBE84 :10000000+2119BA8 :10000000+20EBE84
  :10000000+2106C24 :10000000+20EBE84 :10000000+213C9E8 :10000000+213CC34
  :10000000+225B748 :10000000+222941C :10000000+2214314 :10000000+224812C
  ```

  Conditions: This symptom occurs while trying to obtain data from IP SLAs Path-Echo (rttMonStatsCollectTable) by SNMP polling operation.

  Workaround: There is no workaround other than to disable SNMP configuration from the router.

  More Info: This crash occurred in a customer environment and device with a particular version of the software (Cisco IOS Release 15.1(2)S2). No other similar issue has been identified so far.

- CSCuh63997

  Symptom: Router crashes when service-policy is installed on the interface.

  Conditions: The symptom is observed with service-policies having random-detect aggregate configuration.

Workaround: Use non-aggregate random-detect for WRED configurations. If the platform supports only aggregate random-detect, then there cannot be a workaround other than not using the WRED configuration altogether.

- CSCuh68693

  Symptom: RP crashes [active RP, in the case of a dual RP setup] when the **show otv isis database standard detail** command is used to check details related to MAC addresses.

  Conditions: This symptom occurs in valid OTV configurations (OTV state is UP and AED State is Yes).

  Workaround: There is no workaround.

- CSCuh70868

  Symptom: VPN prefixes are not advertised to more than one eBGP ASBRs even though the filters are received from them.

  Conditions: This symptom occurs when an RT filter is configured between the eBGP ASBRs and the filter allows the VPN prefixes to be sent only to the neighbor from where the best path is received. All the other ASBRs do not receive the VPN prefixes even though maximum-path <> is configured.

  Workaround: There is no workaround.

  More Info: Remove route-target filtering between the eBGP ASBRs.

- CSCuh72031

  Symptom: System might crash while trying to enter into exec mode through VTY.

  Conditions: IPv4 TACACS server configured for login authentication with send-nat-address option.

  Workaround: Remove send-nat-address option.

- CSCuh74735

  Symptom: Intra mag roaming via DHCP request.

  Conditions: This symptom is observed under no specific conditions.

  Workaround: There is no workaround.

- CSCuh74822

  Symptom: Config or unconfig causes MAG configuration to fail with MCSA.

  Conditions: The conditions for this symptom are unknown.

  Workaround: Perform a reload.

- CSCuh75315

  Symptom: RP crash occurs while removing NAT configurations.

  Conditions: This symptom occurs while removing 4k NAT session configurations from UUT.

  Workaround: There is no workaround.

- CSCuh76617

  Symptom: With MVPN BGP C-route signalling, some multicast states in the VRF might remain even when C-route state is withdrawn from BGP.

  Conditions: This symptom occurs when all the BGP sessions on the PE go down (for example, manual clearing of BGP by using the **clear ip bgp** command).

  Workaround: There is no workaround.

- CSCuh78003

  Symptom: Complete loss of network traffic.

  Conditions: This symptom occurs when all xconnects are cleared on a device where pseudowire redundancy is configured and no other network event occurred before this trigger.

  Workaround: Remove and reconfigure the xconnects.

- CSCuh78173

  Symptom: The EVC value shows as I state after a change from MPLS IP to PC MPLS IP.

  Conditions: This symptom occurs when mpls ip is changed from interface to PC.

  Workaround: Remove EVC configuration.

- CSCuh80492

  Symptom: The system crashes and it causes a reload. Messages that can be seen on the console indicate there is a “NULL pointer dereference”. For example:

  ```
  BUG: unable to handle kernel NULL pointer dereference
  ```

  This is followed by a stack trace.

  Conditions: This symptom occurs due to lack of proper locking semantics on the variables controlling the IPC namespace.This crash is unlikely to occur in normal situations. The user will need to have shell access and then access a task file under /proc (for example: /proc/29208/ns/ipc) which gives stats on the IPC namespace.

  Workaround: There is no workaround.

- CSCuh86464

  Symptom: SSS message chunk memory leak.

  Conditions: This symptom occurs when the **clear subscriber session all** command is used while scale sessions are being initiated.

  Workaround: There is no workaround.

- CSCuh89168

  Symptom: The standby resets in a continuous loop.

  Conditions: This symptom occurs on insertion of a new standby RSP with a different license than the one on the active RSP.

  Workaround: There is no workaround.

- CSCuh90094

  Symptom: %MEDIATRACE-3-R_SNMP_COMM_STR_MISSING message is displayed, which suggests that the **snmp-server community public ro** command should be executed. But this command has already been executed on the configuration.

  Conditions: This symptom occurs when there is some access-limit mechanism in place on the SNMP configuration, such as the **snmp mib community-map** command.

  Workaround: Ensure that the first community to appear in the configuration has no access-limit mechanism, or it has one that allows the router to query itself using SNMP.

- CSCuh91225

  Symptom: A router crashes at pki_import_trustpool_bundle.

Conditions: The call-home reporting command will enable smart callhome using HTTPS and send an inventory message to register for smart callhome. If the certificate which is required by HTTPS does not exist in the device, it will try to download it which causes the crash.

Workaround: There is no workaround.

