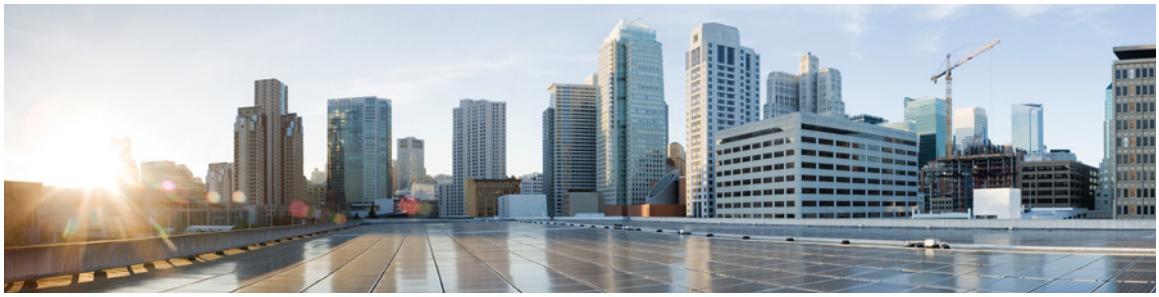

Release Notes for Cisco IOS Release 15.1SY

February 20, 2020

Note

- See this product bulletin for information about the standard maintenance and extended maintenance 15.1SY releases:

  http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-15-0sy/product_bulletin_c25-687567.html

- For general product information about the Catalyst 6500 series switches, refer to these product bulletins:

  http://www.cisco.com/c/en/us/products/switches/catalyst-6500-series-switches/literature.html

The most current version of this document is available on Cisco.com at this URL:

http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-1SY/release_notes.html

Caution Cisco IOS supports redundant configurations with identical supervisor engines. If they are not identical, one supervisor engine will boot first and become active and hold the other in a reset condition.

Contents

This publication consists of these sections:

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

Chronological List of Releases

Note

- See the "Images and Feature Sets" section on page 68 for information about which releases are deferred.

- See the "Hierarchical List of Releases" section on page 3 for information about parent releases.

This is a chronological list of the 15.1SY releases:

- Release 15.1(2)SY16—20 February 2020
- Release 15.1(2)SY15—20 August 2019
- Release 15.1(2)SY14—14 February 2019
- Release 15.1(2)SY13—6 September 2018
- Release 15.1(2)SY12—30 April 2018
- Release 15.1(2)SY11—27 July 2017
- Release 15.1(2)SY10—24 Feb 2017
- Release 15.1(2)SY9—14 Oct 2016
- Release 15.1(2)SY8—01 Sept 2016
- Release 15.1(2)SY7—16 Mar 2016
- Release 15.1(1)SY6—12 Nov 2015
- Release 15.1(2)SY6—19 Sept 2015
- Release 15.1(2)SY5—21 May 2015
- Release 15.1(1)SY5—27 Mar 2015
- Release 15.1(2)SY4—08 Nov 2014
- Release 15.1(1)SY4—10 Oct 2014
- Release 15.1(2)SY3—23 Jun 2014
- Release 15.1(1)SY3—22 Mar 2014
- Release 15.1(2)SY2—03 Mar 2014
- Release 15.1(2)SY1—09 Dec 2013
- Release 15.1(1)SY2—04 Oct 2013
- Release 15.1(2)SY—07 Sep 2013
- Release 15.1(1)SY1—03 May 2013
- Release 15.1(1)SY—15 Oct 2012

Hierarchical List of Releases

These releases support the hardware listed in the "Supported Hardware" section on page 6:

- Release 15.1(2)SY16:
  - Date of release: 20 February 2020
  - Based on Release: 15.1(2)SY15
- Release 15.1(2)SY15:
  - Date of release: 20 August 2019
  - Based on Release: 15.1(2)SY14

- Release 15.1(2)SY14:
  - Date of release: 14 February 2019
  - Based on Release: 15.1(2)SY13
- Release 15.1(2)SY13:
  - Date of release: 6 September 2018
  - Based on Release: 15.1(2)SY12
- Release 15.1(2)SY12:
  - Date of release: 30 April 2018
  - Based on Release: 15.1(2)SY11
- Release 15.1(2)SY11:
  - Date of release: 27 July 2017
  - Based on Release 15.1(2)SY10
- Release 15.1(2)SY10:
  - Date of release: 24 Feb 2017
  - Based on Release 15.1(2)SY9
- Release 15.1(2)SY9:
  - Date of release: 14 Oct 2016
  - Based on Release 15.1(2)SY8
- Release 15.1(2)SY8:
  - Date of release: 01 Sept 2016
  - Based on Release 15.1(2)SY7
- Release 15.1(2)SY7:
  - Date of release: 16 Mar 2016
  - Based on Release 15.1(2)SY6
- Release 15.1(1)SY6:
  - Date of release: 12 Nov 2015
  - Based on Release 15.1(1)SY5
- Release 15.1(2)SY6:
  - Date of release: 19 Sept 2015
  - Based on Release 15.1(2)SY5
- Release 15.1(2)SY5:
  - Date of release: 21 May 2015
  - Based on Release 15.1(2)SY4
- Release 15.1(1)SY5:
  - Date of release: 27 Mar 2015
  - Based on Release 15.1(1)SY4

- Release 15.1(2)SY4:
  - Date of release: 08 Nov 2014
  - Based on Release 15.1(2)SY3
- Release 15.1(1)SY4:
  - Date of release: 10 Oct 2014
  - Based on Release 15.1(1)SY3
- Release 15.1(2)SY3:
  - Date of release: 23 Jun 2014
  - Based on Release 15.1(2)SY2
- Release 15.1(2)SY2:
  - Date of release: 03 Mar 2014
  - Based on Release 15.1(2)SY1
- Release 15.1(2)SY1:
  - Date of release: 09 Dec 2013
  - Based on Release 15.1(2)SY
- Release 15.1(1)SY3:
  - Date of release: 22 Mar 2014
  - Based on Release 15.1(1)SY2
- Release 15.1(1)SY2:
  - Date of release: 04 Oct 2013
  - Based on Release 15.1(1)SY1
- Release 15.1(2)SY:
  - Date of release: 07 Sep 2013
  - Based on Release 15.1(1)SY1
- Release 15.1(1)SY1:
  - Date of release: 03 May 2013
  - Based on Release 15.1(1)SY
- Release 15.1(1)SY:
  - Date of release: 15 Oct 2012
  - Based on Release 15.0(1)SY2 and Release 12.2(33)SXJ3

Note Release 15.1SY supports only Ethernet ports. Release 15.1SY does not support any WAN features or commands.

FPD-Image Dependant Modules

FPD image packages update FPD images. If a discrepancy exists between an FPD image and the Cisco IOS image, the module that has the FPD discrepancy is deactivated until the discrepancy is resolved. These modules use FPD images:

- ASA services module (WS-SVC-ASA-SM1-K9)—See this publication:

  http://www.cisco.com/c/en/us/td/docs/security/asa/asa84/release/notes/asarn85.html
- Network Analysis Module 3 (WS-SVC-NAM3-6G-K9)—See these publications:

  http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-network-analysis-module-software/products-release-notes-list.html

Supported Hardware

These sections describe the hardware supported in Release 15.1(2)SY1 and later releases:

Note Enter the **show power** command to display current system power usage.

Supervisor Engines, PFCs, DFCs, and CFC

Supervisor Engine 2T-10GE

Note For information about DRAM requirements on all supervisor engines, see this publication:

http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/qa_c67_457347.html

Product ID (append "=" for spares)	**Product Description**	**Minimum Software Version**
VS-S2T-10G-XL	Supervisor Engine 2T-10GE with PFC4XL	15.0(1)SY
VS-S2T-10G	Supervisor Engine 2T-10GE with PFC4	

Features

- One of these policy feature cards:
  - Policy Feature Card 4XL (PFC4XL)
  - Policy Feature Card 4 (PFC4)

  See the "Policy Feature Cards Supported with Supervisor Engine 2T" section on page 8.
- Supports 2-Tbps switch fabric connectivity.
- 2-GB DRAM.
- Internal 1-GB bootflash (**bootdisk:**).
- One external slot:
  - **disk0:**
  - For CompactFlash Type II flash PC cards sold by Cisco Systems, Inc., for use in Supervisor Engine 2T-10GE.
- Console ports:
  - EIA/TIA-232 (RS-232) port
  - USB port
- Ports 1, 2, and 3:
  - QoS architecture: **2q4t**/**1p3q4t**
  - Ports 1, 2, and 3: Gigabit Ethernet SFP (fiber SFP or 1000 Mbps RJ-45 SFP)
- Ports 4 and 5:
  - Support for 10-Gigabit Ethernet X2 tranceivers
  - QoS architecture:

  - With ports 1, 2, and 3 enabled: **2q4t/1p3q4t**
  - With ports 1, 2, and 3 disabled: **8q4t/1p7q4t**
- One port group: ports 1 through 5

Note See the *Supervisor Engine 2T-10GE Connectivity Management Processor Configuration Guide* for information about the 10/100/1000 Mbps RJ-45 port.

- Connectivity Management Processor (CMP)—See this publication:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/cmp_configuration/guide/sup2T_10GEcmp.html

Supervisor Engine 2T-10GE Restrictions

- The 1-Gigabit Ethernet ports and the 10-Gigabit Ethernet ports have the same QoS port architecture (**2q4t/1p3q4t**) unless you disable the 1-Gigabit Ethernet ports with the **platform qos 10g-only** global configuration command. With the 1-Gigabit Ethernet ports disabled, the QoS port architecture of the 10-Gigabit Ethernet ports is **8q4t/1p7q4t**.
- In RPR redundancy mode, the ports on a Supervisor Engine 2T-10GE in standby mode are disabled.

Policy Feature Cards Supported with Supervisor Engine 2T

- Policy Feature Card 4 Guidelines and Restrictions, page 8
- Policy Feature Card 4XL, page 10
- Policy Feature Card 4, page 10

Policy Feature Card 4 Guidelines and Restrictions

- The PFC4 supports a theoretical maximum of 131,072 (128K) MAC addresses with 118,000 (115.2K) MAC addresses as the recommended maximum.
- The PFC4 partitions the hardware FIB table to route IPv4 unicast, IPv4 multicast, MPLS, and IPv6 unicast and multicast traffic in hardware. Traffic for routes that do not have entries in the hardware FIB table are processed by the route processor in software.

  The defaults for XL mode are:

  – IPv4 unicast and MPLS: 512,000 routes

  – IPv4 multicast and IPv6 unicast and multicast: 256,000 routes

  The defaults for Non-XL mode are:

  – IPv4 unicast and MPLS: 192,000 routes

  – IPv4 multicast and IPv6 unicast and multicast: 32,000 routes

  Note The size of the global internet routing table plus any local routes might exceed the non-XL mode default partition sizes.

  These are the theoretical maximum numbers of routes for the supported protocols (the maximums are not supported simultaneously):

  – XL mode:

    - IPv4 and MPLS: Up to 1,007,000 routes
    - IPv4 multicast and IPv6 unicast and multicast: Up to 503,000 routes
  - Non-XL mode:
    - IPv4 and MPLS: Up to 239,000 routes
    - IPv4 multicast and IPv6 unicast and multicast: Up to 119,000 routes

  Enter the **platform cef maximum-routes** command to repartition the hardware FIB table. IPv4 unicast and MPLS require one hardware FIB table entry per route. IPv4 multicast and IPv6 unicast and multicast require two hardware FIB table entries per route. Changing the partition for one protocol makes corresponding changes in the partitions of the other protocols. You must enter the **reload** command to put configuration changes made with the **platform cef maximum-routes** command into effect.

  Note With a non-XL-mode system, if your requirements cannot be met by repartitioning the hardware FIB table, upgrade components as necessary to operate in XL mode.

- You cannot use one type of PFC on one supervisor engine and a different type on the other supervisor engine for redundancy. You must use identical policy feature cards for redundancy.
- PFC4—These restrictions apply to a configuration with a PFC4 and these DFCs:
  - PFC4 and DFC4—No restrictions (PFC4 mode).
  - PFC4 and DFC4XL—The PFC4 restricts DFC4XL functionality: the DFC4XL functions as a DFC4 (PFC4 mode).
- PFC4XL—These restrictions apply to a configuration with a PFC4XL and these DFCs:
  - PFC4XL and DFC4—PFC4XL functionality is restricted by the DFC4: after a reload with a DFC4-equipped module installed, the PFC4XL functions as a PFC4 (PFC4 mode).
  - PFC4XL and DFC4XL—No restrictions (PFC4XL mode).
- Switching modules that you install after bootup that are equipped with a DFC that imposes a more restricted PFC mode than the current PFC mode remain powered down.
- You must reboot to use a switching module equipped with a DFC that imposes a more restricted PFC mode than the current PFC mode.
- Enter the **show platform hardware pfc mode** command to display the PFC mode.
- FIB TCAM exception may be thrown in case of a route churn where TCAM utilization is more than 80% of the total utilization. This limitation is applicable to DFC TCAM on -XL line cards. If FIB TCAM exception is thrown for a transit route for IPv4 or IPv6 or MPLS traffic, the route does not get installed in FIB and connectivity gets affected. This can result in elevated CPU usage due to software switching.

Policy Feature Card 4XL

Product ID (append "=" for spares)	Product Description	Minimum Software Version
VS-F6K-PFC4XL	Policy Feature Card 4XL (PFC4XL) **Note** Use VS-F6K-PFC4XL= to upgrade to a PFC4XL.	
	With Supervisor Engine 2T-10GE	15.0(1)SY

Policy Feature Card 4

Product ID (append "=" for spares)	Product Description	Minimum Software Version
VS-F6K-PFC4	Policy Feature Card 4 (PFC4)	
	With Supervisor Engine 2T-10GE	15.0(1)SY

Distributed Forwarding Cards Supported with Supervisor Engine 2T

- Distributed Forwarding Card 4XL, page 10
- Distributed Forwarding Card 4, page 11

Note

- See the "Policy Feature Cards Supported with Supervisor Engine 2T" section on page 8 for Policy Feature Cards (PFC) and Distributed Forwarding Card (DFC) restrictions.
- The DFC4 uses memory that is installed on the switching module.
- For more information about the DFCs, see these documents:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/hardware/Config_Notes/OL_24918.html

  http://www.cisco.com/c/en/us/products/collateral/interfaces-modules/catalyst-6500-series-supervisor-engine-2t/data_sheet_c78-648214.html

Distributed Forwarding Card 4XL

Product ID (append "=" for spares)	Product Description	Minimum Software Version
WS-F6K-DFC4-EXL **WS-F6K-DFC4-AXL**	Distributed Forwarding Card 4XL (DFC4XL)	
	With Supervisor Engine 2T-10GE	15.0(1)SY

Distributed Forwarding Card 4

Product ID (append "=" for spares)	Product Description	Minimum Software Version
WS-F6K-DFC4-E **WS-F6K-DFC4-A**	Distributed Forwarding Card 4 (DFC4)	
	With Supervisor Engine 2T-10GE	15.0(1)SY

Supervisor Engine 720-10GE (CAT6000-VS-S720-10G/MSFC3)

- Supervisor Engine 720-10GE Common Features, page 11
- Supervisor Engine 720-10GE with PFC3C and PFC3CXL, page 12
- Supervisor Engine 720-10GE Restrictions, page 12

Supervisor Engine 720-10GE Common Features

- Switch processor (SP):
  - Internal 1-GB CompactFlash card (**sup-bootdisk:**).
  - 1-GB DRAM.
- Route processor (RP):
  - Internal 64-MB bootflash.
  - 1-GB DRAM.
- One of these:
  - Policy Feature Card 3CXL (PFC3CXL).
  - Policy Feature Card 3C (PFC3C).
  - See the "Policy Feature Cards Supported with Supervisor Engine 2T" section on page 8.
- Integrated 720-Gbps Switch Fabric.
- One external slot:
  - **disk0:**
  - For CompactFlash Type II flash PC cards sold by Cisco Systems, Inc., for use in Supervisor Engine 720-10GE.
- Console port—EIA/TIA-232 (RS-232) port.
- Ports 1 and 2:
  - QoS architecture: **2q4t**/**1p3q4t**
  - Support for Gigabit Ethernet SFPs
- Port 3:
  - 10/100/1000 Mbps RJ-45
  - QoS architecture: **2q4t**/**1p3q4t**
- Ports 4 and 5:
  - Support for 10-Gigabit Ethernet X2 tranceivers

  - QoS architecture: **2q4t/1p3q4t** or **8q4t/1p7q4t**

Note The 1-Gigabit Ethernet ports and the 10-Gigabit Ethernet ports have the same QoS port architecture (**2q4t/1p3q4t**) unless you disable the 1-Gigabit Ethernet ports with the **mls qos 10g-only** global configuration command, which is required to configure DSCP-based queueing. With the 1-Gigabit Ethernet ports disabled, the QoS port architecture of the 10-Gigabit Ethernet ports is **8q4t/1p7q4t**.

- One port group: ports 1 through 5.
- Two Universal Serial Bus (USB) 2.0 ports (not currently enabled)

Supervisor Engine 720-10GE with PFC3C and PFC3CXL

Product ID (append "=" for spares)	**Product Description**	**Minimum Software Versions**
VS-S720-10G-3CXL	Supervisor Engine 720-10GE with PFC3CXL	15.1(1)SY
VS-S720-10G-3C	Supervisor Engine 720-10GE with PFC3C	15.1(1)SY

Supervisor Engine 720-10GE Restrictions

- In RPR redundancy mode, the ports on a Supervisor Engine 720-10GE in standby mode are disabled.
- There are no memory-only upgrade options for the Supervisor Engine 720-10GE.

Supervisor Engine 720 (CAT6000-SUP720/MSFC3)

- Supervisor Engine 720 Common Features, page 12
- Supervisor Engine 720 with PFC3BXL, page 13
- Supervisor Engine 720 with PFC3B, page 14

Supervisor Engine 720 Common Features

- Integrated 720-Gbps Switch Fabric
- Internal 64-MB bootflash device (**sup-bootflash:**) or CompactFlash card (sup-bootdisk:), 512 MB or larger.
  - As an upgrade, WS-CF-UPG=
  - See this publication:

    http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_17277.html
- Two external slots (disk0: and disk1:) for CompactFlash Type II flash PC cards sold by Cisco Systems, Inc., for use in Supervisor Engine 720.

Note Some Supervisor Engine 720 Release 12.2SX images are larger than the bootflash device and must be stored on a CompactFlash card (sup-bootdisk: or disk0: or disk1:).

- Two Ethernet uplink ports:
  - 512-KB packet buffer per port
  - Port 1—Gigabit Interface Converter (GBIC)
  - Port 2—Configurable as either:
    - Gigabit Interface Converter (GBIC)
    - 10/100/1000 Mbps RJ-45
- QoS port architecture (Rx/Tx): **1p1q4t**/**1p2q2t**
- Port grouping:
  - Number of ports: 2
  - Number of port groups: 1
  - Port ranges per port group: 1–2

Supervisor Engine 720 with PFC3BXL

Note If you install WS-SUP720-3BXL=, upgrade the memory on any DFC3-equipped switching modules. See this document for DFC3 memory upgrades:

http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_12409.html

Product ID (append "=" for spares)	**Product Description**	**Minimum Software Versions**
WS-SUP720-3BXL	Supervisor Engine 720 with PFC3BXL: • Switch processor (SP): – Internal 64-MB bootflash device (**sup-bootflash:**) or internal CompactFlash card (sup-bootdisk:) – 1-GB or larger DRAM • Route processor (RP): – 1-GB or larger DRAM – 64-MB bootflash • Policy Feature Card 3BXL (PFC3BXL)—See the "Policy Feature Cards Supported with Supervisor Engine 2T" section on page 8.	15.1(1)SY

Supervisor Engine 720 with PFC3B

Note

- See this document for DFC3 memory upgrades:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_12409.html
- Use WS-F6K-PFC3BXL= to upgrade a WS-SUP720-3B with a PFC3BXL. WS-F6K-PFC3BXL= includes 1 GB memory upgrades for the Supervisor Engine 720 and the MSFC3.
  - If you install WS-F6K-PFC3BXL=, upgrade the memory on any DFC3-equipped switching modules.
  - See this publication for more information about WS-F6K-PFC3BXL=: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_16220.html

Product ID (append "=" for spares)	**Product Description**	**Minimum Software Versions**
WS-SUP720-3B	Supervisor Engine 720 with PFC3B: • Switch processor (SP): – Internal 64-MB bootflash device (**sup-bootflash:**) or internal CompactFlash card (sup-bootdisk:) – 512-MB or larger DRAM • Route processor (RP): – 64-MB bootflash – 512-MB or larger DRAM • Policy Feature Card 3B (PFC3B)—See the "Policy Feature Cards Supported with Supervisor Engine 2T" section on page 8	15.1(1)SY

Policy Feature Cards Supported with Supervisor Engine 720

- Policy Feature Card 3 Guidelines and Restrictions, page 15
- Policy Feature Card 4XL, page 10
- Policy Feature Card 4, page 10
- Policy Feature Card 3BXL, page 17
- Policy Feature Card 3B, page 18

Policy Feature Card 3 Guidelines and Restrictions

- The PFC3C supports a theoretical maximum of 96 K MAC addresses (64 K MAC addresses recommended maximum).
- The PFC3B and PFC3BXL support a theoretical maximum of 64 K MAC addresses (32 K MAC addresses recommended maximum).
- The PFC3 partitions the hardware FIB table to route IPv4 unicast, IPv4 multicast, MPLS, and IPv6 unicast and multicast traffic in hardware. Traffic for routes that do not have entries in the hardware FIB table are processed by the route processor in software.

  The defaults for XL mode are:

  – IPv4 unicast and MPLS—512,000 routes

  – IPv4 multicast and IPv6 unicast and multicast—256,000 routes

  The defaults for non-XL mode are:

  – IPv4 unicast and MPLS—192,000 routes

  – IPv4 multicast and IPv6 unicast and multicast—32,000 routes

  Note The size of the global internet routing table plus any local routes might exceed the non-XL mode default partition sizes.

  These are the theoretical maximum numbers of routes for the supported protocols (the maximums are not supported simultaneously):

  – XL mode:

    • IPv4 and MPLS—Up to 1,007,000 routes

    • IPv4 multicast and IPv6 unicast and multicast—Up to 503,000 routes

  – Non-XL mode:

    • IPv4 and MPLS—Up to 239,000 routes

    • IPv4 multicast and IPv6 unicast and multicast—Up to 119,000 routes

  Enter the mls cef maximum-routes command to repartition the hardware FIB table. IPv4 unicast and MPLS require one hardware FIB table entry per route. IPv4 multicast and IPv6 unicast and multicast require two hardware FIB table entries per route. Changing the partition for one protocol makes corresponding changes in the partitions of the other protocols. You must enter the **reload** command to put configuration changes made with the **mls cef maximum-routes** command into effect.