- CSCuh91645

  Symptom: WS-SUP720-3B crashes while receiving DHCP packets.

  Conditions: This symptom occurs with the **ip dhcp relay information policy-action encapsulate** command.

  Workaround 1. Use the **ip dhcp relay information policy-action replace** command.

  Workaround 2. Use the **no ip dhcp relay information trusted**command.

- CSCuh92051

  Symptom: Per user v4ACL HA replication broken in mcpdev.

  Conditions: This symptom occurs when IPv4 and IPv6 profiles for single users are applied and the v4 profile per user data is not synchronized to the standy.

  Workaround: There is no workaround.

- CSCuh94035

  Symptom: A watchdog timeout crash occurs.

  Conditions: This symptom occurs when DMVPN and IPv4/IPv6 EIGRP are configured. A crash occurs while DUAL is updating the EIGRP topology table.

  Workaround: There is no workaround.

- CSCuh94799

  Symptom: When a Port-channel interface with a carrier delay of 0 milliseconds and one or more service instances configured is removed, an unexpected process termination occurs.

  Conditions: The issue will be seen only when there is both carrier delay of ms 0 configuration and service instance configuration under a Port channel interface, and that Port-channel interface is removed.

  Workaround: There are several work arounds:

  1. Remove the service instance(s) from the Port-channel interface before deleting the interface.
  2. Remove the carrier delay from the Port-channel before deleting the interface.
  3. Configure a non-zero carrier delay instead of a 0 carrier delay.
  4. Don't use carrier-delay on port-channel interfaces in conjunction with service instances. Instead use carrier-delay on port-channel member interfaces. The use of "lacp fast-switchover" on the port-channel interface can also help to avoid the need for carrier-delay in cases where redundant LACP member links are in use.

- CSCuh94879

  Symptom: Cisco IOS crashes after configuring the MHBFD template and map.

  Conditions: This symptom occurs when the following are configured:

  1. bfd-template multi-hop New-Temp
  2. no authentication sha keychain mhop-key-abc
  3. bfd map ipv4 4.4.4.4/32 1.1.1.1/32 New-Temp

  Workaround: There is no workaround.

- CSCuh95503

  Symptom: Iosd crashes while removing match criteria from class map.

  Conditions: This symptom occurs when multiple filters are matched in the same statement and any one of them is deleted.

  Workaround: There is no workaround.

- CSCuh97129

  Symptom: Losing EIGRP Extended communities on BGP L3VPN route.

  Conditions: This symptom is observed when Remote PE-CE connection is brought down and only backup EIGRP path remains in the BGP table.

  Workaround: Clearing the problem route in the VRF will resolve the issue.

- CSCuh97838

  Symptom: Increased CPU Interrupt utilization due to process switching of packets.

  Conditions: This symptom occurs when CESoUDP is configured on the remote PE but is not configured on the local 901.

  Workaround: There are two workarounds:

  1. Configure the CESoUDP on the local 901 before configuring it on the remote PE.

  Or

  2. Remove the CESoUDP from the remote PE.

- CSCuh98997

  Symptom: L2VPN for Route reflector client in peer-policy or peer-group configuration does not work to reflect RFC 6074 update or RFC 4761 updates.

  Conditions: This symptom occurs in he following scenarios:

  1. Template peer-policy is configured with route-reflector-client, or peer-group is configured with route-reflector-client.
  2. Together with prefix-length-size 2 are configured for one or more neighbors.
  3. With no neighbor in bgp l2vpn vpls address-family configuring route-reflector-client explicitly.

  Workaround:Configure a neighbor in bgp l2vpn vpls address-family to have route-reflector-client explicitly.

- CSCui03965

  Symptom: Standby RP keeps on booting after an ISSU upgrade of the standby RP.

  Conditions: The symptom is observed after an ISSU upgrade of the standby RP.

  Workaround: There is no workaround.

- CSCui04262

  Symptom: An error syslog is seen on ASR1K BRAS running XE352.P3 Standby-RP, showing QOS service-policy installation failures:

```
1. Jun 13 14:43:55.323 CEST: %QOS-6-POLICY_INST_FAILED: Service policy installation
failed
2. Jun 13 14:47:10.725 CEST: %QOS-3-INDEX_DELETE: class-group unable to remove index
00B6AA60
3. Jun 13 14:47:10.726 CEST: %QOS-3-UNASSIGNED: A CLASS_REMOVE event resulted in an
(un)assigned index for class-group
target-input-parent$class-default$IPBSA>ci=3#qu=3#qd=4#co=4#pu=police#ru=200K#pd=polic
e#rd=300K<_IN$class-default 4. Jun 13 14:47:10.727 CEST: %QOS-6-RELOAD: Index removal
```

```
failed, reloading self Symptom: An error syslog is seen on ASR1K BRAS running XE352.P3
Standby-RP, showing QOS service-policy installation failures: 1. Jun 13 14:43:55.323
CEST: %QOS-6-POLICY_INST_FAILED: Service policy installation failed 2. Jun 13
14:47:10.725 CEST: %QOS-3-INDEX_DELETE: class-group unable to remove index 00B6AA60 3.
Jun 13 14:47:10.726 CEST: %QOS-3-UNASSIGNED: A CLASS_REMOVE event resulted in an
(un)assigned index for class-group
target-input-parent$class-default$IPBSA>ci=3#qu=3#qd=4#co=4#pu=police#ru=200K#pd=polic
e#rd=300K<_IN$class-default 4. Jun 13 14:47:10.727 CEST: %QOS-6-RELOAD: Index removal
failed, reloading self
```

Conditions: This symptom is observed when on Cisco ASR1000 BRAS, running Cisco IOS Release XE352.P3, Version 15.2(1)S2, CUST-SPECIAL:V152_1_S2_CSCUA32331_4. When churning PPPoE sessions with 2 unique ISG/Shell map services per session, and after a manual RP Failover is done, after a while the error will be seen.

Workaround: There is no workaround.

- CSCui04530

  Symptom: Upon FPD upgrade, you get this error on Cisco IOS c7600 switch:

  ```
  ! %FPD_MGMT-3-BUNDLE_EXTRACT_ERROR: Cannot extract the ssc-600-fpd.bndl bundle from
  sup-bootdisk:c7600-fpd-pkg.151kg - The required bundle is not in the package file.
  Please make sure that you have the right FPD image package file. % Cannot get the
  required data from the indicated file, please verify that you have a valid file and
  entered a valid URL. !
  ```

  Conditions: This symptom is observed under the following conditions:

  ```
  IOS: c7600s72033-advipservicesk9-mz.122-33.SRB3
  CARDS: WS-SSC-600 WS-IPSEC-3
  CLI: upgrade hw-module slot x fpd file sup-bootdisk:c7600-fpd-pkg.151-3.S2.pkg
  ```

  Workaround: Upgrade to FPD image that includes corresponding *.bndl image.

- CSCui06930

  Symptom: Some VLAN VCs which are associated with Service Instance configuration via a bridge domain may not be brought up under some timing conditions.

  Conditions: Upon startup with saved configuration where a VC is associated with an EFP via bridge domain configuration, it is possible that the VC may not be brought up even where the EFP (service Instance) is itself up.

  Workaround: Perform a shut/no shut of the VLAN interface.

- CSCui07997

  Symptom: Route over OSPFv2 sham-link shows two next hop.

  Conditions: This symptom is observed when the route entry is ECMP route between the sham-link and another path.

  Workaround: Break ECMP by adjusting the OSPF cost.

- CSCui09196

  Symptom: During smoke testing using the latest mcp_dev image on a Cisco IOS 7600 series router running Cisco IOS Release 15.4(00.01)S, the router crashes during configuration.

  Conditions: This symptom occurs when a crash occurs in RSP.

  Workaround: There is no workaround.

- CSCui14692

  Symptom: Crash on C819G running 152-4.M1 due to memory corruption at vm_xif_malloc_bounded_stub.

  Conditions: This condition is seen due to recursive function call of fib code, NHRP, IP SLA etc. However, these might not be the only trigger.

  Workaround: There is no workaround.

- CSCui21030

  Symptom: A vulnerability in OSPF implementation of Cisco IOS and Cisco IOS XE could allow an unauthenticated, adjacent attacker to cause a reload of the affected device.

  The vulnerability is due to improper parsing of certain options in OSPF LSA type 11 packets. An attacker could exploit this vulnerability by sending LSA type 11 OSPF packet with unusual options set. An exploit could allow the attacker to cause a reload of the affected device.

  Conditions: This symptom occurs while receiving a bad RI opaque LSA with some unusual options.

  Workaround: There is no workaround.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5.7/4.7: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:A/AC:M/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C

  CVE ID CVE-2013-5527 has been assigned to document this issue.

  Additional details about the vulnerability described here can be found at: http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2013-5527

  Additional information on Cisco’s security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html.

- CSCui21061

  Symptom: Multicast stops working when CDP is disabled on a physical interface that is part of a port-channel.

  Conditions: This issue is seen when “no cdp enable” is issued on the physical interface. It is not seen if CDP is disabled globally, or if there is no port-channel configured.

  Workaround: Disable CDP globally or use a configuration that does not involve a port-channel.

- CSCui24744

  Symptom: An iosd crash is seen.

  Conditions: This symptom occurs on removing **bfd-template single-hop sw-no-echo-sha1** configuration.

  Workaround: There is no workaround.

- CSCui25696

  Symptom: A Cisco ASR 1002-X router experiences a watchdog reset due to a kernel core dump triggered by a possible divide-by-zero condition.

  Conditions: This symptom can occur under any condition.

  Workaround: There is no workaround.

- CSCui26581

  Symptom: A small memory leak is seen when accessing certain parts of PTP MIB.