  Note With a non-XL-mode system, if your requirements cannot be met by repartitioning the hardware FIB table, upgrade components as necessary to operate in XL mode.

- You cannot use one type of PFC3 on one supervisor engine and a different type on the other supervisor engine for redundancy. You must use identical policy feature cards for redundancy.
- PFC3B—These restrictions apply to a configuration with a PFC3B and these DFCs:

  – PFC3B and DFC3B—No restrictions (PFC3B mode; does not support virtual switch mode).

  – PFC3B and DFC3BXL—The PFC3B restricts DFC3BXL functionality: after a reload with a DFC3BXL-equipped module installed, the DFC3BXL functions as a DFC3B (PFC3B mode; does not support virtual switch mode).

  - PFC3B and DFC3C—The PFC3B restricts DFC3C functionality: the DFC3C functions as a DFC3B (PFC3B mode; does not support virtual switch mode).
  - PFC3B and DFC3CXL—The PFC3B restricts DFC3CXL functionality: the DFC3CXL functions as a DFC3B (PFC3B mode; does not support virtual switch mode).
- PFC3BXL—These restrictions apply to a configuration with a PFC3BXL and these DFCs:
  - PFC3BXL and DFC3B—PFC3BXL functionality is restricted by the DFC3B: after a reload with a DFC3B-equipped module installed, the PFC3BXL functions as a PFC3B (PFC3B mode; does not support virtual switch mode).
  - PFC3BXL and DFC3BXL—No restrictions (PFC3BXL mode; does not support virtual switch mode).
  - PFC3BXL and DFC3C—Each restricts the functionality of the other: the PFC3BXL functions as a PFC3B and the DFC3C functions as a DFC3B (PFC3B mode; does not support virtual switch mode).
  - PFC3BXL and DFC3CXL—The PFC3BXL restricts DFC3CXL functionality: the DFC3CXL functions as a DFC3BXL (PFC3BXL mode; does not support virtual switch mode).
- PFC3C—These restrictions apply to a configuration with a PFC3C and these DFCs:
  - PFC3C and DFC3B—PFC3C functionality is restricted by the DFC3B: after a reload with a DFC3B-equipped module installed, the PFC3C functions as a PFC3B (PFC3B mode; does not support virtual switch mode).
  - PFC3C and DFC3BXL—PFC3C functionality is restricted by the DFC3BXL: after a reload with a DFC3BXL-equipped module installed, the PFC3C functions as a PFC3BXL (PFC3BXL mode; does not support virtual switch mode).
  - PFC3C and DFC3C—No restrictions (PFC3C mode).
  - PFC3C and DFC3CXL—The PFC3C restricts DFC3CXL functionality: the DFC3CXL functions as a DFC3C (PFC3C mode).
- PFC3CXL—These restrictions apply to a configuration with a PFC3CXL and these DFCs:
  - PFC3CXL and DFC3B—PFC3CXL functionality is restricted by the DFC3B: after a reload with a DFC3B-equipped module installed, the PFC3CXL functions as a PFC3B (PFC3B mode; does not support virtual switch mode).
  - PFC3CXL and DFC3BXL—PFC3CXL functionality is restricted by the DFC3BXL: after a reload with a DFC3BXL-equipped module installed, the PFC3CXL functions as a PFC3BXL (PFC3BXL mode; does not support virtual switch mode).
  - PFC3CXL and DFC3C—PFC3CXL functionality is restricted by the DFC3C: after a reload with a DFC3C-equipped module installed, the PFC3CXL functions as a PFC3C (PFC3C mode).
  - PFC3CXL and DFC3CXL—No restrictions (PFC3CXL mode).
- Switching modules that you install after bootup that are equipped with a DFC that imposes a more restricted PFC mode than the current PFC mode remain powered down.
- You must reboot to use a switching module equipped with a DFC that imposes a more restricted PFC mode than the current PFC mode.
- Enter the **show platform hardware pfc mode** command to display the PFC mode.
- FIB TCAM exception may be thrown in case of a route churn where TCAM utilization is more than 80% of the total utilization. This limitation is applicable to DFC TCAM on XL line cards. If FIB TCAM exception is thrown for a transit route for IPv4 or IPv6 or MPLS traffic, the route does not get installed in FIB and connectivity gets affected. This can result in elevated CPU usage due to software switching.

Policy Feature Card 3CXL

Note Use VS-F6K-PFC3CXL= to upgrade a VS-S720-10G-3C with a PFC3CXL. See this publication for more information:

http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_16220.html

Product ID (append "=" for spares)	Product Description	Minimum Software Versions
VS-F6K-PFC3CXL	Policy Feature Card 3CXL (PFC3CXL)	
	Supported only with Supervisor Engine 720-10GE	15.1(1)SY

Policy Feature Card 3C

Product ID (append "=" for spares)	Product Description	Minimum Software Versions
VS-F6K-PFC3C **ME-C6524-PFC3C**	Policy Feature Card 3C (PFC3C)	
	Supported only with Supervisor Engine 720-10GE	15.1(1)SY

Policy Feature Card 3BXL

Note Use WS-F6K-PFC3BXL= to upgrade a WS-SUP720 or WS-SUP720-3B with a PFC3BXL. WS-F6K-PFC3BXL= includes 1 GB memory upgrades for the Supervisor Engine 720 and the MSFC3. See this publication for more information:

http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_16220.html

Product ID (append "=" for spares)	Product Description	Minimum Software Versions
WS-F6K-PFC3BXL	Policy Feature Card 3BXL (PFC3BXL)	
	Supported only with Supervisor Engine 720	15.1(1)SY

Policy Feature Card 3B

Note Use WS-F6K-PFC3B= to upgrade a WS-SUP720 with a PFC3B. See this publication for more information:

http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_16220.html

Product ID (append "=" for spares)	**Product Description**	**Minimum Software Versions**
WS-F6K-PFC3B	Policy Feature Card 3B (PFC3B)	
	With Supervisor Engine 720	15.1(1)SY

Distributed Forwarding Cards Supported with Supervisor Engine 720

- Distributed Forwarding Card 3CXL, page 18
- Distributed Forwarding Card 3C, page 19
- Distributed Forwarding Card 3BXL, page 19
- Distributed Forwarding Card 3B, page 21

Note See the "Policy Feature Cards Supported with Supervisor Engine 2T" section on page 8 for Policy Feature Cards (PFC) and Distributed Forwarding Card (DFC) restrictions.

Distributed Forwarding Card 3CXL

Note

- WS-F6700-DFC3CXL uses memory that is installed on the switching module.
- See this publication for information about WS-F6700-DFC3CXL upgrades:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_15893.html
- Requires switching module ROMMON version 12.2(18r)S1 or later. To display the switching module ROMMON version, enter the **remote command module** *module_slot_number* **show version | include ROM** command. To upgrade the switching module ROMMON, see this document:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/rommon/OL_6143.html

Product ID (append "=" for spares)	Product Description	Minimum Software Version
WS-F6700-DFC3CXL	Distributed Forwarding Card 3CXL (DFC3CXL) for use on CEF720 modules **Note** Not supported with Supervisor Engine 2T.	
	With Supervisor Engine 720-10GE	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

Distributed Forwarding Card 3C

Note

- WS-F6700-DFC3C uses memory that is installed on the switching module.
- See this publication for information about WS-F6700-DFC3C upgrades:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_15893.html
- Requires switching module ROMMON version 12.2(18r)S1 or later. To display the switching module ROMMON version, enter the **remote command module** *module_slot_number* **show version | include ROM** command. To upgrade the switching module ROMMON, see this document:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/rommon/OL_6143.html

Product ID (append "=" for spares)	Product Description	Minimum Software Version
WS-F6700-DFC3C	Distributed Forwarding Card 3C (DFC3C) for use on CEF720 modules **Note** Not supported with Supervisor Engine 2T.	
	With Supervisor Engine 720-10GE	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

Distributed Forwarding Card 3BXL

- WS-F6700-DFC3BXL, page 19
- WS-F6K-DFC3BXL, page 20

WS-F6700-DFC3BXL

Note

- Not supported in virtual switch mode.
- WS-F6700-DFC3BXL uses memory that is installed on the switching module.
- See this publication for information about WS-F6700-DFC3BXL upgrades:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_15893.html

- Requires switching module ROMMON version 12.2(18r)S1 or later. To display the switching module ROMMON version, enter the **remote command module** *module_slot_number* **show version | include ROM** command. To upgrade the switching module ROMMON, see this document:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/rommon/OL_6143.html

Product ID (append "=" for spares)	**Product Description**	**Minimum Software Versions**
WS-F6700-DFC3BXL	Distributed Forwarding Card 3BXL (DFC3BXL) for use on CEF720 modules **Note** Not supported with Supervisor Engine 2T.	
	With Supervisor Engine 720-10GE (not supported in VSS mode)	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

WS-F6K-DFC3BXL

Note

- Not supported in virtual switch mode.
- See this publication for information about WS-F6K-DFC3BXL memory upgrades:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_12409.html
- Supervisor Engine 720 supports a WS-F6K-DFC3BXL on these WS-X6516-GBIC switching module hardware revisions:
  - Lower than 5.0
  - 5.5 and higher
- Requires DFC ROMMON version 12.2(18r)S1 or later. To display the switching module ROMMON version, enter the **remote command module** *module_slot_number* **show version | include ROM** command. To upgrade the switching module ROMMON, see this document:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/rommon/OL_6010.html
- Supervisor Engine 720 does not support a DFC3 on WS-X6516-GBIC switching module hardware revisions 5.0 through 5.4. With a Supervisor Engine 720 and with a DFC3 installed, WS-X6516-GBIC switching module hardware revisions 5.0 through 5.4 do not power up.
- With a Supervisor Engine 720 but without a DFC3, WS-X6516-GBIC switching module hardware revisions 5.0 through 5.4 operate in bus mode.
- See external field notice 24494 for more information about Supervisor Engine 720 and a DFC3 on WS-X6516-GBIC switching modules:

  http://www.cisco.com/c/en/us/support/docs/field-notices/200/fn24494.html

Product ID (append "=" for spares)	Product Description	Minimum Software Versions
WS-F6K-DFC3BXL	Distributed Forwarding Card 3BXL (DFC3BXL) for use on dCEF256 and CEF256 modules **Note** Not supported with Supervisor Engine 2T.	
	With Supervisor Engine 720-10GE (not supported in VSS mode)	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

Distributed Forwarding Card 3B

- WS-F6700-DFC3B, page 21
- WS-F6K-DFC3B, page 22

WS-F6700-DFC3B

Note

- Not supported in virtual switch mode.
- WS-F6700-DFC3B uses memory that is installed on the switching module.
- See this publication for information about WS-F6700-DFC3B upgrades:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_15893.html
- Requires switching module ROMMON version 12.2(18r)S1 or later. To display the switching module ROMMON version, enter the **remote command module** *module_slot_number* **show version | include ROM** command. To upgrade the switching module ROMMON, see this document:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/rommon/OL_6143.html

Product ID (append "=" for spares)	Product Description	Minimum Software Versions
WS-F6700-DFC3B	Distributed Forwarding Card 3B (DFC3B) for use on CEF720 modules **Note** Not supported with Supervisor Engine 2T.	
	With Supervisor Engine 720-10GE (not supported in VSS mode)	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

WS-F6K-DFC3B

Note

- Not supported in virtual switch mode.
- See this publication for information about WS-F6K-DFC3B memory upgrades:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_12409.html
- Requires DFC ROMMON version 12.2(18r)S1 or later. To display the switching module ROMMON version, enter the **remote command module** *module_slot_number* **show version | include ROM** command. To upgrade the switching module ROMMON, see this document:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/rommon/OL_6010.html
- Supervisor Engine 720 supports a WS-F6K-DFC3B on these WS-X6516-GBIC switching module hardware revisions:
  - Lower than 5.0
  - 5.5 and higher
- Supervisor Engine 720 does not support a DFC3 on WS-X6516-GBIC switching module hardware revisions 5.0 through 5.4. With a Supervisor Engine 720 and with a DFC3 installed, WS-X6516-GBIC switching module hardware revisions 5.0 through 5.4 do not power up.
- With a Supervisor Engine 720 but without a DFC3, WS-X6516-GBIC switching module hardware revisions 5.0 through 5.4 operate in bus mode.
- See external field notice 24494 for more information about Supervisor Engine 720 and a DFC3 on WS-X6516-GBIC switching modules:

  http://www.cisco.com/c/en/us/support/docs/field-notices/200/fn24494.html

Product ID (append "=" for spares)	**Product Description**	**Minimum Software Versions**
WS-F6K-DFC3B	Distributed Forwarding Card 3B (DFC3B) for use on dCEF256 and CEF256 modules **Note** Not supported with Supervisor Engine 2T.	
	With Supervisor Engine 720-10GE (not supported in VSS mode)	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

Centralized Forwarding Card (WS-F6700-CFC)

Product ID (append "=" for spares)	Product Description	Minimum Software Version
WS-F6700-CFC	Centralized Forwarding Card (CFC) for use on CEF720 modules	
	With Supervisor Engine 2T-10GE	15.0(1)SY
	With Supervisor Engine 720-10GE	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

40-Gigabit Ethernet Switching Modules

WS-X6904-40G-2T 4-Port 40-Gigabit Ethernet Switching Module

Product ID (append "=" for spares)	Product Description	Minimum Software Version
WS-X6904-40G-2TXL (Has WS-F6K-DFC4-EXL) **WS-X6904-40G-2T** (Has WS-F6K-DFC4-E)	4-port 40-Gigabit Ethernet module	
	With Supervisor Engine 2T-10GE	15.0(1)SY1

- WS-X6904-40G-2T and WS-X6904-40G-2TXL are the orderable product IDs.
- The front panel is labeled WS-X6904-40G.
- Cisco IOS software commands display WS-X6904-40G with either WS-F6K-DFC4-E or WS-F6K-DFC4-EXL.
- Has hardware abstraction layer (HAL) support.
- QoS port architecture (Rx/Tx): **1p7q4t** or **2p6q4t/1p7q4t** or **2p6q4t**
- Dual switch-fabric connections:
  - Fabric Channel #1: Ports 1 and 2 or 5 through 12
  - Fabric Channel #2: Ports 3 and 4 or 13 through 20
- Number of ports: 4 or 16
  Number of port groups: 2
  Port per port group:
  –Ports 1 and 2 or 5 through 12
  –Ports 3 and 4 or 13 through 20
- dCEF2T.
- In a 3-slot chassis, supported only with WS-C6503-E hardware revision 1.3 or higher.
- Upgrade to Release15.0(1)SY1 or later before installing WS-X6904-40G (see the "EFSU Compatibility" section on page 68).

- Each bay can support a CFP transceiver (supports one 40 Gigabit Ethernet port) or a FourX adapter (supports four 10 Gigabit Ethernet SFP+ transceivers).
- WS-X6904-40G supported modes (default mode is oversubscribed):
  - 40 Gigabit Ethernet oversubscribed mode:
    —Four 40 Gigabit Ethernet ports
    —Ports 1 through 4
  - 10 Gigabit Ethernet oversubscribed mode:
    —Sixteen 10 Gigabit Ethernet ports
    —Ports 5 through 20
  - Mixed 10/40 Gigabit Ethernet oversubscribed mode:
    —Left bays:
    –Either two 40 Gigabit Ethernet ports (1 and 2)
    –Or eight 10 Gigabit Ethernet ports (5 through 12)
    —Right bays:
    –Either two 40 Gigabit Ethernet ports (3 and 4)
    –Or eight 10 Gigabit Ethernet ports (13 through 20)
  - Performance mode:
    —Configurable per module or per bay:

      no hw-module slot *slot_number* **oversubscription** [**port-group** *port_group_number*]

    —Supported in the top left bay and top right bay.
    —Any of these combinations:
    –40 Gigabit Ethernet port 1 (top left bay) and port 3 (top right bay)
    –10 Gigabit Ethernet ports 5 through 9 (top left bay) and ports 13 through 16 (top right bay)
    –Top left bay: 40 Gigabit Ethernet port 1 or 10 Gigabit Ethernet ports 5 through 9
    Top right bay: 40 Gigabit Ethernet port 3 or 10 Gigabit Ethernet ports 13 through 16
  - 40 Gigabit Ethernet performance mode, 10 Gigabit Ethernet oversubscribed mode:
    —Either of these combinations:
    –Top left bay: 40 Gigabit Ethernet port 1
    Right bays: eight 10 Gigabit Ethernet ports (13 through 20)
    –Left bays: eight 10 Gigabit Ethernet ports (5 through 13)
    Top right bay: 40 Gigabit Ethernet port 3
  - 40 Gigabit Ethernet oversubscribed mode, 10 Gigabit Ethernet performance mode:
    —Either of these combinations:
    –Top left bay: four 10 Gigabit Ethernet ports (5 through 9)
    Right bays: two 40 Gigabit Ethernet ports (3 and 4)
    –Left bays: two 40 Gigabit Ethernet ports (1 and 2)
    Top right bay: four 10 Gigabit Ethernet ports (13 through 16)
- For more information about WS-X6904-40G, see these publications:

  40 Gigabit Ethernet on Cisco Catalyst 6500 Series Switches: How It Works

  40 Gigabit Ethernet Interface Module for Cisco Catalyst 6500 Series Switches Data Sheet

10-Gigabit Ethernet Switching Modules

WS-X6908-10GE 8-Port 10-Gigabit Ethernet X2 Switching Module

Product ID (append "=" for spares)	**Product Description**	**Minimum Software Version**
WS-X6908-10G-XL (Has WS-F6K-DFC4-EXL) **WS-X6908-10G** (Has WS-F6K-DFC4-E)	8-port 10-Gigabit Ethernet X2 module	
	With Supervisor Engine 2T-10GE	15.0(1)SY

- Not supported with Supervisor Engine 720 or Supervisor Engine 720-10GE.
- WS-X6908-10G and WS-X6908-10G-XL are the orderable product IDs.
- The front panel is labeled WS-X6908-10GE.
- Cisco IOS software commands display WS-X6908-10GE with either WS-F6K-DFC4-E or WS-F6K-DFC4-EXL.
- dCEF2T
- QoS port architecture (Rx/Tx): **8q4t/1p7q4t**
- Dual switch-fabric connections
  Fabric Channel #1: Ports 2, 3, 6, 8
  Fabric Channel #2: Ports 1, 4, 5, 7
- Number of ports: 8
  Number of port groups: 8
  Port ranges per port group: 1 port in each group
- In a 3-slot chassis, supported only with WS-C6503-E hardware revision 1.3 or higher.

WS-X6816-10T-2T, WS-X6716-10T 16-Port 10-Gigabit Ethernet Copper Switching Module

Product ID (append "=" for spares)	**Product Description**	**Minimum Software Version**
WS-X6816-10T-2TXL (Has WS-F6K-DFC4-EXL) **WS-X6716-10T-3CXL** (Must be upgraded with WS-F6K-DFC4-EXL=) **WS-X6816-10T-2T** (Has WS-F6K-DFC4-E) **WS-X6716-10T-3C** (Must be upgraded with WS-F6K-DFC4-E=)	16-port 10-Gigabit Ethernet copper (RJ-45) module	
	With Supervisor Engine 2T-10GE	15.0(1)SY
WS-X6716-10T-3CXL (WS-X6716-10T with WS-F6700-DFC3CXL**)** **WS-X6716-10T-3C (WS-X6716-10T** with WS-F6700-DFC3C)	With Supervisor Engine 720-10GE	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

- The orderable product IDs are:
  - WS-X6816-10T-2TXL
  - WS-X6816-10T-2T
  - WS-X6716-10T-3CXL
  - WS-X6716-10T-3C
- The front panel is labeled WS-X6716-10T.
- Cisco IOS software commands display WS-X6716-10T with any DFC.
- dCEF720
- QoS port architecture (Rx/Tx):
  - Oversubscription mode: **1p7q2t/1p7q4t**
  - Performance mode: **8q4t/1p7q4t**
- Dual switch-fabric connections
  Fabric Channel #1: ports 1–8
  Fabric Channel #2: ports 9–16
- Number of ports: 16
  Number of port groups: 4
  Port ranges per port group: 1–4, 5–8, 9–12, 13–16
- When not configured in oversubscription mode, supported in virtual switch links.
- To configure port oversubscription, use the **hw-module slot** command.

WS-X6816-10G-2T, WS-X6716-10G 16-Port 10-Gigabit Ethernet X2 Switching Module

Product ID (append "=" for spares)	Product Description	Minimum Software Version
WS-X6816-10G-2TXL (Has WS-F6K-DFC4-EXL) **WS-X6716-10G-3CXL** (Must be upgraded with WS-F6K-DFC4-EXL=) **WS-X6816-10G-2T** (**Has** WS-F6K-DFC4-E) **WS-X6716-10G-3C** (Must be upgraded with WS-F6K-DFC4-E=)	16-port 10-Gigabit Ethernet X2 module	
	With Supervisor Engine 2T-10GE	15.0(1)SY
WS-X6716-10G-3CXL (**WS-X6716-10G with** WS-F6700-DFC3CXL) **WS-X6716-10G-3C** (**WS-X6716-10G** with WS-F6700-DFC3C)	With Supervisor Engine 720-10GE	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

- The orderable product IDs are:
  - WS-X6816-10G-2TXL
  - WS-X6816-10G-2T
  - WS-X6716-10G-3CXL
  - WS-X6716-10G-3C
- The front panel is labeled WS-X6716-10GE.
- Cisco IOS software commands display WS-X6716-10GE with any DFC.
- dCEF720
- QoS port architecture (Rx/Tx):
  - Oversubscription mode: **1p7q2t/1p7q4t**
  - Performance mode: **8q4t/1p7q4t**
- Dual switch-fabric connections
  Fabric Channel #1: ports 1–8
  Fabric Channel #2: ports 9–16
- Number of ports: 16
  Number of port groups: 4
  Port ranges per port group: 1–4, 5–8, 9–12, 13–16
- When not configured in oversubscription mode, supported in virtual switch links.
- To configure port oversubscription, use the **hw-module slot** command.
- With Supervisor Engine 720-10GE or Supervisor Engine 720 in a 13-slot chassis, supported only in slots 9 through 13 and does not power up in other slots.