  Conditions: This symptom occurs when the following OIDs in the PTP MIB are accessed:

```
cPtpClockRunningPacketsSent: 1.3.6.1.4.1.9.9.760.1.2.4.1.5
cPtpClockRunningPacketsReceived: 1.3.6.1.4.1.9.9.760.1.2.4.1.6
cPtpClockPortRunningPacketsReceived: 1.3.6.1.4.1.9.9.760.1.2.9.1.13
cPtpClockPortRunningPacketsSent: 1.3.6.1.4.1.9.9.760.1.2.9.1.14
cPtpClockPortAssociatePacketsSent: 1.3.6.1.4.1.9.9.760.1.2.11.1.8
cPtpClockPortAssociatePacketsReceived: 1.3.6.1.4.1.9.9.760.1.2.11.1.9
cPtpClockPortAssociateInErrors: 1.3.6.1.4.1.9.9.760.1.2.11.1.10,
cPtpClockPortAssociateOutErrors: 1.3.6.1.4.1.9.9.760.1.2.11.1.11
```

Workaround: Exclude the above OIDs

- CSCui28312

  Symptom: A Cisco IOS router crashes.

  Conditions: This symptom occurs in rare cases on images supporting HA with IPv6 BSR configured, when C-RPs are configured, and then unconfigured shortly after.

  Workaround: There is no workaround.

- CSCui29499

  Symptom: ISIS goes into INIT state.

  Conditions: BFD flap leads to ISIS adjacency not coming up if the following conditions are true:

  1. In P2P mode only
  2. When local node supports RFC6213 and its remote neighbor does not support RFC6213
  3. The P2P link is down and adjacency is deleted on the remote neighbor and up again before the adjacency hold down timer expires on the local node that has the RFC6213 support

  Workaround: Any of the following work arounds will work.

  – Remove BFD on 903, wait for ISIS to come up and configure BFD again

  – Shut and no shut the interface on the local node with RFC6213

  – Not to use P2P link at all

  More Info: Deviation not experienced when EIGRP or OSPF routing protocols were running over the same link as ISIS in testing.

- CSCui30036

  Symptom: Cisco ASR 1001 IDC maverick SPA(ASR1001-IDC-8XT1E1) will not bootup.

  Conditions: This issue is observed with latest Cisco IOS Release XE3.10 and mcp_dev image.

  Workaround: There is no workaround. Use image prior to Cisco IOS Release XE3.10.

- CSCui32105

  Symptom: In rare occasions the standby RP on a dual RP system may crash after performing a switchover.

  Conditions: This symptom occurs when an invalid message is sent from the RP to the RRP.

  Workaround: There is no workaround.

- CSCui33454

  Symptom: Unidirectional traffic flow is observed for PFC based EoMPLS PW due to lost FIB entries in hardware. Receive counter under VC statistics does not increment on one side of PW.

  Counter for VC statistics in “receive” direction does not increment, only send counter increases.

  Conditions: This symptom is observed under the following conditions:

  – EoMPLS PW provisioned on PFC/DFC based linecard

  - The issue is triggered with FIB changes toward the xconnect neighbor peer

  Workaround 1. “Soft”" workaround - Remove and configure back the affected xconnect.

  or “hard” WA in case soft does not help

  Workaround 2. “Hard” workaround - Linecard reload in case of DFC based AC linecard - Supervisor reload in case of non-DFC based AC linecard.

- CSCui39527

  Symptom: Standby RP crashes during VRF transfer.

  Conditions: This symptom occurs on a standby RP with EoGRE tunnel+HA configuration.

  Workaround: There is no workaround.

- CSCui43534

  Symptom: 5760 Wireless LAN crashes during CWA client association when ISE is unreachable.

  Conditions: This symptom is observed when ISE becomes unreachable. Client associates to WLAN with CWA support.

  Workaround:

  1. Configure backup radius.
  2. Remove the MAC filter.

- CSCui44972

  Symptom: A small memory leak is observed while accessing certain parts of the PTP MIB .

  Conditions: This symptom occurs while accessing cPtpClockPortDSName when a boundary clock is configured and there is no license for the boundary clock.

  Workaround: Avoid accessing cPtpClockPortDSName (OID: 1.3.6.1.4.1.9.9.760.1.2.8.1.5).

- CSCui46390

  Symptom: Multiple paths with different VBS or LB for an RFC 4761 prefix is not considered as the same prefix. This causes an interop issue with Cisco IOS XR software and BGP routers of other vendors.

  Conditions: This symptom occurs when:

  1. The **neighbor suppress-signaling-protocol ldp** option is enabled.
  2. Multiple paths exist with different VBS/LB but same RD/VEID/VBO.

  Workaround: There is no workaround.

- CSCui46593

  Symptom: CPU hog crash due to Mwheel Process.

  Conditions: This symptom is observed in a normal operation.

  Workaround: There is no workaround.

- CSCui47248

  Symptom: A traceback is observed.

  Conditions: This symptom occurs when **config replace <clean file>** is done and the replaced configuration file has disabled IP routing but has IPv4 static routes configured.

  Workaround: There is no workaround.

- CSCui47602

  Symptom: Traces at IDMGR-3-INVALID_ID when queried for mplsTunnelTable MIB.

  Conditions: This symptom occurs when there is a GETONE SNMP query for non-existing mplsTunnelTable entries.

  Workaround: Avoid using GETONE SNMP query for non-existing objects. Use GETNEXT queries instead of GETONE whenever possible.