WS-X6708-10GE 8-port 10-Gigabit Ethernet X2 Switching Module

Product ID (append "=" for spares)	Product Description	Minimum Software Versions
WS-X6708-10G-3C (WS-X6708-10GE with WS-F6700-DFC3C**)**	8-port 10-Gigabit Ethernet X2 module **Note** Not supported with Supervisor Engine 2T.	
WS-X6708-10G-3CXL (WS-X6708-10GE with WS-F6700-DFC3CXL**)**	With Supervisor Engine 720-10GE	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

- WS-X6708-10G-3C and WS-X6708-10G-3CXL are the orderable product IDs.
- The front panel is labeled WS-X6708-10GE.
- Cisco IOS software commands display WS-X6708-10GE with either WS-F6700-DFC3C or WS-F6700-DFC3CXL.
- dCEF720
- Supports egress multicast replication
- QoS port architecture (Rx/Tx):
  - Oversubscription mode: **1p7q2t/1p7q4t**
  - Performance mode: **8q4t/1p7q4t**
  - Both modes support DSCP-based queueing
- Dual switch-fabric connections
  Fabric Channel #1: Ports 2, 3, 6, 8
  Fabric Channel #2: Ports 1, 4, 5, 7
- Number of ports: 8
  Number of port groups: 8
  Port ranges per port group: 1 port in each group
- To configure WS-X6708-10GE port oversubscription, use the **hw-module oversubscription** command.
- WS-X6708-10GE ports do not support VACL capture. (CSCsb59015)
- In a 13-slot chassis, supported only in slots 9 through 13 and does not power up in other slots.

WS-X6704-10GE 4-Port 10-Gigabit Ethernet XENPAK Switching Module

Product ID (append "=" for spares)	Product Description	Minimum Software Version
WS-X6704-10G	4-port 10-Gigabit Ethernet XENPAK	
	With Supervisor Engine 2T-10GE	15.0(1)SY
	With Supervisor Engine 720-10GE	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

- WS-X6704-10GE requires one of the following:
  - With Supervisor Engine 2T-10GE:
    - WS-F6K-DFC4-AXL
    - WS-F6K-DFC4-A
  - With Supervisor Engine 720 or Supervisor Engine 720-10GE:
    - WS-F6700-DFC3CXL
    - WS-F6700-DFC3C
    - WS-F6700-DFC3BXL (not supported in virtual switch mode)
    - WS-F6700-DFC3B (not supported in virtual switch mode)
  - With any supervisor engine, WS-F6700-CFC
- dCEF720 with a DFC or CEF720 with a WS-F6700-CFC.
- Requires 512-MB DRAM with a WS-F6700-CFC (CSCtk82279). See this publication:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_12409.html
- QoS port architecture (Rx/Tx): **8q8t/1p7q8t**
- Dual switch-fabric connections:
  Fabric Channel #1: Ports 3 and 4
  Fabric Channel #2: Ports 1 and 2
- Number of ports: 4
  Number of port groups: 4
  Port ranges per port group: 1 port in each group
- WS-X6704-10G is the orderable product ID.
- The front panel is labeled WS-X6704-10GE.
- Cisco IOS software commands display WS-X6704-10GE with any DFC.
- On WS-X6704-10GE ports, STP BPDUs are not exempt from Traffic Storm Control multicast suppression. Do not configure multicast suppression on STP-protected WS-X6704-10GE ports that interconnect network devices. (CSCsg86315)
- With Supervisor Engine 720-10GE or Supervisor Engine 720 in a 13-slot chassis, supported only in slots 9 through 13 and does not power up in other slots.

WS-X6502-10GE 1-port 10-Gigabit Ethernet Switching Module

Product ID (append "=" for spares)	**Product Description**	**Minimum Software Versions**
WS-X6502-10GE	1-port 10-Gigabit Ethernet **Note** Not supported with Supervisor Engine 2T.	
	With Supervisor Engine 720-10GE (not supported in VSS mode)	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

Product ID (append "=" for spares)	Product Description	Minimum Software Versions
Optical Interface Module (OIM) for WS-X6502-10GE		
WS-G6488	10GBASE-LR serial 1310 nm long-reach OIM	
WS-G6483	10GBASE-ER serial 1550 nm extended-reach OIM	

- Not supported in virtual switch mode.
- dCEF256 with a DFC
- QoS port architecture (Rx/Tx): **1p1q8t/1p2q1t**
- Number of ports: 1
  Number of port groups: 1
  Port ranges per port group: 1 port in 1 group
- Use with a DFC requires DFC ROMMON version 12.2(18r)S1 or later. To display the switching module ROMMON version, enter the **remote command module** *module_slot_number* **show version | include ROM** command. To upgrade the switching module ROMMON, see this document:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/rommon/OL_6010.html

Cisco Catalyst 6880-X Series Extensible Fixed Aggregation Switches

Product ID (append "=" for spares)	Product Description	Minimum Software Version
C6880-X-LE	16 10-Gigabit (SFP+)/1-Gigabit ports (SFP), four port card slots, two power supply slots. It supports standard FIB/ACL/NetFlow tables.	15.1(2)SY1
C6880-X	16 10-Gigabit (SFP+)/1-Gigabit ports (SFP), four port card slots, two power supply slots. It supports large FIB/ACL/NetFlow tables.	
C6880-X-LE-16P10G[1]	Multi rate port card with standard tables. This module has 16 10-Gigabit or 1-Gigabit module slots which support 1-Gigabit SFPs or 10-Gigabit SFP+ modules. Supported only on the Catalyst 6880-X-LE switch model.	15.1(2)SY2
C6880-X-16P10G[1]	Multi rate port card with XL tables. This module has 16 10-Gigabit or 1-Gigabit module slots which support 1-Gigabit SFPs or 10-Gigabit SFP+s modules. Supported only on the Catalyst 6880-X switch model.	

Note See these publications for more information:

http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6880-x-switch/data_sheet_c78-728228.html

http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6880-x-switch/white_paper_c11-728540.html

http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6880-x-switch/white_paper_c11-728541.html

http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-1SY/config_guide/sup2T/15_1_sy_swcg_2T.html

1. These port cards are supported only on the specified switch models and are not interoperable.

Cisco Catalyst 6807-XL Modular Switch

Product ID (append "=" for spares)	Product Description	Minimum Software Version
C6807-XL	7-slot modular chassis. The switch supports redundant power supply modules (AC-input), redundant supervisor engines, fan-tray, power supply convertor modules, clock modules, and voltage termination enhanced (VTT-E) modules	15.1(2)SY3

Note See these publications for more information:

http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6807-xl-switch/data_sheet_c78-728229.html

http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6807-xl-switch/white_paper_c11-728264.html

http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-1SY/config_guide/sup2T/15_1_sy_swcg_2T.html

Instant Access Catalyst 6800ia Series Switches

Product ID (append "=" for spares)	Product Description	Minimum Software Version
Catalyst C6800IA-48FPDR	48-port 10/100/1000 RJ-45 PoE-capable Ethernet (24 ports up to 30W, 48 ports up to 15.4W, 740W total; dual power supplies) **Note** • ISSU upgrade or downgrade is not supported with C6800IA-48FPDR. • C6800IA-48FPDR does not support SNMP traps.	
	With Supervisor Engine 2T-10GE	15.1(2)SY3
Catalyst C6800IA-48FPD	48-port 10/100/1000 RJ-45 PoE-capable Ethernet (24 ports up to 30W, 48 ports up to 15.4W, 740W total)	
Catalyst C6800IA-48TD	48-port 10/100/1000 RJ-45 Ethernet	
	With Supervisor Engine 2T-10GE	15.1(2)SY

Note See these publications for more information:

http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6800ia-switch/data_sheet_c78-728230.html

http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6800ia-switch/white_paper_c11-728265.html

http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-1SY/config_guide/sup2T/15_1_sy_swcg_2T/instant_access.html

http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6800ia/hardware/installation/guide/b_c6800ia_hig.html

Gigabit Ethernet Switching Modules

WS-X6848-SFP-2T, WS-X6748-SFP 48-Port Gigabit Ethernet SFP Switching Module

Product ID (append "=" for spares)	**Product Description**	**Minimum Software Version**
WS-X6848-SFP-2TXL (has WS-F6K-DFC4-AXL) **WS-X6848-SFP-2T** (has WS-F6K-DFC4-A) **WS-X6748-SFP** (with WS-F6700-CFC, or upgraded with WS-F6K-DFC4-AXL or WS-F6K-DFC4-A)	48-port Gigabit Ethernet SFP	
	With Supervisor Engine 2T-10GE	15.0(1)SY
WS-X6748-SFP (with WS-F6700-DFC3CXL, WS-F6700-DFC3C, WS-F6700-DFC3BXL (not supported in virtual switch mode) WS-F6700-DFC3B (not supported in virtual switch mode) or WS-F6700-CFC)	With Supervisor Engine 720-10GE	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

- dCEF720 with a DFC or CEF720 with a WS-F6700-CFC.
- QoS architecture: **2q8t/1p3q8t**
- Dual switch-fabric connections
  Fabric Channel #1: Ports 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48
  Fabric Channel #2: Ports 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45, 47
- Number of ports: 48
  Number of port groups: 4
  Port ranges per port group:
  1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23

2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24
25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45, 47
26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48

- On WS-X6848-SFP-2T and WS-X6748-SFP ports, STP BPDUs are not exempt from Traffic Storm Control multicast suppression. Do not configure multicast suppression on STP-protected WS-X6848-SFP-2T or WS-X6748-SFP ports that interconnect network devices.
- With Supervisor Engine 720-10GE or Supervisor Engine 720 in a 13-slot chassis, supported only in slots 9 through 13 and does not power up in other slots.

WS-X6824-SFP-2T, WS-X6724-SFP 24-Port Gigabit Ethernet SFP Switching Module

Product ID (append "=" for spares)	**Product Description**	**Minimum Software Version**
WS-X6824-SFP-2TXL (Has WS-F6K-DFC4-AXL) **WS-X6824-SFP-2T** (Has WS-F6K-DFC4-A) **WS-X6724-SFP** (with WS-F6700-CFC, or upgraded with WS-F6K-DFC4-AXL or WS-F6K-DFC4-A)	24-port Gigabit Mbps Ethernet SFP	
	With Supervisor Engine 2T-10GE	15.0(1)SY
WS-X6724-SFP (with WS-F6700-DFC3CXL, WS-F6700-DFC3C, WS-F6700-DFC3BXL (not supported in virtual switch mode) WS-F6700-DFC3B (not supported in virtual switch mode) or WS-F6700-CFC)	With Supervisor Engine 720-10GE	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

- dCEF720 with a DFC or CEF720 with a WS-F6700-CFC.
- QoS architecture: **2q8t/1p3q8t**
- Number of ports: 24
  Number of port groups: 2
  Port ranges per port group: 1–12, 13–24
- On WS-X6824-SFP-2T and WS-X6724-SFP ports, STP BPDUs are not exempt from Traffic Storm Control multicast suppression. Do not configure multicast suppression on STP-protected WS-X6824-SFP-2T or WS-X6724-SFP ports that interconnect network devices.

WS-X6816-GBIC 16-port Gigabit Ethernet GBIC Switching Module

Product ID (append "=" for spares)	Product Description	Minimum Software Versions
WS-X6816-GBIC	16-port Gigabit Ethernet GBIC **Note** Not supported with Supervisor Engine 2T.	
	With Supervisor Engine 720-10GE (not supported in VSS mode)	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

- dCEF256
- QoS port architecture (Rx/Tx): **1p1q4t/1p2q2t**
- Dual switch-fabric connections
  Fabric Channel #1: Ports 1–8
  Fabric Channel #2: Ports 9–16
- Number of ports: 16
  Number of port groups: 2
  Port ranges per port group: 1–8, 9–16
- WS-X6816-GBIC requires one of these:
  - WS-F6K-DFC3BXL
  - WS-F6K-DFC3B
- Requires DFC ROMMON version 12.2(18r)S1 or later. To display the switching module ROMMON version, enter the **remote command module** *module_slot_number* **show version | include ROM** command. To upgrade the switching module ROMMON, see this document:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/rommon/OL_6010.html
- In a 13-slot chassis, supported only in slots 9 through 13 and does not power up in other slots.

WS-X6516A-GBIC 16-Port Gigabit Ethernet GBIC Switching Module

Product ID (append "=" for spares)	Product Description	Minimum Software Versions
WS-X6516A-GBIC	16-port Gigabit Ethernet GBIC **Note** Not supported with Supervisor Engine 2T.	
	With Supervisor Engine 720-10GE (not supported in VSS mode)	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

- dCEF256 with a DFC
- CEF256
- Supports egress multicast replication
- QoS port architecture (Rx/Tx): **1p1q4t/1p2q2t**
- Number of ports: 16
  Number of port groups: 2
  Port ranges per port group: 1–8, 9–16
- Requires DFC ROMMON version 12.2(18r)S1 or later. To display the switching module ROMMON version, enter the **remote command module** *module_slot_number* **show version | include ROM** command. To upgrade the switching module ROMMON, see this document:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/rommon/OL_6010.html

WS-X6516-GBIC 16-Port Gigabit Ethernet GBIC Switching Module

Product ID (append "=" for spares)	**Product Description**	**Minimum Software Versions**
WS-X6516-GBIC	16-port Gigabit Ethernet GBIC **Note** Not supported with Supervisor Engine 2T.	
	With Supervisor Engine 720-10GE (not supported in VSS mode)	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

- dCEF256 with a DFC
- CEF256
- QoS port architecture (Rx/Tx): **1p1q4t/1p2q2t**
- Number of ports: 16
  Number of port groups: 2
  Port ranges per port group: 1–8, 9–16
- Requires DFC ROMMON version 12.2(18r)S1 or later. To display the switching module ROMMON version, enter the **remote command module** *module_slot_number* **show version | include ROM** command. To upgrade the switching module ROMMON, see this document:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/rommon/OL_6010.html
- Supervisor Engine 720 supports a DFC3 on these WS-X6516-GBIC hardware revisions:
  - Lower than 5.0
  - 5.5 and higher

- Supervisor Engine 720 does not support a DFC3 on WS-X6516-GBIC hardware revisions 5.0 through 5.4. With a Supervisor Engine 720 and with a DFC3 installed, WS-X6516-GBIC hardware revisions 5.0 through 5.4 do not power up.
- With a Supervisor Engine 720 but without a DFC3, WS-X6516-GBIC hardware revisions 5.0 through 5.4 operate in bus mode.
- See external field notice 24494 for more information:

  http://www.cisco.com/c/en/us/support/docs/field-notices/200/fn24494.html

WS-X6416-GBIC 16-port Gigabit Ethernet GBIC Switching Module

Product ID (append "=" for spares)	**Product Description**	**Minimum Software Versions**
WS-X6416-GBIC	16-port Gigabit Ethernet GBIC **Note** Not supported with Supervisor Engine 2T.	
	With Supervisor Engine 720-10GE (not supported in VSS mode)	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

- QoS port architecture (Rx/Tx): **1p1q4t/1p2q2t**
- Number of ports: 16
  Number of port groups: 2
  Port ranges per port group: 1–8, 9–16

WS-X6408A-GBIC 8-port Gigabit Ethernet GBIC Switching Module

Product ID (append "=" for spares)	**Product Description**	**Minimum Software Versions**
WS-X6408A-GBIC	8-port Gigabit Ethernet GBIC **Note** Not supported with Supervisor Engine 2T.	
	With Supervisor Engine 720-10GE (not supported in VSS mode)	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

- QoS port architecture (Rx/Tx): **1p1q4t/1p2q2t**
- Number of ports: 8
  Number of port groups: 1
  Port ranges per port group: 1–8

WS-X6408-GBIC 8-port Gigabit Ethernet GBIC Switching Module

Product ID (append "=" for spares)	Product Description	Minimum Software Versions
WS-X6408-GBIC	8-port Gigabit Ethernet GBIC **Note** Not supported with Supervisor Engine 2T.	
	With Supervisor Engine 720-10GE (not supported in VSS mode)	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

- QoS port architecture (Rx/Tx): **1q4t/2q2t**
- Number of ports: 8
  Number of port groups: 1
  Port ranges per port group: 1–8

10/100/1000 Ethernet Switching Modules

These sections descibe the supported 10/100/1000 Ethernet switching modules:

- WS-X6848-TX-2T, WS-X6748-GE-TX, page 37
- WS-X6548-GE-TX, WS-X6548V-GE-TX, WS-X6548-GE-45AF, page 38
- WS-X6148E-GE-45AT, page 39
- WS-X6148A-GE-TX, WS-X6148A-GE-45AF, page 40
- WS-X6148-GE-TX, WS-X6148V-GE-TX, WS-X6148-GE-45AF, page 40
- WS-X6516-GE-TX, page 41

WS-X6848-TX-2T, WS-X6748-GE-TX

Product ID (append "=" for spares)	Product Description	Minimum Software Version
WS-X6848-TX-2TXL (has WS-F6K-DFC4-AXL) **WS-X6848-TX-2T** (has WS-F6K-DFC4-A) **WS-X6748-GE-TX**	48-port 10/100/1000 RJ-45	
	With Supervisor Engine 2T-10GE	15.0(1)SY
WS-X6748-GE-TX	With Supervisor Engine 720-10GE	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

- dCEF720 with a DFC or CEF720 with a WS-F6700-CFC.
- WS-X6704-10GE requires one of the following:
  - With Supervisor Engine 2T-10GE:
    - WS-F6K-DFC4-AXL
    - WS-F6K-DFC4-A
  - With Supervisor Engine 720 or Supervisor Engine 720-10GE:
    - WS-F6700-DFC3CXL
    - WS-F6700-DFC3C
    - WS-F6700-DFC3BXL (not supported in virtual switch mode)
    - WS-F6700-DFC3B (not supported in virtual switch mode)
  - With any supervisor engine, WS-F6700-CFC
- QoS architecture: **2q8t/1p3q8t**
- Dual switch-fabric connections
  Fabric Channel #1: Ports 25–48
  Fabric Channel #2: Ports 1–24
- Number of ports: 48
  Number of port groups: 4
  Port ranges per port group: 1–12, 13–24, 25–36, 37–48
- On WS-X6848-TX-2T and WS-X6748-GE-TX ports, STP BPDUs are not exempt from Traffic Storm Control multicast suppression. Do not configure multicast suppression on STP-protected WS-X6848-TX-2T or WS-X6748-GE-TX ports that interconnect network devices.
- With Supervisor Engine 720-10GE or Supervisor Engine 720 in a 13-slot chassis, WS-X6748-GE-TX is supported only in slots 9 through 13 and does not power up in other slots.

WS-X6548-GE-TX, WS-X6548V-GE-TX, WS-X6548-GE-45AF

Product ID (append "=" for spares)	**Product Description**	**Minimum Software Versions**
WS-X6548-GE-TX **WS-X6548V-GE-TX** **WS-X6548-GE-45AF**	48-port 10/100/1000 Mbps **Note** Not supported with Supervisor Engine 2T.	
	With Supervisor Engine 720-10GE (not supported in VSS mode)	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

- Supports more than 1 Gbps of traffic per EtherChannel on the WS-X6548-GE-TX (and voice-power daughtercard equipped) switching modules.
- WS-X6548-GE-TX (and voice-power daughtercard equipped) switching modules do not support these features:
  - Jumbo frames
  - 802.1Q tunneling

  - Traffic storm control
- RJ-45
- CEF256
- WS-X6548-GE-TX supports:
  - WS-F6K-VPWR-GE
  - WS-F6K-GE48-AF
  - WS-F6K-48-AF
- WS-X6548V-GE-TX has WS-F6K-VPWR-GE
- WS-X6548-GE-45AF has WS-F6K-GE48-AF or WS-F6K-48-AF
- With WS-F6K-GE48-AF, supports up to 45 ports of ePoE (16.8W).
- QoS port architecture (Rx/Tx): **1q2t/1p2q2t**
- Number of ports: 48
  Number of port groups: 2
  Port ranges per port group: 1–24, 25–48
- The aggregate bandwidth of each set of 8 ports (1–8, 9–16, 17–24, 25–32, 33–40, and 41–48) is 1 Gbps.

WS-X6148E-GE-45AT

Product ID (append "=" for spares)	**Product Description**	**Minimum Software Version**
WS-X6148E-GE-45AT	48-port 10/100/1000 Mbps	
	With Supervisor Engine 2T-10GE	15.0(1)SY
	With Supervisor Engine 2T-10GE in VSS mode	15.1(1)SY

- RJ-45
- WS-X6148E-GE-45AT with WS-F6K-48-AT supports up to 48 ports of Class 4 PoE+ (30.0W).
- QoS port architecture (Rx/Tx): **1q2t/1p3q8t**
- Number of ports: 48
  Number of port groups: 6
  Port ranges per port group: 1–8, 9–16, 17–24, 25–32, 33–40, 41–48
- The aggregate bandwidth of each set of 8 ports (1–8, 9–16, 17–24, 25–32, 33–40, and 41–48) is 1 Gbps.
- WS-X6148E-GE-45AT does not support traffic storm control

WS-X6148A-GE-TX, WS-X6148A-GE-45AF

Product ID (append "=" for spares)	Product Description	Minimum Software Version
WS-X6148A-GE-TX **WS-X6148A-GE-45AF**	48-port 10/100/1000 Mbps	
	With Supervisor Engine 2T-10GE (not supported in VSS mode)	15.0(1)SY
	With Supervisor Engine 720-10GE (not supported in VSS mode)	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

- RJ-45
- WS-X6148A-GE-TX supports WS-F6K-GE48-AF or WS-F6K-48-AF
- WS-X6148A-GE-45AF has WS-F6K-GE48-AF or WS-F6K-48-AF
- With WS-F6K-GE48-AF, supports up to 45 ports of ePoE (16.8W).
- QoS port architecture (Rx/Tx): **1q2t/1p3q8t**
- Number of ports: 48
  Number of port groups: 6
  Port ranges per port group: 1–8, 9–16, 17–24, 25–32, 33–40, 41–48
- The aggregate bandwidth of each port group is 1 Gbps.
- Does not support traffic storm control.

WS-X6148-GE-TX, WS-X6148V-GE-TX, WS-X6148-GE-45AF

Product ID (append "=" for spares)	Product Description	Minimum Software Versions
WS-X6148-GE-TX **WS-X6148V-GE-TX** **WS-X6148-GE-45AF**	48-port 10/100/1000 Mbps **Note** Not supported with Supervisor Engine 2T.	
	With Supervisor Engine 720-10GE (not supported in VSS mode)	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

- RJ-45
- WS-X6148-GE-TX supports:
  - WS-F6K-VPWR-GE
  - WS-F6K-GE48-AF
  - WS-F6K-48-AF

- WS-X6148V-GE-TX has WS-F6K-VPWR-GE
- WS-X6148-GE-45AF has WS-F6K-GE48-AF or WS-F6K-48-AF
- With WS-F6K-GE48-AF, supports up to 45 ports of ePoE (16.8W).
- QoS port architecture (Rx/Tx): **1q2t/1p2q2t**
- Number of ports: 48
  Number of port groups: 2
  Port ranges per port group: 1–24, 25–48
- The aggregate bandwidth of each port group is 1 Gbps.
- WS-X6148-GE-TX, WS-X6148V-GE-TX, and WS-X6148-GE-45AF do not support these features:
  - More than 1 Gbps of traffic per EtherChannel
  - Jumbo frames
  - 802.1Q tunneling
  - Traffic storm control

WS-X6516-GE-TX

Product ID (append "=" for spares)	**Product Description**	**Minimum Software Versions**
WS-X6516-GE-TX	16-port 10/100/1000BASE-T **Note** Not supported with Supervisor Engine 2T.	
	With Supervisor Engine 720-10GE (not supported in VSS mode)	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

- dCEF256 with a DFC
- CEF256
- QoS port architecture (Rx/Tx): **1p1q4t/1p2q2t**
- Number of ports: 16
  Number of port groups: 2
  Port ranges per port group: 1–8, 9–16

100MB Ethernet Switching Modules

- WS-X6148-FE-SFP, page 42
- WS-X6524-100FX-MM, page 42
- WS-X6324-100FX-MM, page 43

WS-X6148-FE-SFP

Product ID (append "=" for spares)	Product Description	Minimum Software Version
WS-X6148-FE-SFP	48-port 100BASE-FX	
	With Supervisor Engine 2T-10GE (not supported in VSS mode)	15.0(1)SY
	With Supervisor Engine 720-10GE (not supported in VSS mode)	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

- Requires Fast Ethernet SFPs
- QoS port architecture (Rx/Tx): **1p1q4t/1p3q8t**
- Number of ports: 48
  Number of port groups: 3
  Port ranges per port group: 1–16, 17–32, and 33–48
- Does not support traffic storm control.

WS-X6524-100FX-MM

Product ID (append "=" for spares)	Product Description	Minimum Software Versions
WS-X6524-100FX-MM	24-port 100FX Ethernet multimode **Note** Not supported with Supervisor Engine 2T.	
	With Supervisor Engine 720-10GE (not supported in VSS mode)	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

- dCEF256 with a DFC
- CEF256
- QoS port architecture (Rx/Tx): **1p1q0t/1p3q1t**
- Number of ports: 24
  Number of port groups: 1
  Port ranges per port group: 1–24

WS-X6324-100FX-MM

Product ID (append "=" for spares)	Product Description	Minimum Software Versions
WS-X6324-100FX-MM	24-port 100FX Ethernet **Note** Not supported with Supervisor Engine 2T.	
	With Supervisor Engine 720-10GE (not supported in VSS mode)	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

- Single mode and multimode MT-RJ
- 128-KB per-port packet buffers
- QoS port architecture (Rx/Tx): **1q4t/2q2t**
- Number of ports: 24
  Number of port groups: 2
  Port ranges per port group: 1–12, 13–24

10/100MB Ethernet Switching Modules

WS-X6548-RJ-45

Product ID (append "=" for spares)	Product Description	Minimum Software Versions
WS-X6548-RJ-45	48-port 10/100TX RJ-45 **Note** Not supported with Supervisor Engine 2T.	
	With Supervisor Engine 720-10GE (not supported in VSS mode)	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

- dCEF256 with a DFC or CEF256
- QoS port architecture (Rx/Tx): **1p1q0t/1p3q1t**
- Number of ports: 48
  Number of port groups: 1
  Port ranges per port group: 1–48

WS-X6548-RJ-21

Product ID (append "=" for spares)	Product Description	Minimum Software Versions
WS-X6548-RJ-21	48-port 10/100TX RJ-21 **Note** Not supported with Supervisor Engine 2T.	
	With Supervisor Engine 720-10GE (not supported in VSS mode)	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

- dCEF256 with a DFC or CEF256
- QoS port architecture (Rx/Tx): **1p1q0t/1p3q1t**
- Number of ports: 48
  Number of port groups: 1
  Port ranges per port group: 1–48

WS-X6148X2-RJ-45, WS-X6148X2-45AF

Product ID (append "=" for spares)	Product Description	Minimum Software Versions
WS-X6148X2-RJ-45 **WS-X6148X2-45AF**	96-port 10/100TX RJ-45 **Note** Not supported with Supervisor Engine 2T.	
	With Supervisor Engine 720-10GE (not supported in VSS mode)	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

- QoS port architecture (Rx/Tx): **1p1q0t/1p3q1t**
- WS-X6148X2-RJ-45 supports WS-F6K-FE48X2-AF
- WS-X6148X2-45AF has WS-F6K-FE48X2-AF

WS-X6196-RJ-21, WS-X6196-21AF

Product ID (append "=" for spares)	Product Description	Minimum Software Versions
WS-X6196-RJ-21 **WS-X6196-21AF**	96-port 10/100TX RJ-21	
	With Supervisor Engine 2T-10GE (not supported in VSS mode)	15.0(1)SY1
	With Supervisor Engine 720-10GE (not supported in VSS mode)	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

- Upgrade to Release15.0(1)SY1 or later before installing WS-X6196-21AF (see the "EFSU Compatibility" section on page 68).
- QoS port architecture (Rx/Tx): **1p1q0t/1p3q1t**
- WS-X6196-RJ-21 supports WS-F6K-FE48X2-AF
- WS-X6196-21AF has WS-F6K-FE48X2-AF

WS-X6348-RJ-45, WS-X6348-RJ-45V

Product ID (append "=" for spares)	Product Description	Minimum Software Versions
WS-X6348-RJ-45 **WS-X6348-RJ-45V**	48-port 10/100TX RJ-45 **Note** Not supported with Supervisor Engine 2T.	
	With Supervisor Engine 720-10GE	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

- Not supported in VSS mode.
- QoS port architecture (Rx/Tx): **1q4t/2q2t**
- WS-X6348-RJ-45 supports WS-F6K-VPWR
- WS-X6348-RJ-45V has WS-F6K-VPWR
- Number of ports: 48
  Number of port groups: 4
  Port ranges per port group: 1–12, 13–24, 25–36, 37–48

WS-X6348-RJ-21V

Product ID (append "=" for spares)	Product Description	Minimum Software Versions
WS-X6348-RJ-21V	48-port 10/100TX RJ-21 **Note** Not supported with Supervisor Engine 2T.	
	With Supervisor Engine 720-10GE	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

- Not supported in VSS mode.
- QoS port architecture (Rx/Tx): **1q4t/2q2t**
- Has WS-F6K-VPWR
- Number of ports: 48
  Number of port groups: 4
  Port ranges per port group: 1–12, 13–24, 25–36, 37–48

WS-X6148A-RJ-45, WS-X6148A-45AF

Product ID (append "=" for spares)	Product Description	Minimum Software Version
WS-X6148A-RJ-45 **WS-X6148A-45AF**	48-port 10/100TX RJ-45	
	With Supervisor Engine 2T-10GE (not supported in VSS mode)	15.0(1)SY
	With Supervisor Engine 720-10GE (not supported in VSS mode)	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

- QoS port architecture (Rx/Tx): **1p1q4t/1p3q8t**
- WS-X6148A-RJ-45 supports WS-F6K-GE48-AF or WS-F6K-48-AF
- WS-X6148A-45AF has WS-F6K-GE48-AF or WS-F6K-48-AF
- Number of ports: 48
  Number of port groups: 6
  Port ranges per port group: 1–8, 9–16, 17–24, 25–32, 33–40, 41–48

WS-X6148-RJ-45, WS-X6148-RJ45V, WS-X6148-45AF

Product ID (append "=" for spares)	Product Description	Minimum Software Versions
WS-X6148-RJ-45 **WS-X6148-RJ45V** **WS-X6148-45AF**	48-port 10/100TX RJ-45 **Note** Not supported with Supervisor Engine 2T.	
	With Supervisor Engine 720-10GE (not supported in VSS mode)	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

- QoS port architecture (Rx/Tx): **1q4t/2q2t**
- WS-X6148-RJ-45 supports WS-F6K-VPWR
- WS-X6148-RJ-45V has WS-F6K-VPWR
- WS-X6148-45AF has WS-F6K-48-AF
- Number of ports: 48
  Number of port groups: 4
  Port ranges per port group: 1–12, 13–24, 25–36, 37–48

WS-X6148-RJ-21, WS-X6148-RJ21V, WS-X6148-21AF

Product ID (append "=" for spares)	Product Description	Minimum Software Versions
WS-X6148-RJ-21 **WS-X6148-RJ21V** **WS-X6148-21AF**	48-port 10/100TX RJ-21 **Note** Not supported with Supervisor Engine 2T.	
	With Supervisor Engine 720-10GE (not supported in VSS mode)	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

- QoS port architecture (Rx/Tx): **1q4t/2q2t**
- WS-X6148-RJ-21 supports WS-F6K-VPWR
- WS-X6148-RJ-21V has WS-F6K-VPWR
- WS-X6148-21AF has WS-F6K-48-AF
- Number of ports: 48
  Number of port groups: 4
  Port ranges per port group: 1–12, 13–24, 25–36, 37–48

Power over Ethernet Daughtercards

WS-F6K-GE48-AF, WS-F6K-48-AF

Product ID (append "=" for spares)	**Product Description**	**Minimum Software Versions**
WS-F6K-GE48-AF **WS-F6K-48-AF**	IEEE 802.3af PoE daughtercard for: • WS-X6548-GE-TX • WS-X6148-GE-TX • WS-X6148A-GE-TX • WS-X6148A-RJ-45	
	With Supervisor Engine 2T-10GE	15.0(1)SY
	With Supervisor Engine 720-10GE	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

- WS-F6K-GE48-AF and WS-F6K-48-AF are not FRUs for these switching modules:
  - WS-X6148-RJ-45 or WS-X6148-RJ-45V (replace with WS-X6148-45AF-UG=).
  - WS-X6148-RJ-21 or WS-X6148-RJ-21V (replace with WS-X6148-21AF-UG=).
- With WS-X6548-GE-TX, WS-X6148-GE-TX, and WS-X6148A-GE-TX, supports up to 45 ports of ePoE (16.8W).

WS-F6K-FE48X2-AF

Product ID (append "=" for spares)	**Product Description**	**Minimum Software Versions**
WS-F6K-FE48X2-AF	IEEE 802.3af PoE daughtercard for WS-X6148X2-RJ-45 and WS-X6196-RJ-21	
	With Supervisor Engine 720-10GE	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

WS-F6K-VPWR-GE

Product ID (append "=" for spares)	Product Description	Minimum Software Versions
WS-F6K-VPWR-GE	Prestandard PoE daughtercard for WS-X6548-GE-TX and WS-X6148-GE-TX	
	With Supervisor Engine 720-10GE	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

WS-F6K-VPWR

Product ID (append "=" for spares)	Product Description	Minimum Software Versions
WS-F6K-VPWR	Prestandard PoE daughtercard for: • WS-X6348-RJ-45 • WS-X6348-RJ-21V • WS-X6148-RJ-45 • WS-X6148-RJ-21	
	With Supervisor Engine 720-10GE	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

Transceivers

CFP Modules

Product ID (append "=" for spares)	Product Description	Minimum Software Version
CFP-40G-LR4	40GBASE-LR4	15.0(1)SY1

Product ID (append "=" for spares)	Product Description	Minimum Software Version
CFP-40G-SR4	40GBASE-SR4	15.0(1)SY1
CVR-CFP-4SFP10G	FourX coverter to convert each 40GE port into 4 10GE SFP+ ports	15.0(1)SY1

X2 Modules

Note

- WS-X6716-10G and WS-X6708-10GE do not support X2 modules that are labeled with a number that ends with -01. (This restriction does not apply to X2-10GB-LRM.)
- All X2 modules shipped since WS-X6716-10G became available provide EMI compliance with WS-X6816-10G and WS-X6716-10G.
- Some X2 modules shipped before WS-X6716-10G became available might not provide EMI compliance with WS-X6816-10G and WS-X6716-10G. See the information listed for each type of X2 module in the following table.
- For information about X2 modules, see the *Cisco 10GBASE X2 Modules* data sheet:

  http://www.cisco.com/c/en/us/products/collateral/interfaces-modules/10-gigabit-modules/product_data_sheet0900aecd801f92aa.html

Product ID (append "=" for spares)	Product Description		Minimum Software Version
CVR-X2-SFP10G	10G X2 to SFP+ Converter		15.0(1)SY
DWDM-X2-60.61=	10GBASE-DWDM 1560.61 nm X2 (100-GHz ITU grid)	ITU 21	15.0(1)SY
DWDM-X2-59.79=	10GBASE-DWDM 1559.79 nm X2 (100-GHz ITU grid)	ITU 22	15.0(1)SY
DWDM-X2-58.98=	10GBASE-DWDM 1558.98 nm X2 (100-GHz ITU grid)	ITU 23	15.0(1)SY
DWDM-X2-58.17=	10GBASE-DWDM 1558.17 nm X2 (100-GHz ITU grid)	ITU 24	15.0(1)SY
DWDM-X2-56.55=	10GBASE-DWDM 1556.55 nm X2 (100-GHz ITU grid)	ITU 26	15.0(1)SY
DWDM-X2-55.75=	10GBASE-DWDM 1555.75 nm X2 (100-GHz ITU grid)	ITU 27	15.0(1)SY
DWDM-X2-54.94=	10GBASE-DWDM 1554.94 nm X2 (100-GHz ITU grid)	ITU 28	15.0(1)SY
DWDM-X2-54.13=	10GBASE-DWDM 1554.13 nm X2 (100-GHz ITU grid)	ITU 29	15.0(1)SY
DWDM-X2-52.52=	10GBASE-DWDM 1552.52 nm X2 (100-GHz ITU grid)	ITU 31	15.0(1)SY
DWDM-X2-51.72=	10GBASE-DWDM 1551.72 nm X2 (100-GHz ITU grid)	ITU 32	15.0(1)SY
DWDM-X2-50.92=	10GBASE-DWDM 1550.92 nm X2 (100-GHz ITU grid)	ITU 33	15.0(1)SY
DWDM-X2-50.12=	10GBASE-DWDM 1550.12 nm X2 (100-GHz ITU grid)	ITU 34	15.0(1)SY
DWDM-X2-48.51=	10GBASE-DWDM 1548.51 nm X2 (100-GHz ITU grid)	ITU 36	15.0(1)SY
DWDM-X2-47.72=	10GBASE-DWDM 1547.72 nm X2 (100-GHz ITU grid)	ITU 37	15.0(1)SY
DWDM-X2-46.92=	10GBASE-DWDM 1546.92 nm X2 (100-GHz ITU grid)	ITU 38	15.0(1)SY

Product ID (append "=" for spares)	Product Description		Minimum Software Version
DWDM-X2-46.12=	10GBASE-DWDM 1546.12 nm X2 (100-GHz ITU grid)	ITU 39	15.0(1)SY
DWDM-X2-44.53=	10GBASE-DWDM 1544.53 nm X2 (100-GHz ITU grid)	ITU 41	15.0(1)SY
DWDM-X2-43.73=	10GBASE-DWDM 1543.73 nm X2 (100-GHz ITU grid)	ITU 42	15.0(1)SY
DWDM-X2-42.94=	10GBASE-DWDM 1542.94 nm X2 (100-GHz ITU grid)	ITU 43	15.0(1)SY
DWDM-X2-42.14=	10GBASE-DWDM 1542.14 nm X2 (100-GHz ITU grid)	ITU 44	15.0(1)SY
DWDM-X2-40.56=	10GBASE-DWDM 1540.56 nm X2 (100-GHz ITU grid)	ITU 46	15.0(1)SY
DWDM-X2-39.77=	10GBASE-DWDM 1539.77 nm X2 (100-GHz ITU grid)	ITU 47	15.0(1)SY
DWDM-X2-38.98=	10GBASE-DWDM 1538.98 nm X2 (100-GHz ITU grid)	ITU 48	15.0(1)SY
DWDM-X2-38.19=	10GBASE-DWDM 1538.19 nm X2 (100-GHz ITU grid)	ITU 49	15.0(1)SY
DWDM-X2-36.61=	10GBASE-DWDM 1536.61 nm X2 (100-GHz ITU grid)	ITU 51	15.0(1)SY
DWDM-X2-35.82=	10GBASE-DWDM 1535.82 nm X2 (100-GHz ITU grid)	ITU 52	15.0(1)SY
DWDM-X2-35.04=	10GBASE-DWDM 1535.04 nm X2 (100-GHz ITU grid)	ITU 53	15.0(1)SY
DWDM-X2-34.25=	10GBASE-DWDM 1534.25 nm X2 (100-GHz ITU grid)	ITU 54	15.0(1)SY
DWDM-X2-32.68=	10GBASE-DWDM 1532.68 nm X2 (100-GHz ITU grid)	ITU 56	15.0(1)SY
DWDM-X2-31.90=	10GBASE-DWDM 1531.90 nm X2 (100-GHz ITU grid)	ITU 57	15.0(1)SY
DWDM-X2-31.12=	10GBASE-DWDM 1531.12 nm X2 (100-GHz ITU grid)	ITU 58	15.0(1)SY
DWDM-X2-30.33=	10GBASE-DWDM 1530.33 nm X2 (100-GHz ITU grid)	ITU 59	15.0(1)SY
X2-10GB-T	10GBASE-T X2 Module for CAT6A/CAT7 copper cable		15.1(1)SY
X2-10GB-ZR	10GBASE-ZR X2 Module for SMF		15.0(1)SY
X2-10GB-CX4	10GBASE for CX4 (copper) cable		15.0(1)SY
X2-10GB-ER	10GBASE-ER Serial 1550-nm extended-reach, single-mode fiber (SMF), dispersion-shifted fiber (DSF) **Note** X2-10GB-ER modules labeled with a number that ends with -02 do not provide EMI compliance with WS-X6716-10G.		15.0(1)SY
X2-10GB-LR	10GBASE-LR Serial 1310-nm long-reach, single-mode fiber (SMF), dispersion-shifted fiber (DSF) **Note** X2-10GB-LR modules labeled with a number that ends with -02 or -03 do not provide EMI compliance with WS-X6716-10G.		15.0(1)SY
X2-10GB-LRM	10GBASE-LRM for FDDI-grade multimode fiber (MMF) **Note** Not supported by the **show idprom** command. (CSCsj35671)		15.0(1)SY
X2-10GB-LX4	10GBASE-LX4 Serial 1310-nm multimode (MMF) **Note** • See field notice 62840 for information about unsupported 10GBASE-LX4 modules: http://www.cisco.com/c/en/us/support/docs/field-notices/misc/FN62840.html • X2-10GB-LX4 modules labeled with a number that ends with -01 to -03 do not provide EMI compliance with WS-X6716-10G.		15.0(1)SY

Product ID (append "=" for spares)	Product Description	Minimum Software Version
X2-10GB-SR	10GBASE-SR Serial 850-nm short-reach multimode (MMF)	15.0(1)SY

10 GE SFP+ Modules

Product ID (append "" for spares)	Product Description	Minimum Software Version
SFP-10G-ZR	10GBASE-ZR SFP+ for 1550 nm SMF	15.1(2)SY3
DWDM-SFP10G-61.41	10GBASE-DWDM 1561.41 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-60.61	10GBASE-DWDM 1560.61 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-59.79	10GBASE-DWDM 1559.79 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-58.98	10GBASE-DWDM 1558.98 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-58.17	10GBASE-DWDM 1558.17 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-57.36	10GBASE-DWDM 1557.36 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-56.55	10GBASE-DWDM 1556.55 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-55.75	10GBASE-DWDM 1555.75 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-54.94	10GBASE-DWDM 1554.94 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-54.13	10GBASE-DWDM 1554.13 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-53.33	10GBASE-DWDM 1553.33 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-52.52	10GBASE-DWDM 1552.52 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-51.72	10GBASE-DWDM 1551.72 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-50.92	10GBASE-DWDM 1550.92 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-50.12	10GBASE-DWDM 1550.12 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-49.32	10GBASE-DWDM 1549.32 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-48.51	10GBASE-DWDM 1548.51 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-47.72	10GBASE-DWDM 1547.72 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-46.92	10GBASE-DWDM 1546.92 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-46.12	10GBASE-DWDM 1546.12 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-45.32	10GBASE-DWDM 1545.32 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-44.53	10GBASE-DWDM 1544.53 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-43.73	10GBASE-DWDM 1543.73 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-42.94	10GBASE-DWDM 1542.94 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-42.14	10GBASE-DWDM 1542.14 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-41.35	10GBASE-DWDM 1541.35 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-40.56	10GBASE-DWDM 1540.56 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-39.77	10GBASE-DWDM 1539.77 nm SFP+ (100-GHz ITU grid)	15.1(2)SY

Product ID (append “” for spares)	Product Description	Minimum Software Version
DWDM-SFP10G-38.98	10GBASE-DWDM 1538.98 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-38.19	10GBASE-DWDM 1538.19 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-37.40	10GBASE-DWDM 1537.40 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-36.61	10GBASE-DWDM 1536.61 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-35.82	10GBASE-DWDM 1535.82 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-35.04	10GBASE-DWDM 1535.04 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-34.25	10GBASE-DWDM 1534.25 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-33.47	10GBASE-DWDM 1533.47 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-32.68	10GBASE-DWDM 1532.68 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-31.90	10GBASE-DWDM 1531.90 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-31.12	10GBASE-DWDM 1531.12 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-30.33	10GBASE-DWDM 1530.33 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
SFP-10G-LR	10GBASE-LR for 1310 nm SMF	15.0(1)SY1
SFP-10G-ER	10GBASE-ER for 1550 nm SMF	15.0(1)SY1
SFP-10G-LRM	10GBASE-LRM 1310 nm MMF and SMF	15.0(1)SY
SFP-10G-SR	10GBASE-SR 850 nm MMF	15.0(1)SY
SFP-H10GB-CU1M	1m Twinax cable, passive, 30AWG cable assembly	15.0(1)SY
SFP-H10GB-CU3M	3m Twinax cable, passive, 30AWG cable assembly	15.0(1)SY
SFP-H10GB-CU5M	5m Twinax cable, passive, 24AWG cable assembly	15.0(1)SY

XENPAKs

Note

- For information about DWDM XENPAKs, see the *Cisco 10GBase DWDM XENPAK Modules* data sheet:

  http://www.cisco.com/c/en/us/products/collateral/interfaces-modules/dwdm-transceiver-modules/product_data_sheet0900aecd801f9333.html

- For information about other XENPAKs, see the *Cisco 10GBASE XENPAK Modules* data sheet:

  http://www.cisco.com/c/en/us/products/collateral/interfaces-modules/catalyst-6500-series-supervisor-engine-720/product_data_sheet09186a008007cd00.html

Product ID (append “=” for spares)	Product Description	Minimum Software Version
XENPAK-10GB-LRM	10GBASE-LRM XENPAK Module for MMF **Note** Not supported by the **show idprom** command. (CSCsl21260)	15.0(1)SY