- CSCui47732

  Symptom: When Router 1 and Router 2 have full OSPF adjacency, and interface loopback 0 on Router 2 is not an OSPF interface, Router 1 cannot reach Router 2's loopback 0. MPLS LDP is configured using both Router 1 and Router 2 loopback 0 as router-id, so LDP neighbor cannot be formed between them. When **mpls ldp sync** is configured under **router ospf**, Router 2 is generating max-metric router LSAs to Router 1, which is expected. However, when **no mpls ldp sync** is configured, OSPF doesn't rebuild router LSA and still sends router LSA with metric 65535.

  Conditions: This symptom occurs when **mpls ldp sync** cannot be configured due to LDP being in down state.

  Workaround: Use the **flap interface** or **clear ospf process** command, followed by a router LSA refresh.

- CSCui49185

  Symptom: On a Cisco IOS ASR 1002x series router running Cisco IOS Release 15.4(01)S, a crash occurs.

  Conditions: This symptom occurs when MLDP over GRE is configured, with paths being added and removed. The counter of the number of paths in a CEF path list is not updated correctly. When they wrap at 256 this may cause a crash. The problem occurs when a path is removed without decrementing the counter properly. The problem is observed when a path is added/removed from a path list 256 times.

  Workaround: Do not modify paths using the method described.

- CSCui53213

  Symptom: Traffic forwards through the VC even when the EVC is in a shut state.

  Conditions: This symptom occurs in scalable EoMPLS.

  Workaround: There is no workaround.

- CSCui53428

  Symptom: Forwarding state is not preserved on the Cisco ASR 9000 series router after an SSO in the Cisco ASR 903 router.

  Conditions: This symptom occurs when an SSO is performed on the Cisco ASR 903 router.

  Workaround: There is no workaround.

- CSCui61928

  Symptom: The chunk mgr process consumes a lot of memory and does not free it up. This may lead to insufficient processor memory.

  Conditions: This symptom occurs when a static BFD session constantly flaps. Dynamic BFD sessions are not affected.

  Workaround: This situation can be avoided by:

  1. Preventing a constantly flapping static BFD session.
  2. Removing the BFD configuration.

3. Configuring BFD dampening (in the BFD template mode).

- CSCui62441

  Symptom: Complete traffic drop for few seconds is seen after few minutes of performing SSO switchover.

  Conditions: This symptom occurs only after a few minutes of performing an SSO switchover.

  Workaround: There is no workaround.

- CSCui67308

  Symptom: Cisco IOS Router constantly crashes after enabling TE tunnel over BDI interface.

  Conditions: This symptom is observed when TE tunnel is exits a BDI interface. This is not a supported design.

  Workaround: Use physical interface for TE tunnels.

- CSCui69873

  Symptom: A crash occurs in ospfv3_db_scope_str().

  Conditions: This symptom is observed when you enable **debug ospfv3 lsdb**.

  Workaround: There is no workaround.

- CSCui74609

  Symptom: After a RSP switchover the backup pseudowire state is down and never recovers to standby state.

  Conditions: This symptom occurs on CEM circuits in a SAToP environment after a SSO switchover.

  Workaround: There is no workaround.

- CSCui76564

  Symptom: A roaming mobile customer (example: iPASS, Boingo etc.) logs on via a Web-Portal-Page and the ISG doesn't send in the radius accounting-request packet from the V-Cookie to the Radius Server.

  Conditions: This symptom occurs depending on the ISG setup. In this case L & V Cookie must be sent in accounting-request from the ISG to the AAA Server.

  Workaround: There is no workaround.

- CSCui82259

  Symptom: Cisco IOS router reloads, giving a traceback.

  Conditions: This symptom occurs when the failover is initiated from the primary link (GX) to the secondary link (BGAN) or from BGAN to GX for multiple VRFs at the same time, using an EEM script.

  Workaround: There is no workaround.

- CSCui82757

  Symptom: Session query responses in lite sessions have inconsistent calling-station-ID behavior.

  Conditions: This symptom occurs when:

  1. Walkby feature is enabled with L4R & PBHK features applied to lite session.
  2. Session query is sent to ISG.

  Workaround: Do not use calling-station-ID.

- CSCui85019

  Symptom: When the command **show xconnect** is entered, it may result in a memory leak. This can be observed by entering the command **show memory debug leaks chunks** and seeing entries like this:

  ```
  router#show memory debug leaks chunks Adding blocks for GD...
  I/O memory
  Address Size Alloc_pc PID Alloc-Proc Name
  Chunk Elements:
  AllocPC Address Size Parent Name
  Processor memory
  Address Size Alloc_pc PID Alloc-Proc Name AA3F8B4 2348 6D0B528 97 Exec
  PW/UDP VC event trace
  ```

  Conditions: This symptom is observed when one or more xconnects are configured with UDP encapsulation.

  Workaround: There is no workaround.

- CSCui87915

  Symptom: The VC is not going down after the access interface is down.

  Conditions: This symptom occurs in scalable eompls under port-channel and the member link is shut down.

  Workaround: The EFPs under the member link can be reconfigured once the member link is down.

- CSCui89069

  Symptom: An ISIS flap is observed on performing SSO.

  Conditions: This symptom occurs when **nsf ietf** is configured and one or more loopbacks are configured as passive interfaces.

  Workaround 1. Use **nsf cisco**.