Product ID (append "=" for spares)	Product Description	Minimum Software Version
DWDM-XENPAK	10GBASE dense wavelength-division multiplexing (DWDM) 100-GHz ITU grid	15.0(1)SY
WDM-XENPAK-REC	10GBASE receive-only wavelength division multiplexing (WDM)	15.0(1)SY
XENPAK-10GB-CX4	10GBASE for CX4 (copper) cable; uses Infiniband connectors	15.0(1)SY
XENPAK-10GB-ER	10GBASE-ER Serial 1550-nm extended-reach, single-mode fiber (SMF), dispersion-shifted fiber (DSF) **Note** XENPAK-10GB-ER units with Part No. 800-24557-01 are not supported, as described in this external field notice (CSCee47030): http://www.cisco.com/c/en/us/support/docs/field-notices/200/fn29736.html	15.0(1)SY
XENPAK-10GB-ER+	10GBASE-ER Serial 1550-nm extended-reach, single-mode fiber (SMF), dispersion-shifted fiber (DSF)	15.0(1)SY
XENPAK-10GB-LR	10GBASE-LR Serial 1310-nm long-reach, single-mode fiber (SMF), dispersion-shifted fiber (DSF)	15.0(1)SY
XENPAK-10GB-LR+	10GBASE-LR Serial 1310-nm long-reach, single-mode fiber (SMF), dispersion-shifted fiber (DSF)	15.0(1)SY
XENPAK-10GB-LW	10GBASE-LW XENPAK Module with WAN PHY for SMF **Note** XENPAK-10GB-LW operates at an interface speed compatible with SONET/SDH OC-192/STM-64. XENPAK-10GB-LW links might go up and down if the data rate exceeds 9Gbs. (CSCsi58211)	15.0(1)SY
XENPAK-10GB-LX4	10GBASE-LX4 Serial 1310-nm multimode (MMF)	15.0(1)SY
XENPAK-10GB-SR	10GBASE-SR Serial 850-nm short-reach multimode (MMF)	15.0(1)SY
XENPAK-10GB-ZR	10GBASE for any SMF type	15.0(1)SY

Small Form-Factor Pluggable (SFP) Modules

Gigabit Ethernet SFPs

Note

- For information about coarse wavelength-division multiplexing (CWDM) SFPs, see the *Cisco CWDM GBIC and SFP Solutions* data sheet:

  http://www.cisco.com/c/en/us/products/collateral/interfaces-modules/cwdm-transceiver-modules/product_data_sheet09186a00801a557c.html

- For information about DWDM SFPs, see the *Cisco CWDM GBIC and SFP Solutions* data sheet:

  http://www.cisco.com/c/en/us/products/collateral/interfaces-modules/dwdm-transceiver-modules/product_data_sheet0900aecd80582763.html

- See the "Unsupported Hardware" section on page 67 for information about unsupported DWDM-SFPs.
- For information about other SFPs, see the *Cisco SFP Optics For Gigabit Ethernet Applications* data sheet:

  http://www.cisco.com/c/en/us/products/collateral/interfaces-modules/gigabit-ethernet-gbic-sfp-modules/product_data_sheet0900aecd8033f885.html

Product ID (append "=" for spares)	**Product Description**	**Minimum Software Version**
GLC-BX-D	1000BASE-BX10 SFP module for single-strand SMF, 1490-nm TX/1310-nm RX wavelength	15.0(1)SY
GLC-BX-U	1000BASE-BX10 SFP module for single-strand SMF, 1310-nm TX/1490-nm RX wavelength	15.0(1)SY
GLC-LH-SMD **GLC-LH-SM**	1000BASE-LX/LH SFP **Note** Supported with WS-X6904-40G-2T in Release 15.1(1)SY1 and later releases.	15.0(1)SY
GLC-SX-MMD **GLC-SX-MM**	1000BASE-SX SFP **Note** Supported with WS-X6904-40G-2T in Release 15.1(1)SY1 and later releases.	15.0(1)SY
GLC-T	1000BASE-T 10/100/1000 SFP module **Note** • Supported only at 1000 Mbps. • Supported with WS-X6904-40G-2T in Release 15.1(1)SY1 and later releases.	15.0(1)SY
GLC-ZX-SM	1000BASE-ZX SFP module	15.0(1)SY
CWDM-SFP-1470	CWDM 1470-nm (Gray) Gigabit Ethernet, 1 and 2 Gb Fibre Channel SFP module	15.0(1)SY
CWDM-SFP-1490	CWDM 1490-nm (Violet) Gigabit Ethernet, 1 and 2 Gb Fibre Channel SFP module	15.0(1)SY
CWDM-SFP-1510	CWDM 1510-nm (Blue) Gigabit Ethernet, 1 and 2 Gb Fibre Channel SFP module	15.0(1)SY
CWDM-SFP-1530	CWDM 1530-nm (Green) Gigabit Ethernet, 1 and 2 Gb Fibre Channel SFP module	15.0(1)SY
CWDM-SFP-1550	CWDM 1550-nm (Yellow) Gigabit Ethernet, 1 and 2 Gb Fibre Channel SFP module	15.0(1)SY
CWDM-SFP-1570	CWDM 1570-nm (Orange) Gigabit Ethernet, 1 and 2 Gb Fibre Channel SFP module	15.0(1)SY
CWDM-SFP-1590	CWDM 1590-nm (Red) Gigabit Ethernet, 1 and 2 Gb Fibre Channel SFP module	15.0(1)SY
CWDM-SFP-1610	CWDM 1610-nm (Brown) Gigabit Ethernet, 1 and 2 Gb Fibre Channel SFP module	15.0(1)SY
DWDM-SFP-5817	1000BASE-DWDM 1558.17 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-5252	1000BASE-DWDM 1552.52 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-5172	1000BASE-DWDM 1551.72 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-5012	1000BASE-DWDM 1550.12 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-4692	1000BASE-DWDM 1546.92 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-4373	1000BASE-DWDM 1543.73 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-4214	1000BASE-DWDM 1542.14 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-3977	1000BASE-DWDM 1539.77 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY

Product ID (append "=" for spares)	Product Description	Minimum Software Version
DWDM-SFP-3898	1000BASE-DWDM 1538.98 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-3582	1000BASE-DWDM 1535.82 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-3504	1000BASE-DWDM 1535.04 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-6061	1000BASE-DWDM 1560.61 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-5979	1000BASE-DWDM 1559.79 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-5898	1000BASE-DWDM 1558.98 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-5655	1000BASE-DWDM 1556.55 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-5575	1000BASE-DWDM 1555.75 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-5494	1000BASE-DWDM 1554.94 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-5413	1000BASE-DWDM 1554.13 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-5092	1000BASE-DWDM 1550.92 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-4851	1000BASE-DWDM 1548.51 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-4772	1000BASE-DWDM 1547.72 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-4612	1000BASE-DWDM 1546.12 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-4453	1000BASE-DWDM 1544.53 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-4294	1000BASE-DWDM 1542.94 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-4056	1000BASE-DWDM 1540.56 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-3819	1000BASE-DWDM 1538.19 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-3661	1000BASE-DWDM 1536.61 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-3425	1000BASE-DWDM 1534.25 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-3268	1000BASE-DWDM 1532.68 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-3190	1000BASE-DWDM 1531.90 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-3112	1000BASE-DWDM 1531.12 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-3033	1000BASE-DWDM 1530.33 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY

Fast Ethernet SFPs

Note

- The CAT6000-VS-S720-10G/MSFC3 and WS-X6148-FE-SFP supports Fast Ethernet SFPs.
- For information about Fast Ethernet SFPs, see the *Cisco 100BASE-X SFP For Fast Ethernet SFP Ports* data sheet:

  http://www.cisco.com/c/en/us/products/collateral/interfaces-modules/fast-ethernet-sfp-modules/product_data_sheet0900aecd801f931c.html
- GLC-GE-100FX Fast Ethernet SFPs are not supported.

Product ID (append "=" for spares)	Product Description	Minimum Software Version
GLC-FE-100BX-U	100BASE-BX10-U SFP	15.0(1)SY
GLC-FE-100BX-D	100BASE-BX10-D SFP	
GLC-FE-100EX	100BASEEX SFP	
GLC-FE-100ZX	100BASEZX SFP	
GLC-FE-100FX	100BASEFX SFP	
GLC-FE-100LX	100BASELX SFP	

Gigabit Interface Converters (GBICs)

Note The support listed in this section applies to all modules that use GBICs.

Product ID (append "=" for spares)	Product Description	Minimum Software Versions
WDM-GBIC-REC	Receive-only wavelength division multiplexing (WDM) GBIC	15.0(1)SY
DWDM-GBIC	Dense wavelength division multiplexing (DWDM) GBIC	15.0(1)SY
CWDM-GBIC-1470	Cisco 1000BASE-CWDM GBIC, 1470 nm (Gray)	15.0(1)SY
CWDM-GBIC-1490	Cisco 1000BASE-CWDM GBIC, 1490 nm (Violet)	15.0(1)SY
CWDM-GBIC-1510	Cisco 1000BASE-CWDM GBIC, 1510 nm (Blue)	15.0(1)SY
CWDM-GBIC-1530	Cisco 1000BASE-CWDM GBIC, 1530 nm (Green)	15.0(1)SY
CWDM-GBIC-1550	Cisco 1000BASE-CWDM GBIC, 1550 nm (Yellow)	15.0(1)SY
CWDM-GBIC-1570	Cisco 1000BASE-CWDM GBIC, 1570 nm (Orange)	15.0(1)SY
CWDM-GBIC-1590	Cisco 1000BASE-CWDM GBIC, 1590 nm (Red)	15.0(1)SY
CWDM-GBIC-1610	Cisco 1000BASE-CWDM GBIC, 1610 nm (Brown)	15.0(1)SY
WS-G5483	1000BASET GBIC	15.0(1)SY
WS-G5484	Short wavelength, 1000BASE-SX	15.0(1)SY
WS-G5486	Long wavelength/long haul, 1000BASE-LX/LH	15.0(1)SY
WS-G5487	Extended distance, 1000BASE-ZX	15.0(1)SY

Service Modules

Note

- For service modules that run their own software, see the service module software release notes for information about the minimum required service module software version.
- With SPAN configured to include a port-channel interface to support a service module, be aware of CSCth03423 and CSCsx46323.
- EtherChannel configuration can impact some service modules. In particular, distributed EtherChannels (DECs) can interfere with service module traffic. See this field notice for more information:

  http://www.cisco.com/c/en/us/support/docs/field-notices/610/fn61935.html

Application Control Engine (ACE) Module

Product ID (append "=" for spares)	**Product Description**	**Minimum Software Versions**
ACE30-MOD-K9	Application Control Engine (ACE) module	
	With Supervisor Engine 2T-10GE	15.0(1)SY
	With Supervisor Engine 720-10GE	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

- ACE modules run their own software—See these publications:

  http://www.cisco.com/c/en/us/support/interfaces-modules/ace-application-control-engine-module/tsd-products-support-model-home.html

  See the ACE module software release notes for information about the minimum required service module software version.

ASA Services Module

Product ID (append "=" for spares)	Product Description	Minimum Software Versions
WS-SVC-ASA-SM1-K7	ASA Services Module	
	With Supervisor Engine 2T-10GE	15.1(1)SY3
	With Supervisor Engine 720-10GE	
	With Supervisor Engine 720	
WS-SVC-ASA-SM1-K9	ASA Services Module	
	With Supervisor Engine 2T-10GE	15.0(1)SY1
	With Supervisor Engine 720-10GE	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

- Upgrade to the minimum software version or later before installing an ASA services module (see the "EFSU Compatibility" section on page 68).
- ASA modules run their own software—See these publications:

  http://www.cisco.com/c/en/us/support/interfaces-modules/catalyst-6500-series-7600-series-asa-services-module/tsd-products-support-model-home.html

  See the module software release notes for information about the minimum required service module software version.

Firewall Services Module (FWSM)

Product ID (append "=" for spares)	Product Description	Minimum Software Version
WS-SVC-FWM-1-K9	Firewall Services Module	
	With Supervisor Engine 2T-10GE	15.0(1)SY
	With Supervisor Engine 720-10GE	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

- With Firewall Services Module Software Release 2.3(1) and later releases, WS-SVC-FWM-1-K9 maintains state when an NSF with SSO redundancy mode switchover occurs.
- WS-SVC-FWM-1-K9 runs its own software—See these publications:

  http://www.cisco.com/c/en/us/support/interfaces-modules/catalyst-6500-series-firewall-services-module/tsd-products-support-model-home.html

  See the WS-SVC-FWM-1-K9 software release notes for information about the minimum required WS-SVC-FWM-1-K9 software version.

Intrusion Detection System Modules (IDSMs)

Product ID (append "=" for spares)	Product Description	Minimum Software Versions
WS-SVC-IDSM2-K9	Intrusion Detection System Module 2; CEF256 **Note** Not supported with Supervisor Engine 2T.	
	With Supervisor Engine 720-10GE (not supported in VSS mode)	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

- The IDSM runs its own software—See these publications:

  http://www.cisco.com/c/en/us/support/interfaces-modules/catalyst-6500-series-intrusion-detection-system-idsm-2-services-module/tsd-products-support-model-home.html

  See the IDSM software release notes for information about the minimum required IDSM software version.

Network Analysis Modules (NAMs)

Product ID (append "=" for spares)	Product Description	Minimum Software Version
WS-SVC-NAM3-6G-K9 **WS-SVC-NAM-2** **WS-SVC-NAM-1**	Network Analysis Module 3 Network Analysis Module 2 Network Analysis Module 1	
	With Supervisor Engine 2T-10GE	15.0(1)SY1
	With Supervisor Engine 720-10GE	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

- Upgrade to Release 15.0(1)SY1 or later before installing WS-SVC-NAM3-6G-K9 (see the "EFSU Compatibility" section on page 68).
- NAM modules run their own software—See these publications for more information:
  - http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-network-analysis-module-software/products-release-notes-list.html
  - http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-network-analysis-module-software/tsd-products-support-series-home.html

  See the software release notes for information about the minimum required NAM software version.

Wireless Services Modules (WiSMs)

Product ID (append "=" for spares)	Product Description	Minimum Software Versions
WS-SVC-WISM2-1-K9 **WS-SVC-WISM2-3-K9** **WS-SVC-WISM2-5-K9**	Wireless Services Module 2 (WiSM2)	
	With Supervisor Engine 2T-10GE	15.0(1)SY
	With Supervisor Engine 720-10GE	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY
WS-SVC-WISM-1-K9	Wireless Services Module (WiSM)	
	With Supervisor Engine 2T-10GE	15.0(1)SY
	With Supervisor Engine 720-10GE	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY
Wireless services modules run their own software—See these publications: http://www.cisco.com/c/en/us/support/interfaces-modules/services-modules/products-release-notes-list.html See the wireless services modules software release notes for information about the minimum required wireless services module software version.		

Power Supplies

WS-C6503-E Power Supplies

Product ID (append "=" for spares)	Product Description	Minimum Software Version
PWR-1400-AC	1,400 W AC power supply	15.0(1)SY
PWR-950-AC	950 W AC power supply	15.0(1)SY
PWR-950-DC	950 W DC power supply	15.0(1)SY

WS-C6504-E Power Supplies

Product ID (append "=" for spares)	Product Description	Minimum Software Version
PWR-2700-AC/4	2700 W AC power supply	15.0(1)SY
PWR-2700-DC/4	2700 W DC power supply	15.0(1)SY

All Other Power Supplies

Note The power supplies in this section are not supported in these chassis:

- Catalyst 6503-E
- Catalyst 6504-E

Product ID (append "=" for spares)	Product Description	Minimum Software Version
WS-CAC-8700W-E	8,700 W AC power supply	15.0(1)SY
	Note • WS-CAC-8700W-E supports a remote power cycling feature. • See this publication for more information: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/hardware/Chassis_Installation/Cat6500/6500_ins.html	
PWR-6000-DC	6,000 W DC power supply	15.0(1)SY
WS-CAC-6000W	6,000 W AC power supply	
PWR-4000-DC	4,000 W DC power supply	
WS-CAC-4000W	4,000 W AC power supply	
+WS-CAC-3000W	3,000 W AC power supply	
WS-CAC-3000W	3,000 W AC power supply	
WS-CAC-2500W	2,500 W AC power supply	
WS-CDC-2500W	2,500 W DC power supply	

Chassis

- 13-Slot Chassis, page 63
- 9-Slot Chassis, page 64
- 6-Slot Chassis, page 66

- 4-Slot Chassis, page 66
- 3-Slot Chassis, page 67

Note Chassis with 64 MAC addresses automatically enable the Extended System ID feature, which is enabled with the spanning-tree extend system-id command. You cannot disable the extended-system ID in chassis that support 64 MAC addresses. The Extended System ID feature might already be enabled in your network, because it is required to support both extended-range VLANs and any chassis with 64 MAC addresses. **Enabling the extended system ID feature for the first time updates the bridge IDs of all active STP instances, which might change the spanning tree topology.**

13-Slot Chassis

Note With Supervisor Engine 2T-10GE, the slot reserved for a redundant supervisor engine can be populated with one of these modules:

- WS-X6148E-GE-45AT
- WS-X6148A-GE-TX, WS-X6148A-GE-45AF
- WS-X6148-FE-SFP
- WS-X6148A-RJ-45, WS-X6148A-45AF
- WS-X6196-RJ-21, WS-X6196-21AF

Product ID (append "=" for spare)	**Product Description**	**Minimum Software Version**
WS-C6513-E	• 13 slots • Slot 7 and slot 8 are reserved for supervisor engines • 64 chassis MAC addresses	
	With Supervisor Engine 2T-10GE	15.0(1)SY
	With Supervisor Engine 720-10GE	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY
CISCO7613-S	• 13 slots • Slot 7 and slot 8 are reserved for supervisor engines • 64 chassis MAC addresses	
	With Supervisor Engine 2T-10GE	15.1(1)SY

Product ID (append "=" for spare)	Product Description	Minimum Software Version
WS-C6513	Catalyst 6513 chassis: • 13 slots • 64 chassis MAC addresses • Use with Supervisor Engine 720-10GE or Supervisor Engine 720 requires WS-C6K-13SLT-FAN2 • These modules are supported only in slots 9 through 13 and do not power up in other slots: – WS-X6700 series switching modules except WS-X6724-SFP – WS-X6816-GBIC switching modules – WS-SVC-WISM-1-K9 **Note** Not supported with Supervisor Engine 2T.	
	With Supervisor Engine 720-10GE	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

9-Slot Chassis

Product ID (append "=" for spare)	Product Description	Minimum Software Version
WS-C6509-V-E	• 9 vertical slots • 64 chassis MAC addresses • Required power supply: – 2,500 W DC or higher – 3,000 W AC or higher	
	With Supervisor Engine 2T-10GE	15.0(1)SY
	With Supervisor Engine 720-10GE	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

Product ID (append "=" for spare)	Product Description	Minimum Software Version
WS-C6509-E	• 9 horizontal slots • Chassis MAC addresses: – Before April 2009—1024 chassis MAC addresses – Starting in April 2009—64 chassis MAC addresses **Note** Chassis with 64 MAC addresses automatically enable the Extended System ID feature, which is enabled with the spanning-tree extend system-id command. You cannot disable the extended-system ID in chassis that support 64 MAC addresses. The Extended System ID feature might already be enabled in your network, because it is required to support both extended-range VLANs and any chassis with 64 MAC addresses. **Enabling the extended system ID feature for the first time updates the bridge IDs of all active STP instances, which might change the spanning tree topology.** • Requires 2,500 W or higher power supply	
	With Supervisor Engine 2T-10GE	15.0(1)SY
	With Supervisor Engine 720-10GE	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY
CISCO7609-S	• 9 vertical slots • 64 chassis MAC addresses • Required power supply: – 2,500 W DC or higher – 3,000 W AC or higher	
	With Supervisor Engine 2T-10GE	15.0(1)SY1

6-Slot Chassis

Product ID (append "=" for spare)	Product Description	Minimum Software Version
WS-C6506-E	• 6 slots • Chassis MAC addresses: – Before April 2009—1024 chassis MAC addresses – Starting in April 2009—64 chassis MAC addresses **Note** Chassis with 64 MAC addresses automatically enable the Extended System ID feature, which is enabled with the spanning-tree extend system-id command. You cannot disable the extended-system ID in chassis that support 64 MAC addresses. The Extended System ID feature might already be enabled in your network, because it is required to support both extended-range VLANs and any chassis with 64 MAC addresses. **Enabling the extended system ID feature for the first time updates the bridge IDs of all active STP instances, which might change the spanning tree topology.** • Requires 2,500 W or higher power supply	
	With Supervisor Engine 2T-10GE	15.0(1)SY
	With Supervisor Engine 720-10GE	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY
CISCO7606-S	• 6 slots • 64 chassis MAC addresses	
	With Supervisor Engine 2T-10GE	15.1(1)SY1

4-Slot Chassis

Product ID (append "=" for spare)	Product Description	Minimum Software Version
WS-C6504-E	• 4 slots • 64 chassis MAC addresses	
	With Supervisor Engine 2T-10GE	15.0(1)SY
	With Supervisor Engine 720-10GE	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY
CISCO7604	• 4 slots • 64 chassis MAC addresses	
	With Supervisor Engine 2T-10GE	15.1(1)SY

3-Slot Chassis

Product ID (append "=" for spare)	Product Description	Minimum Software Version
WS-C6503-E	• 3 slots • 64 chassis MAC addresses • WS-X6904-40G-2T and WS-X6908-10GE are supported only with WS-C6503-E hardware revision 1.3 or higher.	
	With Supervisor Engine 2T-10GE	15.0(1)SY
	With Supervisor Engine 720-10GE	15.1(1)SY
	With Supervisor Engine 720	15.1(1)SY

Unsupported Hardware

Release 15.1SY supports only the hardware listed in the "Supported Hardware" section on page 6. Unsupported modules remain powered down if detected and do not affect system behavior.

Release 12.2SX supported these modules, which are not supported in Release 15.1SY:

- Supervisor Engine 32 (CAT6000-SUP32/MSFC2A)
- ME 6500 Series Ethernet Switches (ME6524)
- Policy Feature Card 3A and Distributed Forwarding Card 3A
- 76-ES+XT-4TG3CXL, 76-ES+XT-4TG3C
- 76-ES+XT-2TG3CXL, 76-ES+XT-2TG3C
- 7600-ES+4TG3CXL, 7600-ES+4TG3C
- 7600-ES+2TG3CXL, 7600-ES+2TG3C
- Shared Port Adapter (SPA) Interface Processors (SIPs) and Shared Port Adapters (SPAs)
- Services SPA Carrier (SSC) and Services SPAs
- Enhanced FlexWAN Module
- Anomaly Guard Module(AGM)
- Traffic Anomaly Detector Module (ADM)
- Communication Media Module (CMM)
- Content Switching Module (CSM)
- Content Switching Module with SSL (CSM-S)
- Secure Sockets Layer (SSL) Services Module

Images and Feature Sets

Use Cisco Feature Navigator to display information about the images and feature sets in Release 15.1SY.

The releases includes strong encryption images. Strong encryption images are subject to U.S. and local country export, import, and use laws. The country and class of end users eligible to receive and use Cisco encryption solutions are limited. See this publication for more information:

http://www.cisco.com/web/about/doing_business/legal/global_export_trade/general_export/contract_compliance.html

Universal Boot Loader Image

The Universal Boot Loader (UBL) image is a minimal network-aware image that can download and install a Cisco IOS image from a running active supervisor engine in the same chassis. When newly installed as a standby supervisor engine in a redundant configuration, a supervisor engine running the UBL image automatically attempts to copy the image of the running active supervisor engine in the same chassis.

EFSU Compatibility

SX SY EFSU Compatibility Matrix (XLSX - Opens with Microsoft Excel)

Cisco IOS Behavior Changes

Behavior changes describe the minor modifications that are sometimes introduced in a software release. When behavior changes are introduced, existing documentation is updated.

Release 15.1(2)SY16

- CSCvi48253: Self-signed certificates expire on 00:00 1 Jan 2020 UTC, can't be created after that time
- CSCvq66030: Cisco IOS and Cisco IOS XE Software Web UI Cross-Site Request Forgery Vulnerability

Release 15.1(2)SY8

- CSCuh97087 (Transport Input)
  In previous Cisco IOS release versions , the default was the " transport input all" command and device allows all transport protocols and accepts the incoming network connections to tty lines by default. But Based on the CSDL's product Security Baseline Requirement (SEC-MGT-DEFT-2) transport input has been changed to NONE from ALL through CSCuh97087 and documented.

  Now we must configure an incoming transport {protocol | all } command before the line will accept incoming connections, Otherwise default is NONE and cisco devices cannot accept the connections to tty lines .

Old behavior: transport input all
New behavior (After fix): transport input none
It has already documented and the command is available in this location.
http://www.cisco.com/c/en/us/td/docs/ios/termserv/command/reference/tsv_book/tsv_s1.html#pgfId-1069219

- CSCuu55288 (Mechanism to throttle NDE export)
  Default behavior will be same.
  Command *flow hardware export priority low* reduces the process priority from Critical to medium and because of this command flow export time may vary based on the CPU usage in the system.
- CSCva39982 (IPv6 neighbor discovery packet processing behavior)
  Before fix: To rate limit the ipv6 icmp nd type 13-137 packets, there is classmap in the default policy-map, which gets programmed on control plane

  sh policy-map policy-default-autocopp | b ndv6
  Class class-copp-match-ndv6
  police rate 1000 pps, burst 1000 packets
  conform-action set-discard-class-transmit 48
  exceed-action drop

  so for both valid ipv6 icmp nd type 13-137 packets (i.e with hop-limit 255) and invalid packets (with hop-limit < 255), there is single policy . So this allows attacker to send a crafted IPv6 ND packet that will cause dropping of valid CPU-bound ipv6 icmp nd traffic.
  Fix: Added a class-map above "class-copp-match-ndv6" named as *class-copp-match-ndv6hl* as follows
  FM-NAT#sh policy-map policy-default-autocopp | b ndv6

  Class class-copp-match-ndv6hl

  police rate 10 pps, burst 1 packets

  conform-action drop

  exceed-action drop

  Class class-copp-match-ndv6

  police rate 1000 pps, burst 1000 packets

  conform-action set-discard-class-transmit 48

  exceed-action drop

so that all ipv6 icmp nd type 133-137 packets having invalid hop-limit (!=255) will be dropped in hardware.
For this class-map to be effective , following points has to be considered:

- This new class-map doesn't get applied on reload only, as auto-copp gets saved in the start-up config, and on reload the saved policy reappears.
- to apply the policy-map with new class-map, user has to remove the default control plane policy using *no policy-map policy-default-autocopp*, the new class-map for policy-default-autocopp appears upon reload.
- In config-mode a cli is available *no platform qos auto-copp*, which when applied , removes the policy-map policy-default-autocopp
- and when *platform qos auto-copp* applied, regenerates the policy-map *policy-default-autocopp* along with new class-map "class-copp-match-ndv6hl" and add service-policy to control-plane.

- CSCub46031 (knob to turn off auto-copp)
  This enhancement deals with following CLI creation : *no platform qos auto-copp* .
  Initial Issue: If the user wishes to remove the default control plane policy using *no policy-map policy-default-autocopp*, the same config for policy-default-autocopp reappears upon reload.
  Fix/Enhancement: New CLI has been introduced in config mode : *no platform qos auto-copp*.
  Suppose the user issuesthis command prior to or after issuing *no policy-map policy-default-autocopp*, the config for policy-map policy-default-autocopp doesnt reappear after reload and thereby fixing the issue.
  Also, if the user wants to reconfigure the policy-default-autocopp configs, they can issue *platform qos auto-copp* command which will immediately regenerate the config and add the service-policy to control plane if there was no policy there in the first place. In the case there was another policy on the control plane, while the policy map will be regenerated it wont be attached to control-plane.
- CSCva69133: cli changes needed for fix in CSCva39982

Release 15.1(2)SY7

- Deprecated CLI command

  Old behavior: Running the CLI command "*show platform fex-debug status*" is no longer supported.

  New behavior: Use the new CLI command "*show fex <fex-id>*" instead.

  Additional Information: http://tools.cisco.com/bugsearch/bug/CSCux45230

Release 15.1(1)SY2

- New **radius-server** commands

  Old behavior: The RADIUS server does not have Point-to-Point Tunneling Protocol (PPTP) tunnel-specific information because the tunnel-client endpoint and tunnel-server endpoint attributes are missing in the access-request packets sent to the RADIUS server.

  New behavior: The following commands are introduced to identify the hostname or address of the network access server (NAS) at the initiator and server end of the Point-to-Point Tunneling Protocol (PPTP) tunnel by sending the Tunnel-Client-Endpoint attribute and the Tunnel-Server-Endpoint attribute in access-request packets to the RADIUS server.

  – **radius-server attribute 66 include-in-access-req**

  – **radius-server attribute 67 include-in-access-req**

  Additional Information:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/m1/sec-m1-cr-book/sec-cr-r1.html

New Features in Release 15.1(2)SY16

These sections describe the new features in Release 15.1(2)SY16, 20February 2020:

- New Hardware Features in Release 15.1(2)SY16, page 71
- New Software Features in Release 15.1(2)SY16, page 71

New Hardware Features in Release 15.1(2)SY16

None.

New Software Features in Release 15.1(2)SY16

None.

New Features in Release 15.1(2)SY15

These sections describe the new features in Release 15.1(2)SY15, 20 August 2019:

- New Hardware Features in Release 15.1(2)SY15, page 71
- New Software Features in Release 15.1(2)SY15, page 71

New Hardware Features in Release 15.1(2)SY15

None.

New Software Features in Release 15.1(2)SY15

None.

New Features in Release 15.1(2)SY14

These sections describe the new features in Release 15.1(2)SY14, 14 February 2019:

- New Hardware Features in Release 15.1(2)SY14, page 71
- New Software Features in Release 15.1(2)SY14, page 71

New Hardware Features in Release 15.1(2)SY14

None.

New Software Features in Release 15.1(2)SY14

None.

New Features in Release 15.1(2)SY13

These sections describe the new features in Release 15.1(2)SY13, 6 September 2018:

- New Hardware Features in Release 15.1(2)SY13, page 72
- New Software Features in Release 15.1(2)SY13, page 72

New Hardware Features in Release 15.1(2)SY13

None.

New Software Features in Release 15.1(2)SY13

None.

New Features in Release 15.1(2)SY12

These sections describe the new features in Release 15.1(2)SY12, 30April 2018:

- New Hardware Features in Release 15.1(2)SY12, page 72
- New Software Features in Release 15.1(2)SY12, page 72

New Hardware Features in Release 15.1(2)SY12

None.

New Software Features in Release 15.1(2)SY12

None.

New Features in Release 15.1(2)SY11

These sections describe the new features in Release 15.1(2)SY11, 27 July 2017:

- New Hardware Features in Release 15.1(2)SY11, page 72
- New Software Features in Release 15.1(2)SY11, page 72

New Hardware Features in Release 15.1(2)SY11

None.

New Software Features in Release 15.1(2)SY11

None.

New Features in Release 15.1(2)SY10

These sections describe the new features in Release 15.1(2)SY10, 24 Feb 2017:

- New Hardware Features in Release 15.1(2)SY10, page 73
- New Software Features in Release 15.1(2)SY10, page 73

New Hardware Features in Release 15.1(2)SY10

None.

New Software Features in Release 15.1(2)SY10

None.

New Features in Release 15.1(2)SY9

These sections describe the new features in Release 15.1(2)SY9, 14 Oct 2016:

- New Hardware Features in Release 15.1(2)SY9, page 73
- New Software Features in Release 15.1(2)SY9, page 73

New Hardware Features in Release 15.1(2)SY9

None.

New Software Features in Release 15.1(2)SY9

None.

New Features in Release 15.1(2)SY8

These sections describe the new features in Release 15.1(2)SY8, 01 Sept 2016:

- New Hardware Features in Release 15.1(2)SY8, page 73
- New Software Features in Release 15.1(2)SY8, page 73

New Hardware Features in Release 15.1(2)SY8

None.

New Software Features in Release 15.1(2)SY8

None.

New Features in Release 15.1(2)SY7

These sections describe the new features in Release 15.1(2)SY7, 16 Mar 2016:

- New Hardware Features in Release 15.1(2)SY7, page 74
- New Software Features in Release 15.1(2)SY7, page 74

New Hardware Features in Release 15.1(2)SY7

None.

New Software Features in Release 15.1(2)SY7

None.

New Features in Release 15.1(1)SY6

These sections describe the new features in Release 15.1(1)SY6, 12 Nov 2015:

- New Hardware Features in Release 15.1(1)SY6, page 74
- New Software Features in Release 15.1(1)SY6, page 74

New Hardware Features in Release 15.1(1)SY6

None.

New Software Features in Release 15.1(1)SY6

None.

New Features in Release 15.1(2)SY6

These sections describe the new features in Release 15.1(2)SY6, 19 Sept 2015:

- New Hardware Features in Release 15.1(2)SY6, page 74
- New Software Features in Release 15.1(2)SY6, page 74

New Hardware Features in Release 15.1(2)SY6

None.

New Software Features in Release 15.1(2)SY6

None.

New Features in Release 15.1(2)SY5

These sections describe the new features in Release 15.1(2)SY5, 21 May 2015:

- New Hardware Features in Release 15.1(2)SY5, page 75
- New Software Features in Release 15.1(2)SY5, page 75

New Hardware Features in Release 15.1(2)SY5

None.

New Software Features in Release 15.1(2)SY5

- Manage FEX switch-ID allocation from Controller after stack is booted up.
- QoS Certification
- OID for Peer Interface of VSL link in CISCO-VIRTUAL-SWITCH-MIB
- Trifecta-ASA NPE

New Features in Release 15.1(1)SY5

These sections describe the new features in Release 15.1(1)SY5, 27 Mar 2015:

- New Hardware Features in Release 15.1(1)SY5, page 75
- New Software Features in Release 15.1(1)SY5, page 75

New Hardware Features in Release 15.1(1)SY5

None.

New Software Features in Release 15.1(1)SY5

None.

New Features in Release 15.1(2)SY4

These sections describe the new features in Release 15.1(2)SY4, 08 Nov 2014:

- New Hardware Features in Release 15.1(2)SY4, page 75
- New Software Features in Release 15.1(2)SY4, page 75

New Hardware Features in Release 15.1(2)SY4

None.

New Software Features in Release 15.1(2)SY4

None.

New Features in Release 15.1(1)SY4

These sections describe the new features in Release 15.1(1)SY4, 10 Oct 2014:

New Hardware Features in Release 15.1(1)SY4

None.

New Software Features in Release 15.1(1)SY4

None.

New Features in Release 15.1(2)SY3

These sections describe the new features in Release 15.1(2)SY3, 23 Jun 2014:

New Hardware Features in Release 15.1(2)SY3

- Catalyst C6800IA-48FPDR Instant Access client with dual power supplies.
- WS-SVC-ASA-SM1-K7 ASA Services Module.
- SFP-10G-ZR support on WS-X6904-40G-2T—See this publication:

  http://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/data_sheet_c78-455693.html

New Software Features in Release 15.1(2)SY3

None.

New Features in Release 15.1(2)SY2

These sections describe the new features in Release 15.1(2)SY, 03 Mar 2014:

New Hardware Features in Release 15.1(2)SY2

- C6880-X-LE-16P10G port card support on the Cisco Catalyst 6880-X switch—See the "Cisco Catalyst 6880-X Series Extensible Fixed Aggregation Switches" section on page 30

- C6880-X-16P10G port card support on Cisco Catalyst 6880-X switch—See "Cisco Catalyst 6880-X Series Extensible Fixed Aggregation Switches" section on page 30

New Software Features in Release 15.1(2)SY2

- Instant Access on Cisco Catalyst 6880-X switch—See this publication:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-1SY/config_guide/sup2T/15_1_sy_swcg_2T/instant_access.html

Caution On Cisco Catalyst 6880-X switch, in performance mode, the disabled ports in 15.1(2)SY1 are ports 3-4, 7-8, 11-12 and 15-16, while the disabled ports in 15.1(2)SY2 are ports 5-8 and 13-16. Before you upgrade to 15.1(2)SY2, reconfigure to the available open ports (1-4 and 9-12) to prevent an outage.

- VSS Quad-Sup SSO (VS4O)—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/15.1SY/config_guide/sup2T/virtual_switching_systems.html#VSS_Quad-Sup_SSO_(VS4O)
- Etherchannel on IA clients.
- Instant Access on VSS Quad-Sup.
- 1G IA parent-client connectivity.

New Features in Release 15.1(2)SY1

These sections describe the new features in Release 15.1(2)SY1, 09 Dec 2013:

- New Hardware Features in Release 15.1(2)SY1, page 77
- New Software Features in Release 15.1(2)SY1, page 77

New Hardware Features in Release 15.1(2)SY1

- Cisco Catalyst 6880-X Series Extensible Fixed Aggregation Switches, page 30
- Cisco Catalyst 6807-XL Modular Switch, page 31

New Software Features in Release 15.1(2)SY1

None.

New Features in Release 15.1(2)SY

These sections describe the new features in Release 15.1(2)SY, 07 Sep 2013:

- New Hardware Features in Release 15.1(2)SY, page 78
- New Software Features in Release 15.1(2)SY, page 78

New Hardware Features in Release 15.1(2)SY

- Instant Access Catalyst 6800ia Series Switches—See this publication:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-1SY/config_guide/sup2T/15_1_sy_swcg_2T/instant_access.html
- DWDM SFP10G Support on WS-X6904-40G-2T—See this publication:

  http://www.cisco.com/c/en/us/products/collateral/interfaces-modules/dwdm-transceiver-modules/data_sheet_c78-711186.html

New Software Features in Release 15.1(2)SY

- BGP Support for IP Prefix Export from a VRF Table into the Global Table—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/configuration/15-mt/irg-15-mt-book/irg-prefix-export.html
- EIGRP IPv6 Graceful Restart (GR)—The EIGRP IPv6 Graceful Restart (GR) feature is enabled by default in EIGRP IPv6 configurations. GR is a way to rebuild forwarding information in routing protocols and resets router's control plane without impacting (global) routing.
- Granular enablement of CTS SGACL at interface level—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cts/configuration/15-sy/sec-cts-15-sy-book/cts_sgacl_int.html
- Instant Access—See this publication:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-1SY/config_guide/sup2T/15_1_sy_swcg_2T/instant_access.html
- IPv6 Multicast VRF Lite—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipmulti_pim/configuration/15-sy/imc-pim-15-sy-book/imc_basic_ipv6.html
- ISIS Features in IP services—The IP services image supports ISIS features.
- ISIS MTR for multicast address family only—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mtr/configuration/15-sy/mtr-15-sy-book/isis-mtr-multicast-address-family.html
- ISSU support for FEX—See this publication:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-1SY/config_guide/sup2T/15_1_sy_swcg_2T/instant_access.html
- Medianet Metadata—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mdata/configuration/15-sy/mdata-15sy-book/metadata-framework.html
- MediaTrace 1.0—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios/media_monitoring/configuration/guide/15_1m_and_t/mm_15_1m_and_t/mm_mediatrace.html
- MoFRR—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipmulti_serv/configuration/15-sy/imc-serv-15-sy-book/Multicast_only_Fast_Re-Route.html
- MVPNv6—See this publication:

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

- OSPF Support for Multi-VRF on CE Routers—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/15-sy/iro-15-sy-book/iro-sup-vrf.html

- OSPFv3 MIB—See this publication:

  http://www.cisco.com/c/en/us/td/docs/wireless/asr_901/mib/reference/asr_mib.html

- OSPFv3 NSR—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/15-sy/iro-15-sy-book/iro-ospfv3-nsr.html

- Performance Monitor (Phase 1)—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/media_monitoring/configuration/15-sy/mm-15-sy-book/mm-pasv-mon.html

- Service Discovery Gateway—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dns/configuration/15-sy/dns-15-sy-book/dns-15-sy-book_chapter_0100.html

New Features in Release 15.1(1)SY3

These sections describe the new features in Release 15.1(1)SY3, 21 Mar 2014:

- New Hardware Features in Release 15.1(1)SY3, page 79
- New Software Features in Release 15.1(1)SY3, page 79

New Hardware Features in Release 15.1(1)SY3

None.

New Software Features in Release 15.1(1)SY3

None.

New Features in Release 15.1(1)SY2

These sections describe the new features in Release 15.1(1)SY2, 04 Oct 2013:

- New Hardware Features in Release 15.1(1)SY2, page 79
- New Software Features in Release 15.1(1)SY2, page 80

New Hardware Features in Release 15.1(1)SY2

None.

New Software Features in Release 15.1(1)SY2

None.

New Features in Release 15.1(1)SY1

These sections describe the new features in Release 15.1(1)SY1, 03 May 2013:

New Hardware Features in Release 15.1(1)SY1

- WS-X6904-40G-2T switching module support for:
  - GLC-LH-SMD 1G SFP
  - GLC-SX-MMD 1G SFP
  - GLC-T 1G SFP
- Supervisor Engine 2T support with the 7606-S chassis

New Software Features in Release 15.1(1)SY1

- DHCPv6 - Relay chaining for Prefix Delegation—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dhcp/configuration/15-sy/dhcp-15-sy-book/ip6-dhcp-rel-agent.html
- Egress Microflow Destination-Only Policing—See this publication:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-1SY/config_guide/sup2T/15_1_sy_swcg_2T/qos_class_mark_police.html
- Global QoS Policy—See this publication:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-1SY/config_guide/sup2T/15_1_sy_swcg_2T/denial_of_service.html

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-1SY/config_guide/sup720/15_1_sy_swcg_720/denial_of_service.html
- HSRP aware PIM—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipmulti_pim/configuration/15-sy/imc-pim-15-sy-book/imc_hsrp_aware.html
- Interfaces MIB: SNMP context based access—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/15-sy/snmp-15-sy-book/nm-snmp-vpn-context.html
- LISP Locator/ID Separation Protocol—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_lisp/configuration/15-sy/irl-15-sy-book.html
- LISP Virtualization—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_lisp/configuration/15-sy/irl-15-sy-book.html

- Medianet 2.2 features in Cat6500 Ipbase images—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/media_monitoring/configuration/15-sy/mm-15-sy-book.html

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/media_monitoring/configuration/15-sy/mm-15-sy-book/mm-mediatrace.html
- MPLS TE - Bundled Interface Support (EtherChannel and MLP)—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_te_path_setup/configuration/15-sy/mp-te-path-setup-15-sy-book/mp-te-path-setup-15-sy-book_chapter_01100.html
- Multicast Feature Reformation Packaging Changes—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/15.1SY/release_notes.html#New_Software_Features_in_Release_15.1(1)SY1
- SGT Name export in NetFlow—See this publication:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/trustsec/configuration/guide/trustsec/appc_cat6k.html
- TrustSec Diagnostic Tool Kits - Packet Trace—See this publication:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/trustsec/configuration/guide/trustsec/command_sum.html
- TrustSec SGA Conditional Debugging Capabilities—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp/configuration/15-sy/iap-15-sy-book.html
- TrustSec SGA SYSLOG Messages—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios/15_0sy/system/messages/15sysmg.html
- VPLS PIM and IGMP Snooping (LAN Interfaces)—See this publication:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-1SY/config_guide/sup2T/15_1_sy_swcg_2T/vpls.html
- VSS Quad-Sup SSO (VS4O)—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/15.1SY/config_guide/sup2T/virtual_switching_systems.html#VSS_Quad-Sup_SSO_(VS4O)
- VSS Quad-Sup Uplink Forwarding with HA domains—See this publication:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-1SY/config_guide/sup720/15_1_sy_swcg_720/virtual_switching_systems.html
- WCCPv2 - IPv6 Support—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp/configuration/15-sy/iap-15-sy-book/iap-wccp.html

New Features in Release 15.1(1)SY

These sections describe the new features in Release 15.1(1)SY, 15 Oct 2012:

- New Hardware Features in Release 15.1(1)SY, page 82
- New Software Features in Release 15.1(1)SY, page 82

New Hardware Features in Release 15.1(1)SY

- 7604S chassis support with the Supervisor Engine 2T—See this publication:
- 7613-S chassis support with the Supervisor Engine 2T—See this publication:
- SFP+ LRM transceiver support—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/15.1SY/release_notes.html#10_GE_SFP+_Modules
- X2-10GB-T transceiver support—See this publication:
- With Supervisor Engine 2T, VSS mode support for the WS-X6148E-GE-45AT module.