  Workaround 2. Continue to use **nsf ietf** but configure **ip router isis <process_name>** on the loopback interfaces.

- CSCui90811

  Symptom: While running the Cisco IOS 15.3S release and Cisco IOS 15.4S release software for the L2VPN pseudowire redundancy feature on a Cisco router, the traffic is dropped when the primary pseudowire becomes active.

  Conditions: Initially the primary pseudowire is down due to either a local or a remote core-facing interface being shutdown. The backup pseudowire is active and traffic flows through the backup pseudowire. Later, when the backup pseudowire is down, the primary pseudowire is brought up and becomes active and traffic is not able to flow through primary pseudowire and is dropped.

  Workaround: There is no workaround.

- CSCui95398

  Symptom: Configuration CLI to enable/disable “diag false alarm detection”.

  Conditions: As of now this can be used to control the result of sprp_inband ping failure.

  Workaround:Nil

  More Info: “platform diagnostic false-alarm-detection” is the CLI.

- CSCui99031

  Symptom: In a pair of Cisco 7609-S routers running c7600rsp72043-advipservicesk9-mz.151-3.S5.bin IOS, phase 1 fails to establish due to a “signature invalid!” error when rsa-sig is used for phase 1 authentication.

  Conditions: This symptom occurs under the following conditions:

  – rsa-sig is used for phase 1 authentication

  – site to site tunnel

  Workaround: Use PSK instead of PKI.

- CSCuj00746

  Symptom: On performing an upgrade from 9.512 to 9.523, there is a label allocation failure in VPWS circuits as they are trying to utilize the labels that are already used by the VPLS circuits that are present in the database.

  Conditions: This symptom occurs when both VPWS and VPLS circuits are configured on the same node before upgrading.

  Workaround: Removing the VPLS circuit brings up the VPWS circuits. Re-configuring the VPLS circuit is also successful with a different local label assigned.

- CSCuj04178

  Symptom: A crash occurs at vpdn_apply_vpdn_template_pptp.

  Conditions: The conditions for this symptom are unknown.

  Workaround: There is no workaround.

- CSCuj06347

  Symptom: Cisco IOS and Cisco NX-OS software contain a vulnerability that could allow an authenticated, local attacker to poison the LISP map cache on the router configured as an Ingress Tunnel Router (ITR).

  Conditions: This symptom occurs when an attacker has a privilege 0 local access to the ITR and executes **lig** commands.

  Workaround:

  1. Configure **privilege exec level 1 lig<nCmdBold>, to prevent privilege level 0 users from executing the lig** command.

  2. Use separate VRFs for the EID and RLOC spaces, assuming the attacker does not have access to the RLOC case.

  3. Using GETVPN or other crypto in the RLOC space may mitigate against this, but not in the common deployment scenario, where crypto maps are applied to the LISP0 interface.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 1.5/1.4:

  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:L/AC:M/Au:S/C:N/I:P/A:N/E:F/RL:W/RC:C

  No CVE ID has been assigned to this issue.

  Additional information on Cisco's security vulnerability policy can be found at the following URL:

  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCuj16742

  Symptom: In a pseudowire redundancy configuration, packets may fail to flow even though the xconnect virtual circuit appears to be up.

  Conditions: This symptom has been observed when the xconnect is re-provisioned while the primary pseudowire is down and the backup pseudowire is up. The issue has only been observed on Circuit Emulation (CEM) attachment circuits, but it is possible other attachment circuit types may be affected as well.

  Workaround: Completely unconfigure the xconnect and then reconfigure it.

- CSCuj17482

  Symptom: On a device running low on memory, an EFP is attempted to be deleted, but fails due to lack of memory. The second attempt at removing that same EFP causes the router to restart.

  Conditions: This symptom occurs when the a lot of configuration has been applied to the device, causing high memory usage.

  Workaround: Do not over-configure the device.

- CSCuj22189

  Symptom: On a Cisco ASR series router, a crash occurs when **mpls ip** is added under the interface.

  Conditions: This symptom occurs when the hidden command **snmp-server hc poll** is already configured.

  Workaround: Ensure that the hidden command **snmp-server hc poll** has not been configured.

- CSCuj23896

  Symptom: The Cisco Catalyst 4500-X Series Switches crash while running wireshark.

  Conditions: This symptom occurs when the following conditions are met:

  1. Capture is started with ipv4/ipv6/mac filter (using match keyword).
  2. Capture is stopped and modified to use different filter.
  3. Capture is started again.

  Workaround: Avoid using **monitor capture <name> match <ipv4/ipv6/mac>.** Use an ACL/class-map which is created from the configuration mode.

- CSCuj30702

  Symptom: This bug is specific to port channel sub interface configuration in ES+ card. This bug is not relevant to any other port channel configuration in ES+, that is, EVC/Bridge-Domain over PoCH sub-int etc, and other card types, such as ES20/ LAN cards are free from this bug. Any type of IP communication on port channel sub interfaces in ES+ cards fail. Such an issue is seen only with port channel sub interfaces on ES+ and not seen with port channel main interfaces.

  Conditions: This symptom will only be seen with images where the fix of CSCuh40617 is integrated.