New Software Features in Release 15.1(1)SY

- AAA-Domain Stripping at server group level—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/15-sy/sec-usr-aaa-15-sy-book/sec-domain-stripping.html
- Add support for the 61XX linecards in the 6513-E standby sup's slot with sup2T—See this publication.
- Auto Interleaved Port priority for LACP—See this publication:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-1SY/config_guide/sup2T/15_1_sy_swcg_2T/etherchannel.html

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-1SY/config_guide/sup720/15_1_sy_swcg_720/etherchannel.html
- BFD - Static Route Support—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bfd/configuration/15-sy/irb-15-sy-book/irb-bi-fwd-det.html
- BFD - VRF Support—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bfd/configuration/15-sy/irb-15-sy-book/irb-bi-fwd-det.html
- BFD IPv6 Encaps Support—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bfd/configuration/15-sy/irb-15-sy-book/ip6-route-bfd-encaps.html
- BFD Support for IP Tunnel (GRE, with IP address)—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bfd/configuration/15-sy/irb-15-sy-book/irb-bi-fwd-det.html
- BFD Support over port channel—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bfd/configuration/15-sy/irb-15-sy-book/irb-bi-fwd-det.html

- BGP - Remove/Replace Private AS Filter—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/configuration/15-sy/irg-15-sy-book/irg-remove-as.html

- BGP Event Based VPN Import—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/configuration/15-sy/irg-15-sy-book/irg-event-vpn-import.html

- BGP Neighbor Policy—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/configuration/15-sy/irg-15-sy-book/irg-neighbor-policy.html

- BGP Per Neighbor SOO Configuration—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/configuration/15-sy/irg-15-sy-book/irg-neighbor-soo.html

- BGP PIC Edge for IP/MPLS—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/configuration/15-sy/irg-15-sy-book/irg-bgp-mp-pic.html

- BGP RT changes without PE-CE neighbor impact—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios/iproute_bgp/configuration/guide/12_2sr/irg_12_2sr_book/irg_event_vpn_import.html

- BGP: RT Constrained Route Distribution—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/configuration/15-sy/irg-15-sy-book/irg-rt-filter.html

- BGPConsistency Checker—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/configuration/15-sy/irg-15-sy-book/irg-consistency-check.html

- Callhome V2 enhancements—See this publication:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-1SY/config_guide/sup2T/15_1_sy_swcg_2T/callhome.html

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-1SY/config_guide/sup720/15_1_sy_swcg_720/callhome.html

- Capabilities Manager—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/saf/configuration/15-sy/saf-15-sy-book/saf-capman.html

- RADIUS Change of Authorization (CoA)—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/15-sy/sec-usr-aaa-15-sy-book/sec-rad-coa.html

  https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/15-sy/sec-usr-aaa-15-sy-book/sec-cfg-authentifcn.html

- Cisco Express Forwarding - SNMP CEF-MIB Support—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipswitch_cef/configuration/15-sy/isw-cef-15-sy-book/isw-cef-snmp-mib.html

  http://www.cisco.com/c/en/us/td/docs/ios/ipswitch/configuration/guide/12_4/isw_12_4_book/cef_snmp_mib.html

- Cisco IOS Shell—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios/netmgmt/configuration/guide/Convert/IOS_Shell/nm_ios_shell.html

- Cisco TrustSec L3 Identity Port Mapping—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cts/configuration/15-sy/sec-cts-15-sy-book/sec-cts-id-port-map.html

  http://www.cisco.com/c/en/us/td/docs/switches/lan/trustsec/configuration/guide/trustsec/ident-conn_config.html

- Cisco TrustSec NDAC, Network Device Admission Control—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cts/configuration/15-sy/sec-cts-15-sy-book/sec-cts-ndac.html

  http://www.cisco.com/c/en/us/td/docs/switches/lan/trustsec/configuration/guide/trustsec/ident-conn_config.html

- Cisco TrustSec Subnet to SGT Mapping—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cts/configuration/15-sy/sec-cts-15-sy-book/cts-subnet-sgt-map.html

  http://www.cisco.com/c/en/us/td/docs/switches/lan/trustsec/configuration/guide/trustsec/ident-conn_config.html

- CISCO-IP-URPF-MIB Support—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios/sec_data_plane/configuration/guide/convert/sec_data_urpf_15_1_book/sec_urpf_mib.html

- Client Information Signalling Protocol (CISP)—See this publication:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-1SY/config_guide/sup2T/15_1_sy_swcg_2T/dot1x_port_based_authentication.html

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-1SY/config_guide/sup720/15_1_sy_swcg_720/dot1x_port_based_authentication.html

- Configurable System Controller Reset Threshold—With a redundant supervisor engine, if a TM_DATA_PARITY_ERROR, TM_LINK_ERR_INBAND, or TM_NPP_PARITY_ERROR error occurs, the affected supervisor engine reloads.

  Without a redundant supervisor engine, if a TM_DATA_PARITY_ERROR, TM_LINK_ERR_INBAND, or TM_NPP_PARITY_ERROR error occurs, one of the following happens:

  – If the system controller reset threshold has not been reached, reset the system controller ASIC.

  – If the system controller reset threshold has been reached, reload the supervisor engine.

  The default system controller reset threshold value is 1, configurable with the **platform system-controller reset-threshold** *threshold_value* command. The value range is 1 through 100.

  TM_DATA_PARITY_ERROR, TM_LINK_ERR_INBAND, and TM_NPP_PARITY_ERROR errors cause system messages.

  – Before the threshold is reached, the errors cause the following system messages:

    %SYSTEM_CONTROLLER-<>-THRESHOLD
    %SYSTEM_CONTROLLER-<>-ERROR
    %SYSTEM_CONTROLLER-<>-MISTRAL_RESET

  - After the threshold is reached, the errors cause the following system messages:

    %SYSTEM_CONTROLLER-<>-ERROR
    %SYSTEM_CONTROLLER-<>-FATAL

- Configuring ITU-T Y.1731 Fault Management Functions—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cether/configuration/15-sy/ce-15-sy-book/ce-cfm-ieee-y1731.html

- Console disconnect—See this publication:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/commands/additional_commands/cmds1.html

  Note This feature is enabled by default.

- CoPP Microflow policing—See this publication:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-1SY/config_guide/sup2T/15_1_sy_swcg_2T/control_plane_policing_copp.html

- Copy based sampling—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_basic/configuration/15-sy/mp-basic-15-sy-book/mp-ip-aware-mpls-netflow.html

- Custom Location Type—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cether/command/ce-cr-book.html

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cether/command/ce-cr-book/ce-e1.html

- DHCP - Server Port Based Address Allocation—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dhcp/configuration/15-sy/dhcp-15-sy-book/dhcp-prt-bsd-aa.html

- DHCP Relay Server Id Override and Link Selection Option 82 Suboptions—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dhcp/configuration/15-sy/dhcp-15-sy-book/dhcp-relay-svr-option-82.html

- Diagnostic Signatures—See this publication:
- EIGRP IPv6 VRF-Lite—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios/iproute_eigrp/configuration/guide/12_2sr/ire_12_2sr_book/ire_cfg_eigrp.html

- EIGRP MIB—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios/iproute_eigrp/configuration/guide/12_2sr/ire_12_2sr_book/ire_mib.html

- EIGRP Wide Metrics—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_eigrp/configuration/15-sy/ire-15-sy-book/ire-wid-met.html

- EIGRP/SAF HMAC-SHA-256 Authentication—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_eigrp/configuration/15-sy/ire-15-sy-book/ire-sha-256.html

- Embedded Event Manager (EEM) 3.1—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios/netmgmt/configuration/guide/12_2sx/nm_12_2sx_book/nm_eem_overview.html

  http://www.cisco.com/c/en/us/td/docs/ios/netmgmt/configuration/guide/12_2sx/nm_12_2sx_book/nm_eem_policy_cli.html

  http://www.cisco.com/c/en/us/td/docs/ios/netmgmt/configuration/guide/12_2sx/nm_12_2sx_book/nm_eem_policy_tcl.html
- Embedded Event Manager (EEM) 3.2—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios/netmgmt/configuration/guide/nm_eem_3-2.html
- Embedded Event Manager (EEM) 4.0—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/eem/configuration/15-mt/eem-15-mt-book/eem-overview.html
- Enabling OSPFv2 on an Interface Using the ip ospf area Command—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/15-sy/iro-15-sy-book.html
- EnergyWise 2.5—See this publication:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/energywise/phase2_5/ios/configuration/guide/2_5ewise.html
- EnergyWise Pre Phase 2.5—See this publication:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/energywise/phase2/ios/release/notes/OL19810.html
- EVN EIGRP—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/evn/configuration/15-sy/evn-15-sy-book/evn-confg.html

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/evn/configuration/15-sy/evn-15-sy-book/evn-overview.html
- EVN OSPF—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/evn/configuration/15-sy/evn-15-sy-book/evn-confg.html

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/evn/configuration/15-sy/evn-15-sy-book/evn-overview.html
- EVN Route Replication—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/evn/configuration/15-sy/evn-15-sy-book/evn-shared-svcs.html
- Flex Links Interface Preemption—See this publication:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-1SY/config_guide/sup2T/15_1_sy_swcg_2T/flexlinks.html

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-1SY/config_guide/sup720/15_1_sy_swcg_720/flexlinks.html
- Flexible Netflow - IPv6 bridged flows—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fnetflow/configuration/15-sy/fnf-15-sy-book/cfg-ipv6-brg.html

- FTP IPv6 Support—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_nman/configuration/15-sy/ip6n-15-sy-book/ip6-tftp-supp.html

- Geo Location Type support—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cether/command/ce-cr-book.html

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cether/command/ce-cr-book/ce-e1.html

- HA support for mLDP—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipmulti_lsm/configuration/15-sy/imc-lsm-15-sy-book/imc_ha_mldp.html

- Hierarchical shaping and two priority queues on WS-X6904-40G-2T—See this publication:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-1SY/config_guide/sup2T/15_1_sy_swcg_2T/qos_policy_based_queueing.html

- IEEE 802.1x - RADIUS Change of Authorization (CoA)—See this publication:

  https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/15-sy/sec-usr-aaa-15-sy-book/sec-cfg-authentifcn.html

  http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_a3.html

- IGMPv3 Host Stack—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipmulti_igmp/configuration/15-sy/imc-igmp-15-sy-book/imc_igmpv3_hoststack.html

- IP Aware MPLS Netflow—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_basic/configuration/15-sy/mp-basic-15-sy-book/mp-ip-aware-mpls-netflow.html

- IP Multicast Load Splitting - Equal Cost Multipath (ECMP) using S, G and Next-hop—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipmulti_optim/configuration/15-sy/imc-optim-15-sy-book/imc_load_splt_ecmp.html

- IP SLAs - LSP Health Monitor with LSP Discovery—See this publication:

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

- IP SLAs VRF Aware 2.0—See this publication:

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

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

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

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

- IP Tunnel - SSO—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/configuration/15-sy/ir-15-sy-book/ir-impl-tun.html

- IP-RIP Delay Start—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_rip/command/irr-cr-book/irr-cr-rip.html

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_rip/configuration/15-sy/bsm-15-sy-book/irr-cfg-info-prot.html
- IPv6 - Config Logger—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_nman/configuration/15-sy/ip6n-15-sy-book/ip6-emb-mgmt.html
- IPv6 - HTTP(S)—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_nman/configuration/15-sy/ip6n-15-sy-book/ip6-emb-mgmt.html
- IPv6 - Per Interface Neighbor Discovery Cache Limit—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_basic/configuration/15-sy/ip6b-15-sy-book/ip6-nd-cache.html
- IPv6 - TCL—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_nman/configuration/15-sy/ip6n-15-sy-book/ip6-emb-mgmt.html
- IPv6 ACL Extensions for Hop by Hop Filtering—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_acl/configuration/15-sy/sec-data-acl-15-sy-book/ip6-sec-acl-ext.html
- IPv6 BSR - Configure RP mapping—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipmulti_pim/configuration/15-sy/imc-pim-15-sy-book/imc_basic_ipv6.html
- IPv6 Device Tracking—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/15-sy/ip6-dev-track.html
- IPv6 Neigbor Discovery Non-Stop Forwarding (NSF)—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_basic/configuration/15-sy/ip6b-15-sy-book/ip6-neighb-disc.html
- IPv6 Neighbor Discovery Inspection—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/15-sy/ip6-nd-inspect.html
- IPv6 Policy-Based Routing—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_pi/configuration/15-sy/iri-15-sy-book/ip6-pbr.html
- IPv6 Router Advertisement (RA) Guard—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/15-sy/ip6f-15-sy-book/ip6-ra-guard.html
- IPv6 Routing: OSPF for IPv6 (OSPFv3) Authentication Support with IPsec—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/15-sy/iro-15-sy-book/ip6-route-ospfv3-auth-ipsec.html
- IPv6 Support for IPSec and IKEv2—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnips/configuration/15-sy/sec-sec-for-vpns-w-ipsec-15-sy-book/sec-cfg-vpn-ipsec.html

- IPV6 VACL (Vlan Access Control List)—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/15.1SY/config_guide/sup2T/vlan_acls.html#IPV6_VACL_(Vlan_Access_Control_List)

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/15.1SY/config_guide/sup720/vlan_acls.html#IPV6_VACL_(Vlan_Access_Control_List)

- IPv6: NSF & Graceful Restart for MP-BGP IPv6 Address Family—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/configuration/15-sy/irg-15-sy-book/ip6-mbgp-nsf-gr-rest.html

- IS-IS - MPLS LDP Synchronization—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_ldp/configuration/15-sy/mp-ldp-15-sy-book/mp-ldp-igp-synch.html

- ISIS BFD TLV—The IS-IS Bidirectional Forwarding Detection (BFD) Tag Length Value (TLV) feature provides a faster method to detect a loss of an IS-IS adjacency. Before, when an IS-IS adjacency reached the UP state (and therefore could be used for forwarding), a BFD session needed to be established with that neighbor. Now, a BFD session is maintained as long as the hello holddown timer for the neighbor does not expire, which is new for BFD TLV. The BFD session is only deleted if the neighbor hello times out. If BFD signals to IS-IS that a session has gone DOWN, the adjacency associated with that session will transition to DOWN state. Once the BFD session goes back UP, the adjacency state can transition back to an UP state.

  For a given IS-IS topology, IS-IS determines if BFD is usable for a given neighbor on that topology. BFD is not usable when BFD is enabled on both sides and the BFD session is down. When there are multiple BFD sessions enabled for different address families, such as IPv4 and IPv6, if BFD is not usable for any address family, then BFD is consider not usable for the entire adjacency on that topology. For example, if both IPv4 and IPv6 BFD are enabled for single topology, if either the IPv4 BFD session is down or IPv6 BFD session is down, the neighbor state will be set to DOWN state. If BFD is not enabled for a given address family, then BFD is considered usable for that address family.

  For single topology mode, the neighbor state is down when either the IPv4 or IPv6 BFD session is not BFD usable, that is, if BFD is enabled on both sides and the BFD session is DOWN. If BFD is not enabled on either side, BFD will be set to TRUE. For multi-topology mode, IS-IS adjacency will be in UP state as long as any topology is UP . However, the neighbor for the topology where BFD is consider not usable is considered down for that specific topology. For example, if both IPv4 and IPv6 BFD are enabled, and the IPv4 session is DOWN and IPv6 session is UP, then the IS-IS adjacency is still UP. In this case, the IPv4 neighbor is considered DOWN and ipv6 neighbor is considered UP.

- ISIS client for BFD c-bit support—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bfd/configuration/xe-3s/irb-xe-3s-book/irb-bfd-isis-cbit.html

- ISIS IPv6 client for BFD—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bfd/configuration/15-sy/irb-15-sy-book/ip6-bfd-isis-client.html

- ISIS MTR for multicast address familly only—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mtr/configuration/15-sy/mtr-15-sy-book/isis-mtr-multicast-address-family.html

- IS-IS Support for an IS-IS Instance per VRF for IP—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_isis/configuration/15-sy/irs-15-sy-book/irs-instance-vrf.html

- ISSU - IPv6 Multicast—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipmulti_resil/configuration/15-sy/imc-resil-15-sy-book/imc_high_availability.html

- ISSU - MPLS VPN 6VPE & 6PE ISSU support—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_ha/configuration/15-sy/mp-ha-15-sy-book/mp-6vpe-6pe-issu-sso.html

- L2VPN Advanced VPLS (A-VPLS)—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_l2_vpns/configuration/15-sy/mp-l2-vpns-15-sy-book/mp-l2vpn-adv-vpls.html

- LACP 1:1 hotstandby dampening—See this publication:
- Linecards not supported in 15.1(1)SY—See this publication:
- LLDP Inline Power Negotiation for PoE+—See this publication:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-1SY/config_guide/sup2T/15_1_sy_swcg_2T/power_over_ethernet.html+

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-1SY/config_guide/sup720/15_1_sy_swcg_720/power_over_ethernet.html+

- LLDP IPv6 address support—See this publication:

- LLDP IPv6 address support—The release support IPv6 Link Layer Discovery Protocol (LLDP) and LLDP Media Endpoint Discovery (MED) addresses.
- Mac Move and Replace—See this publication:

- Manually configured IPv6 in IPv4 with IPSec—The Manually Configured IPv6 in IPv4 with IPsec feature complies with U.S. Government IPv6 (USGv6) guidelines by supporting the following IPsec features:
  - IPv6 Support for IPsec and IKEv2. For more information about this feature, see the “Configuring Internet Key Exchange Version 2 (IKEv2) and FlexVPN Site-to-Site” module and the “Configuring Security for VPNs with IPsec” module at the following links:

    http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/15-sy/sec-flex-vpn-15-sy-book/sec-cfg-ikev2-flex.html

    http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnips/configuration/15-sy/sec-sec-for-vpns-w-ipsec-15-sy-book/sec-cfg-vpn-ipsec.html

  - OSPF for IPv6 (OSPFv3) Authentication Support with IPsec. For more information about this feature, see the “IPv6 Routing: OSPF for IPv6 Authentication Support with IPsec” module at the following link:

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

  - Call Home version 2 enhancements.

- Medianet Metadata—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mdata/configuration/15-sy/mdata-15sy-book/metadata-framework.html

- MLD Group Limits—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipmulti_lsm/configuration/15-sy/imc-lsm-15-sy-book/ip6-mcast-mld-limits.html

- mLDP Filtering—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipmulti_lsm/configuration/15-sy/imc-lsm-15-sy-book/imc_mldp_filter.html

- MLDP-Based MVPN—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipmulti_lsm/configuration/15-sy/imc-lsm-15-sy-book/imc_mldp-based_mvpn.html

- MPLS LDP - IGP Synchronization—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_ldp/configuration/15-sy/mp-ldp-15-sy-book/mp-ldp-igp-synch.html

- MPLS over GRE—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_l2_vpns/configuration/15-sy/mp-l2-vpns-15-sy-book/vpls-o-gre.html

- MPLS Pseudowire Status Signaling—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_l2_vpns/configuration/15-sy/mp-l2-vpns-15-sy-book/mp-pw-status.html

- MPLS TE - BFD-triggered Fast Reroute (FRR)—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_te_path_protect/configuration/15-sy/mp-te-path-protect-15-sy-book/mp-te-bfd-frr.html

- MPLS Traffic Engineering (TE) - Path Protection—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_te_path_protect/configuration/15-sy/mp-te-path-protect-15-sy-book/mp-te-path-prot.html

- MTR Support for Multicast—See this publication:

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

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mtr/configuration/15-sy/mtr-15-sy-book/isis-mtr-multicast-address-family.html

- Multi-auth Vlan Assignment—See this publication:

- Multicast Expansion Table Enhancement for VPLS—See this publication:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/commands/additional_commands.html

- Multicast Service Reflection—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipmulti_serv/configuration/15-sy/imc-serv-15-sy-book/imc_service_reflect.html

- MVPN - Data MDT Enhancements—Multicast distribution tree (MDT) groups were selected at random when the traffic passed the threshold and there was a limit of 255 MDTs before they were reused. The MVPN - Data MDT Enhancements feature provides the ability to deterministically map the groups from inside the VPN routing and forwarding (S,G) entry to particular data MDT groups, through an access control list (ACL).

  The user can now map a set of VPN routing and forwarding (S,G) to a data MDT group in one of the following ways:

  – 1:1 mapping (1 permit in ACL)

  – Many to 1 mapping (many permits in ACL)

  – Many to many mapping (multiple permits in ACL and a nonzero mask data MDT)

  Because the total number of configurable data MDTs is 1024, the user can use this maximum number of mappings in any of the described combinations.

- NAT - VRF Aware NAT—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/15-sy/nat-15-sy-book/iadnat-mpls-vpn.html

- NEAT (Network Edge Authentication Topology)—See this publication:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-1SY/config_guide/sup2T/15_1_sy_swcg_2T/dot1x_port_based_authentication.html

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-1SY/config_guide/sup720/15_1_sy_swcg_720/dot1x_port_based_authentication.html

- Netflow Data Export to a collector in a VRF—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios/netflow/command/reference/nf_book/nf_01.html

- Netflow(TNF) Export L2 mac and port information for IPv4—See this publication:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-1SY/config_guide/sup720/15_1_sy_swcg_720/netflow.html

- NHRP Reformation move to IP Services—The Next Hop Resolution Protocol (NHRP) is supported in the IP Services image.

- No Service Password-Recovery 15.1SY—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cfg/configuration/15-sy/sec-usr-cfg-15-sy-book/sec-no-svc-pw-recvry.html

- NSF/SSO - IPv6 Multicast—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipmulti_resil/configuration/15-sy/imc-resil-15-sy-book/imc_high_availability.html

- NTPv4 MIB—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/bsm/configuration/15-sy/bsm-15-sy-book/bsm-ntpv4-mib.html

- NTPv4 Orphan Mode support, Range for trusted key configuration—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/bsm/configuration/15-sy/bsm-15-sy-book/bsm-time-calendar-set.html

- NTPv4 with support for IPv4 and IPv6—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/bsm/configuration/15-sy/bsm-15-sy-book/ip6-ntpv4.html

- OSPF - Non-Stop Routing—See this publication:

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

- OSPF for Routed Access—The OSPF for Routed Access feature allows users to extend layer 3 routing capabilities to the access or Wiring Closet. OSPF for Routed Access supports only one OSPFv2 and one OSPFv3 instance with a maximum number of 200 dynamically learned routes permitted.

  With the typical hub and spoke topology in a campus environment, the Wiring Closets (spokes) are connected to the distribution switch (Hub) forwarding all non-local traffic to the distribution layer. There is no requirement to hold a complete routing table at the Wireless Closet switches. In best practices designs, the distribution switch sends a default route to the Wiring Closet switch for reaching inter- area and external routes (OSPF Stub area configuration). The OSPF for Routed Access feature supporst this type of topology.

  The IP base image supports OSPF for Routed Access. The Enterprise services image continues to be required if multiple OSPFv2 and OSPFv3 instances with no route restrictions are required. Additionally, Enterprise Services is required to enable the VRF-lite feature.