  Workaround: The connections will work fine if it is moved to the main interface or by using EVC BD configurations.

- CSCuj31090

  Symptom: When L2TPv3-based pseudowire is configured between two PE routers and different VLAN ids are used on the ACs on both sides, ES+ on egress PE does not rewrite a dot1q VLAN tag when sending a frame toward CE.

  Conditions: This symptom occurs when: 1. Both ACs are Ethernet VLAN type. 2. Different dot1q tag is used on both ACs.

Workaround: Configure the same dot1q tag for the ACs on both PEs.

- CSCuj31151

  Symptom: If an impedance option is specified for an external clock in the **network-clock input-source** configuration, other configuration (such as hold-off or wait-to-restore) may fail to be applied.

  Conditions: This symptom is seen when using external clock inputs with an impedance option specified.

  Workaround: It may be possible to achieve the desired behaviour using global configuration (for example global hold-off or wait-to-restore configuration), if not, there is no workaround.

- CSCuj44262

  Symptom: The 10GigE port is not up even though the XFP transmits laser.

  Conditions: This symptom occurs under the following conditions:

  – Using SPA-1X10GE-L-V2 and XFP-10G-MM-SR.

  – Leaving the interface in shutdown state for a long time (over 6hrs).

  Workaround: Reload the SPA.

- CSCuj47238

  Symptom: There is a difference in the Y1731 probe within **show ip sla statistics**.

  Conditions: This symptom is seen in the Cisco 7600 series routers.

```
service instance 400 ethernet evc1000 description -- EVC Cliente BUSINESS---
encapsulation dot1q 400 second-dot1q 100 <==HERE rewrite ingress tag pop 2 symmetric
<==HERE xconnect 172.16.12.6 1000 encapsulation mpls cfm mep domain OPM mpid 2
mdr-rm01#sh ip sla statistics 1 IPSLAs Latest Operation Statistics
IPSLA operation id: 1 Delay Statistics for Y1731 Operation 1 Type of operation: Y1731
Delay Measurement Latest operation start time: 12:06:21.041 CET Wed Sep 11 2013 Latest
operation return code: OK Distribution Statistics:
Interval Start time: 12:06:21.041 CET Wed Sep 11 2013 Elapsed time: 50 seconds Number
of measurements initiated: 44 <== HERE Number of measurements completed: 32 <== HERE
Flag: OK
```

  Workaround: There is no workaround.

- CSCuj48676

  Symptom: Following MIBs have wrong values reported:

```
cfmConditionsProfile cfmAlarmHistoryConditionsProfile cfmFlowMetricConditionsProfile
cfmFlowMonitorConditionsProfile
```

  Conditions: This symptom is observed when Performance Monitor feature is configured with threshold-crossing-alarms.

  Workaround: There is no workaround.

- CSCuj50401

  Symptom: An ND cache entry is not created for an ISIS IPv6 neighbour when an ISIS adjacency is established.

  Conditions: This symptom occurs when ISIS IPv6 is configured and has an established adjacency with the neighboring node.

  Workaround: There is no workaround.

Further Problem Description: The impact is negligible because the fix is an optimization. As an optimization a new entry is created in the ND cache when a new ISIS adjacency is established. The defect means that an ND cache entry is not created when an adjacency is established, causing slight delays when data starts flowing. An entry will be created normally when data flows to the neighbor.

- CSCuj57367

  Symptom: A 10 gig line card crashes on a Cisco 7600 platform with the following or similar errors:

  ```
  %SYS-DFC3-3-MGDTIMER: Uninitialized timer, timer stop, timer = 30CCCFB0. -Process= "RO
  Notify Timers", ipl= 0, pid= 7 -Traceback= 2060E1BCz 2060E8E4z %SYS-DFC3-3-MGDTIMER:
  Uninitialized timer, timer stop, timer = 30CCD154. -Process= "RO Notify Timers", ipl=
  0, pid= 7 -Traceback= 2060E1BCz 2060E8E4z %SYS-DFC3-3-MGDTIMER: Uninitialized timer,
  timer stop, timer = 30CCCFB0. -Process= "RO Notify Timers", ipl= 0, pid= 7 -Traceback=
  2060E1BCz 2060E8E4z
  08:54:43 Central Tue Oct 1 2013: Address Error (load or instruction fetch) exception,
  CPU signal 10, PC = 0x20642A08
  ```

  Conditions: This symptom occurs when a large number of IPC messages are used.

  Workaround: There is no workaround.

  More Info: On mac-scaling, the L2-DRV application sends more ICC messages(though not always). But periodically(approximately 2-3 minutes), some burst of around 150 ICC messages are sent by the SP towards the RP. This means that mac-scaling has a direct correlation with the number of IPC messages being sent.

- CSCuj66352

  Symptom: A system crash is observed in the SNMP engine.

  Conditions: This symptom occurs under the following conditions:

  – ?show subscriber session?

  – polling the ISG-MIB -clearing the subscriber

  Workaround: Do not use SNMP polling.

- CSCuj68932

  Symptom: L2TPv3 tunnel with digest fails to establish. Cisco IOS device gives the following messages when "debug l2tp all" and "“debug l2tp packet detail” are enabled:

  ```
  L2TP _____:________: ERROR: SCCRQ AVP 59, vendor 0: unknown L2TP _____:________:
  Unknown IETF AVP 59 in CM SCCRQ
  ```

  Conditions: This issue is observed when IOS device peers with non-IOS device that sends IETF L2TPv3 digest AVP (IETF AVP 59) in L2TP control message. This issue is present in S images starting from Cisco IOS Release 12.2(33)XNC and in T train from Cisco IOS Release 15.3(2)T.

  Workaround: There is no workaround.

- CSCuj72553

  Symptom: The OSPF router may stay without a router LSA after NSF restarts which means that routing in the OSPF domain is seriously affected.

  Conditions: This symptom occurs under the following conditions:

  – OSPF NSF is terminated for some reason.

  – **mpls traffic-eng nsr** is configured.

  Workaround: Remove **mpls traffic-eng nsr**.

  More Info: Example of **show ip ospf nsf** after a failed NSF:

  ```
  Router#sh ip ospf 1 nsf
  ```

```
Routing Process "ospf 1"
IETF Non-Stop Forwarding enabled
restart-interval limit: 120 sec
Last IETF NSF restart 03:33:06 ago terminated after 5 secs, reason: Event
nbr 1-way
IETF NSF helper support enabled
Cisco NSF helper support enabled
Restart resync LSA state: TE has requested data
Restart resync Adj state: TE has requested data
OSPF restart state is NO_RESTART
Handle 140515696469576, Router ID 10.1.1.1, checkpoint Router ID 0.0.0.0
Config wait timer interval 10, timer not running
Dbase wait timer interval 120, timer not running
```

Router LSA generation is prevented by flag described on lines:

```
Restart resync LSA state: TE has requested data
Restart resync Adj state: TE has requested
```

Note: TE resync is not completed, although NSF is completed.

- CSCuj73822

  Symptom: A router crashes while removing the Locator ID Separation Protocol configuration **router lisp <id>** or **site <site-name>** sub-modes.

  Conditions: This symptom occurs when “allowed-locator list {ipv4 | ipv6} <prefix-list>” is present under the lisp site being deconfigured.

  Workaround: Remove the “allowed-locator list {ipv4 | ipv6} <prefix-list>” configuration from all the map-server sites before removing the “site <site-name>” sub-mode configuration (or removing the “router lisp <id>” sub-mode).

- CSCuj88523

  Symptom: In a pseudowire redundancy configuration, traffic may fail to flow after a switchover to a backup pseudowire.

  Conditions: This symptom occurs on the Cisco 7600 series routers.

  Workaround: Execute the following commands on the attachment circuit interface: -**shutdown** -**no shutdown**

- CSCuj96186

  Symptom: When auto-tunnel and RSVP graceful restart are configured, the standby crashes after an SSO (NSR is not configured).

  Conditions: This symptom occurs under the following conditions:

  – Configure auto-tunnel

  – Configure RSVP graceful restart without NSR

  – Perform an SSO

  Workaround: Disable RSVP graceful restart or remove the auto-tunnel configuration.

- CSCuj99537

  Symptom: Not all LI streams that are properly configured via SNMPv3 and appropriate ACLs and are programmed in TCAM, are intercepted and forwarded towards MD.

  Conditions: This symptom occurs in an SIP-400 based LI.

  Workaround: Remove and reapply the problematic tap but it doesn’t prevent the problem from reoccurring if new LI taps are applied via SNMPv3

- CSCul11995

  Symptom: An L2TPv3 session fails to establish and Cisco IOS receives a StopCCN message from the peer with the following message in response to its ICRP message: "No handler for attr 68 (68)"

  Conditions: This symptom occurs when IOS device peers with non-IOS devices send IETF L2TPv3 Pseudowire Type AVP (IETF AVP 68) in an ICRP message.

  Workaround: There is no workaround.

Open and Resolved Bugs - Cisco ASR 901 Series Routers in 15.4(1)S

For detailed information on Open and Resolved bugs on Cisco ASR 901 Series Routers in 15.4(1)S, see the following document:

http://www.cisco.com/en/US/docs/wireless/asr_901/Release/Notes/asr901_rn_15_4_1_S.html

Open and Resolved Bugs - Cisco ASR 901 S Series Routers in 15.4(1)S

For detailed information on Open and Resolved bugs on Cisco ASR 901 S Series Routers in 15.4(1)S, see the following document:

http://www.cisco.com/en/US/docs/wireless/asr_901s/rn/b_release_notes_for_asr901s.html

Open and Resolved Bugs - Cisco ME 3600x and ME 3800x Series Routers in 15.4(1)S

For detailed information on Open and Resolved bugs on Cisco ME 3600x and Cisco ME 3800x Series Routers in 15.4(1)S, see the following document:

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.4_1_S/release/notes/ol31008.html

Related Documentation

The following sections describe the documentation available for Cisco IOS Release 15.4S. 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 229
- Cisco Feature Navigator, page 229
- Cisco IOS Software Documentation Set, page 230
- Notices, page 230
- Obtaining Documentation and Submitting a Service Request, page 232

Platform-Specific Documents

Cisco 7600 Series Routers

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

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 15.4S 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

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.

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.
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

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.

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.