- OSPF Graceful Shutdown—See this publication:

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

- OSPF support for NSSA RFC 3101—See this publication:

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

- OSPF TTL Security Check—See this publication:

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

- OSPFv3 Address Families—See this publication:

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

- OSPFv3 BFD—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bfd/configuration/15-sy/irb-15-sy-book/ip6-route-bfd-ospfv3.html

- OSPFv3 Fast Convergence - LSA and SPF throttling—See this publication:

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

- OSPFv3 Graceful Restart—See this publication:

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

- OSPFv3 IPSec ESP Encryption and Authentication—See this publication:

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

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

- OSPFv3 VRF-Lite/PE-CE—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/command/iro-cr-book.html

- Parser concurrency and locking Improvements—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/config-mgmt/configuration/15-sy/config-mgmt-15-sy-book/cm-parse-improve.html

- Password strength and management for Common Criteria—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/15-sy/sec-usr-aaa-15-sy-book/sec-aaa-comm-criteria-pwd.html

- Per Port Location Configuration—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cether/configuration/15-sy/ce-15-sy-book/ce-per-port-loc-config.html

- PIM MIB Extension for IP Multicast—See this publication:

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

- PIMv6: Anycast RP solution—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipmulti_pim/configuration/15-sy/imc-pim-15-sy-book/imc_basic_ipv6.html

- PoE Plus (PoE+, PoEP) support—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/15.1SY/config_guide/sup2T/power_over_ethernet.html#PoE_Plus_(PoE+,_PoEP)_support

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/15.1SY/config_guide/sup720/power_over_ethernet.html#PoE_Plus_(PoE+,_PoEP)_support

- POE/POEP support on Sup2T in VSS mode—See this publication:

- Port Security on Etherchannel Trunk Port—See this publication:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-1SY/config_guide/sup2T/15_1_sy_swcg_2T/port_security.html

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-1SY/config_guide/sup720/15_1_sy_swcg_720/port_security.html

- Product Security Baseline: Password encryption and complexity restrictions—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cfg/configuration/15-sy/sec-usr-cfg-15-sy-book/sec-cfg-sec-4cli.html

- Radius over IPv6—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/15-sy/sec-usr-aaa-15-sy-book/ip6-aaa-support.html

- Radius Per-VRF Server Group—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/15-sy/sec-usr-aaa-15-sy-book/sec-per-vrf-aaa.html

- Radius Statistics VIA SNMP—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_rad/configuration/15-sy/sec-usr-rad-15-sy-book/sec-cfg-radius.html

- RSVP Support for Ingress Call Admission Control—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_rsvp/configuration/15-sy/qos-rsvp-15-sy-book/config-rsvp.html

- SAF Dynamic Neighbors—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/saf/configuration/15-sy/saf-15-sy-book/saf-dyn-neigh.html

- Show Command Section Filter—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/command/Cisco_IOS_Configuration_Fundamentals_Command_Reference.html

- Smart Install—See this publication:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/smart_install/configuration/guide/smart_install.html

- SSH Re-Key Support for Server—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_ssh/configuration/15-sy/sec-usr-ssh-15-sy-book/sec-usr-ssh-sec-shell.html

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/d1/sec-d1-cr-book/sec-cr-i3.html

- SSHv2 Enhancements—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_ssh/configuration/15-sy/sec-usr-ssh-15-sy-book/sec-secure-shell-v2.html

- SSHv2 Enhancements for RSA Keys—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_ssh/configuration/15-sy/sec-usr-ssh-15-sy-book/sec-secure-shell-v2.html

- SSO - MPLS VPN 6VPE & 6PE SSO support—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_ha/configuration/15-sy/mp-ha-15-sy-book/mp-6vpe-6pe-issu-sso.html

- Static Route Support for BFD over IPv6—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bfd/configuration/15-sy/irb-15-sy-book/ip6-bfd-static.html

- Storm Control action -- Port disable—See this publication:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-1SY/config_guide/sup2T/15_1_sy_swcg_2T/traffic_storm_control.html

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-1SY/config_guide/sup720/15_1_sy_swcg_720/traffic_storm_control.html

- Switch location configuration—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cether/command/ce-cr-book.html

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cether/command/ce-cr-book/ce-e1.html

- Tacacs over IPv6—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/15-sy/sec-usr-aaa-15-sy-book/ip6-tacacs.html

- TFTP IPv6 support—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_nman/configuration/15-sy/ip6n-15-sy-book/ip6-tftp-supp.html

- TrustSec Identity Port Mapping—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cts/configuration/15-sy/sec-cts-15-sy-book/sec-cts-id-port-map.html

  http://www.cisco.com/c/en/us/td/docs/switches/lan/trustsec/configuration/guide/trustsec/arch_over.html

- TrustSec Security Group Name Download—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cts/configuration/15-sy/sec-cts-15-sy-book/sec-cts-sg-download.html

- TrustSec SGA Environment-Data Change of Authority—See this publication:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/trustsec/configuration/guide/trustsec/arch_over.html

- TrustSec SGA SGACL Policy Change of Authority—See this publication:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/trustsec/configuration/guide/trustsec/arch_over.html

- TrustSec SGT Caching—See this publication:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/trustsec/configuration/guide/trustsec/arch_over.html

- TrustSec SGT RBACL Monitor Mode (Dryrun)—See this publication:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/trustsec/configuration/guide/trustsec/arch_over.html

- TrustSec SxP Loop Detection—See this publication:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/trustsec/configuration/guide/trustsec/arch_over.html

- TTL Security Support for OSPF on IPv6—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/15-sy/iro-15-sy-book/iro-ttl-sec-ospfv3.html

- VPLS Autodiscovery, BGP-based—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_l2_vpns/configuration/15-sy/mp-l2-vpns-15-sy-book/vpls-auto-bgp.html

- VPLS over GRE and MPLS over GRE—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_l2_vpns/configuration/15-sy/mp-l2-vpns-15-sy-book/vpls-o-gre.html

- VRF aware NTP—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/bsm/configuration/15-sy/bsm-15-sy-book/bsm-time-calendar-set.html

- VRF aware source interface for syslog transactions—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/esm/configuration/15-sy/esm-15-sy-book/esm-vrf.html

  http://www.cisco.com/c/en/us/td/docs/ios/ipv6/command/reference/ipv6_book/ipv6_09.html

  http://www.cisco.com/c/en/us/td/docs/ios/netmgmt/command/reference/nm_book/nm_09.html

- VRF support for TFTP server, TFTP Client, and FTP client—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/command/Cisco_IOS_Configuration_Fundamentals_Command_Reference.html

- VRF-aware ARP debug—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_arp/configuration/15-sy/arp-15-sy-book/arp-vrfaware-arp.html
- VRRPv3 Protocol Support—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/15-sy/fhp-15-sy-book/fhrp-vrrpv3.html
- WCCP - Configurable Router ID—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp/configuration/15-sy/iap-15-sy-book/iap-wccp-cfg-rtr-id.html
- WCCP: Fast Timers—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp/configuration/15-sy/iap-15-sy-book/iap-wccp-ftimers.html
- Web Services Management Agent (WSMA)—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/wsma/configuration/15-sy/wsma-15-sy-book/wsma.html
- Web Services Management Agent with TLS—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/wsma/configuration/15-sy/wsma-15-sy-book/wsma-tls.html
- WSMA and XMLPI enhancement—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/wsma/configuration/15-sy/wsma-15-sy-book/wsma.html
- XML-PI—See this publication:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/xmlpi/configuration/15-sy/xml-pi-15-sy-book/xml-pi.html

Software Features from Earlier Releases

Use Cisco Feature Navigator to display supported features that were introduced in earlier releases.

Unsupported Commands

Cisco IOS images for the Supervisor Engine 2T do not support **mls** commands or **mls** as a keyword. See this document for a list of some of the **mls** commands that have been replaced:

http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/replacement_commands.html

Note Some of the replacement commands support different keyword and parameter values than those supported by the Release 12.2SX commands.

Cisco IOS images for the Supervisor Engine 2T do not support these commands:

- **ip multicast helper-map**
- **ip pim accept-register route-map**

Unsupported Features

Note The IPsec Network Security feature (configured with the crypto ipsec command) is supported in software only for administrative connections to Catalyst 6500 series switches.

These features are not supported in Release 15.1SY:

- WAN features
- Performance Routing (PfR)
- OER Border Router Only Functionality
- Flexible NetFlow on Supervisor Engine 720-10GE and Supervisor Engine 720
- IOS Server Load Balancing (SLB)

  Note Release 15.1SY supports server load balancing (SLB) as implemented on the Application Control Engine (ACE) module (ACE30-MOD-K9).

- AppleTalk
- Cisco Group Management Protocol (CGMP)
- Distance Vector Multicast Routing Protocol (DVMRP)
- Dynamic creation of L2 entries for Multicast source-only traffic
- IDS Copy

  Note Release 15.1SY supports the SPAN and VACL redirect features, which have equivalent functionality.

- Inter-Switch Link (ISL) trunking

  Note Release 15.1SY supports IEEE 802.1Q trunking.

- NAC - L2 IP NAC LAN Port IP
- These Novell NetWare protocols:
  - Internetwork Packet Exchange (IPX)
  - NetWare Link-Services Protocol (NLSP)
  - Service Advertising Protocol (SAP)
  - IPX Access Control List Violation Logging
  - IPX Access List Plain English Filters
  - IPX Control Protocol
  - IPX Encapsulation for 802.10 VLAN
  - IPX Multilayer Switching (IPX MLS)
  - IPX Named Access Lists

  - IPX SAP-after-RIP
- Network Based Application Recognition (NBAR)
- Per-VLAN Spanning Tree (PVST) mode (**spanning-tree mode pvst** global configuration mode command) on Supervisor Engine 2T

Note Release 15.1SY supports these spanning tree protocols:
—Rapid Spanning Tree Protocol (RSTP):
- **spanning-tree mode rapid-pvst** global configuration mode command
- Enabled by default

—Multiple Spanning Tree Protocol (MSTP):
- **spanning-tree mode mst** global configuration mode command
- Can be enabled

- Router-Port Group Management Protocol (RGMP)
- Stub IP Multicast Routing
- TCP Intercept

Note Release 15.1SY supports the Firewall Services Module (WS-SVC-FWM-1-K9).

- Integrated routing and bridging (IRB)
- Concurrent routing and bridging (CRB)
- Remote source-route bridging (RSRB)
- AppleTalk
- Distance Vector Multicast Routing Protocol (DVMRP)

Restrictions

Identifier	Component	Description
CSCvi28828	nat	Dynamic Nat preferred over Static Nat with Route maps, For overlapping IP addresses.
CSCue03536	accsw-fex	6800IA Host port takes 1 minute to go down after "shut" w/ 255 vlans
CSCue69088	accsw-fex	6800IA Image downloaded twice when IA controller pushes image.
CSCue63014	accsw-fex	OBFL info for 6800IA stack modules does not show on 6800IA stack master
CSCtx50938	cat6000-acl	c2ma2: FHS: Ra guard features not working without creating the SVI.
CSCtr15373	cat6000-acl	Standby crashes when copy config from tftp to running-config
CSCts70036	cat6000-acl	With mld snooping,no egress traff seen on v6 vacl vlan after reload/sso.
CSCub95435	cat6000-env	Sup2T can't deliver 100% throughput on certain 67xx/68xx line cards
CSCum92372	cat6000-env	6880-X : during ISSU from 15.1(2)SY2 to 15.1(2)SY1, Standby gets stuck
CSCsh58964	cat6000-fabric	BFD node down is detected by OIR
CSCud98528	cat6000-fabric	CFEX: sh inventory does not show vid, transceiver info on controller

Identifier	Component	Description
CSCum45172	cat6000-filesys	6880-X : Unable to generate core dump file
CSCuj04111	cat6000-firmware	6880-X Switch: multicast pkts upto 64 byte dropped in certain conditions
CSCtx83397	cat6000-l2	changing switchport mode doesn't reflect in the STP instances
CSCub86977	cat6000-l2-infra	c4hd1: Config sync seen with +encapsulation dot1Q 100
CSCta83272	cat6000-l2-mcast	IGMP snooping not supported over VPLS ckt.
CSCth16692	cat6000-l2-mcast	IGMPSN report suppression failed to redir MIXED mode same group joins
CSCta03980	cat6000-l2-mcast	PIMSN:No multicast data flood with IGMPSN disable & PIMSN enabled
CSCsv98626	cat6000-l2-mcast	Ear8 MVR interaction with IGMP snooping: when IGMPSN is disabled
CSCua92717	cat6000-l2-mcast	sh ip igmp snooping subscriber-rate not working in SUP 720 mtrose images
CSCub68144	cat6000-l2-mcast	MCVPLS: Traffic drop seen when 2 PEs sent IGMPv2 join for the same group
CSCto92033	cat6000-l2-mcast	Multicast data frames blackholed if RTR-GRD is ON and Snooping is OFF
CSCtl86457	cat6000-l2-mcast	RL for IP Multicast Control frames doesn't work properly
CSCty00850	cat6000-l2-mcast	Root sends GQ instead global leave due to L2 MLD querier flaps
CSCub68068	cat6000-l2-mcast	Wrong Pseudo Port added as mrtr port after IGMPv2 Leave sent
CSCtd18777	cat6000-mcast	NAT config punt Multicast frames to Process Switching
CSCtg58715	cat6000-mcast	"show mac addr static vlan" CLI does not display mcast entries
CSCtf59230	cat6000-mcast	Earl8 performance impact on Bidir-PIM routing cases
CSCtg91060	cat6000-mcast	IPV6 PING not working on SVI when MLD Snooping is turned ON
CSCug86353	cat6000-mcast	Counter not upd for h/w switched pkts in show ip pim interface count
CSCti43981	cat6000-mcast	HW BiDir mroutes not restored after temporarily losing the RP path
CSCto75104	cat6000-mcast	Mcast Traffic blkholing upon VSS DA when all VSL links are on DFC
CSCuh77881	cat6000-mcast	MET is not programmed for few LSM groups with P2MP with ttl-RL config
CSCti97217	cat6000-mcast	Traffic forwarding to incorrect fabric channel after PO shu/no shut
CSCue59513	cat6000-mcast	VS4O: After SSO Traffic flood to uninterested receivers in vlan ~30 sec
CSCtr05033	cat6000-mpls	Caveats for MPLS VPN over mGRE
CSCue20501	cat6000-mpls	Tagged packets are dropped by FEX Node in Port mode EoMPLS
CSCud83572	cat6000-netflow	FEX: fex-node-id's and layer2 fields can not export together
CSCtq43621	cat6000-rommon	fc2 image:Verification FAILED err seen on bootup whn cs_fips disable_dev
CSCua37884	cat6000-routing	MA2: IPV6 BFD sessions keep flapping periodically when interval < 200ms
CSCtz90055	cat6000-routing	MA2:No recirc in case of BGP PIC on MPLS TE causing traffic drop
CSCuc85040	cat6000-routing	Equal cost paths not programmed in hardware for 6800-IA clients
CSCtz90758	cat6000-routing	MA2 : CEF glean rate-limiter not working for IPv6
CSCtj16159	cat6000-svc	standby reboots twice and comes up in rpr due to config sync fail
CSCui44669	cat6000-vntag	MK1:FEX:Traffic loss upon Estelle Reset (loss while come up)
CSCtw91029	cts	clear cts role-based counters does not give expected results
CSCui49308	fex-infra	IP fragmentation/MTU issues on FEX host Port
CSCub99424	ip-tunnels	TB seen @ xdr_mcast_receive_process on sso

Identifier	Component	Description
CSCty37278	ip-tunnels	Tunnel forwarding down if no global IP address configured.
CSCtz90970	ip-tunnels	A loop in the OCE chain has been detected when IPinIP tunnel goes down
CSCth50799	pim	Multicast traffic slow convergence with 20k-30k mroute entries

Caveats in Release 15.1SY

Open Caveats in Release 15.1(2)SY

Identifier	Component	Description
CSCuz97414	aaa	Bulk-sync failure due to ip radius source-interface Vlan701 vrf VRF_MGMT
CSCur88582	cat6000-ipc	CSCup64093 : Revisit due to ipc related error on New Active (crash file)
CSCvb23949	cat6000-firmware	Ping Process is not successful with speed 100 after reloading the box
CSCux80288	cat6000-ha	VSS switchover takes too much time for ECMP/MEC

Open Caveats in Release 15.1(1)SY

Identifier	Component	Description
CSCue27826	c6k-l3-lisp	LISP: set dscp tunnel with LISP not marking outer hdr for IPv6 traffic
CSCug08012	cat6000-acl	LISP: Encap traffic drops if we unconfigure "ipv4 etr"
CSCue72286	cat6000-diag	MA2b:Diagnostic handler is not found for DFC card after switchover
CSCuj53393	cat6000-filesys	Trifecta: Trifecta LC hangs during bootup at rommon.
CSCuf24777	cat6000-l2-mcast	MCVPLS: PIMSN (*,g) mroutes not removed after stops joins and source
CSCuf83644	cat6000-lisp	LISP: Traffic drop on ITR encap when destined to PETR
CSCud42723	cat6000-lisp	LISP:Adj is pointing to recirc instead of LISP0 for IPv6 VRF traffic
CSCud26697	cat6000-ltl	%BIT-SW1-4-OUTOFRANGE: error on 11/17 build
CSCud45116	cat6000-mcast	MCVPLS: Traffic drop seen at other Rx when one of the Rx sends leave
CSCtj90838	cat6000-medianet	packet counters in "show policy-map type perf int" not working on Cat6k
CSCug28878	cat6000-qos	c4mk1: Traceback@vs_get_pslot_switch_id
CSCue65316	cat6000-routing	MA2b:MPLS recirc goes missing for newly added NHRP node in L2oGRE
CSCug23479	cat6k-vs-infra	Switch PMK configured on slot 6 sup not synced to sup on slot 5
CSCtn53347	ip-tunnels	Issue with tunnel path_mtu_discovery after sso switchover
CSCue53147	ipmulticast	C4 Quadsup Traffic drops seen twice~2 sec after 130 seconds of sso
CSCtz48366	ipsec-core	Standby config is getting marked dirty during boot due to ctid/crypto
CSCub89797	mpls-mfi	Standby Router reloads due to Config Sync: Line-by-Line sync failure
CSCtz12715	nat	TB while deleting Static nat entry which has interface as global address

Caveats Resolved in Release 15.1(2)SY16

Identifier	Component	Description
CSCvi48253	pki	Self-signed certificates expire on 00:00 1 Jan 2020 UTC, can't be created after that time
CSCvp79333	ssh	SSH may crash due to a corrupt MAC

Caveats Resolved in Release 15.1(2)SY15

Identifier	Component	Description
CSCuu40566	cts	C6509E-SUP2T crash eap_fast_process_server_provi_hello
CSCuv06790	cts	IPDT enabled on PortChannel

Caveats Resolved in Release 15.1(2)SY14

Identifier	Component	Description
CSCvk25074	cat6000-dot1x	cat6000 authentication violation restrict does not stop all traffic in Closed authentication

Caveats Resolved in Release 15.1(2)SY13

Identifier	Component	Description
CSCvi05126	ipsec-isakmp	ISAKMP Notification messages carry unnecessary data

Caveats Resolved in Release 15.1(2)SY12

Identifier	Component	Description
CSCvd72069	asr1k-spa-infra	Test CLI Removal- SPA SIP Security Vulnerability
CSCuv31135	bgp	Disable connected-check in one side only makes route as unreachable
CSCuu76493	energywise	Cisco IOS and IOS XE Software EnergyWise Denial of Service Vulnerabilities
CSCvd73664	ethernet-lldp	Link Layer Discovery Protocol Format String Vulnerability
CSCvd73487	ethernet-lldp	Link Layer Discovery Protocol Buffer Overflow Vulnerability
CSCvh43691	glbp	Crash at glbp address comparison.
CSCus29873	ip	Active RP Crash on EoGRE Session Scale
CSCuj73916	ipsec-isakmp	Cisco IOS and IOS XE Software Internet Key Exchange Version 1 Denial of Service Vulnerability
CSCum85493	ipsec-isakmp	IPSEC session fails to come up with tunnel protection
CSCum44673	ntp	Limited Mode 6 denial-of-service vulnerability on NTP server and client

Identifier	Component	Description
CSCux99025	ntp	Evaluation of Cisco IOS and IOS-XEl for NTP January 2016
CSCva74756	ospf	OSPF Rogue LSA with maximum sequence number vulnerability
CSCva46459	ssh	SSH session hangs if it is not closed properly
CSCuc53853	tcp	Cisco IOS Switch HTTP Server DoS Vulnerability
CSCus42252	telnet	Cisco IOS XE Software User EXEC Mode Root Shell Access Vulnerability

Caveats Resolved in Release 15.1(2)SY11

Identifier	Component	Description
CSCve26748	cat6000-env	720 QUAD sup :: Delay in port going down during CSSO crash

Caveats Resolved in Release 15.1(2)SY10

Identifier	Component	Description
CSCuw14021	accsw-fex	6800 IA host ports may remain \"shut\" after IA module is reloaded
CSCum41167	bgp	Importing multipath routes changes next-hop to 0.0.0.0 and traffic fails
CSCux73118	cat6000-acl	Active Sup Crash when ping vrf with inside global address
CSCut40437	cat6000-acl	ACL addrgroup/portgroup object-group names are missing after SSO
CSCuv86525	cat6000-acl	SUP2T drops DHCP OFFER when snooping is enabled on DHCP-Server vlan
CSCva00330	cat6000-cm	IPv6 ACL not programming in hw
CSCuq64784	cat6000-env	sso: fake temp alarm fall back to normal "show env alarm" -alarm seen
CSCuy46992	cat6000-eobc	ifInDiscards seen via SNMP on EOBC(EO0/2) does not match CLI counter
CSCux07070	cat6000-firmware	High CPU due to Interrupt on C6880-X-16P10G
CSCus31811	cat6000-firmware	Recovery patch is triggered from Firmware seen in ISSU run version
CSCva43178	cat6000-hw-fwding	ipIfStatsHCOutOctets.ipv6 calculated wrong value at port-channel I/F
CSCuz97186	cat6000-l2	6880X VSL Ports show as "Half-duplex" after ISSU version up
CSCux69697	cat6000-l2-ec	flow control inconsistency for MEC after module reload
CSCux06506	cat6000-l2-infra	sup6t: After Peform 2 sso,power-up LC card-(VSL/RSL)Ports not coming up
CSCvb36172	cat6000-l2-mcast	IGMP Join for groups 224.0.0.x are programmed in the IGMP snooping table
CSCvb36981	cat6000-mcast	Multicast stream failures because of missing pmask in FPOE
CSCuq88523	cat6000-mpls	VPLS configuration and removal causing atom mem leaks
CSCvc82203	cat6000-mpls	IPv6 traffic not working after switchover
CSCuy64453	cat6000-sw-fwding	Sup2T - IBC freeze check code needs to be enhanced
CSCue38584	eigrp	EIGRP incorrectly compares metrics between EIGRP and MP-BGP (EIGRP)
CSCux91478	fex-infra	Specific FEX ID will not come online due to SDP timeout

Identifier	Component	Description
CSCva42833	ip-acl	Object groups with a unique combination command gets rejected
CSCuz22824	os-logging	CHUNKBADFREEMAGIC: Bad free magic number in chunk header - crash
CSCub43400	sla	Sequence error returned for some probes
CSCvb16274	vpdn	PPTP Start-Control-Connection-Reply packet leaks router memory contents

Caveats Resolved in Release 15.1(2)SY9

Identifier	Component	Description
CSCvb29204	ipsec-isakmp	BenignCertain on IOS and IOS-XE

Caveats Resolved in Release 15.1(2)SY8

Identifier	Component	Description
CSCva39982	cat6000-acl	IPv6 neighbor discovery packet processing behavior
CSCuy15043	cat6000-acl	MCL failure seen with "ip device tracking max 5" cli leads to RPR mode.
CSCux46815	cat6000-cm	Inconsistent RACL Reduced and BAD LOU errors
CSCuv62448	cat6000-cm	Mem leaks after adding DAI config with DHCP snooping
CSCva51425	cat6000-env	QuadSup:save information if sup reloads due to sw watchdog timeout
CSCuv08707	cat6000-env	C6880-X - module 5 asic-1 temperature is "N/O"
CSCuw30287	cat6000-env	Alingment fix for EHCI controller data structures
CSCux67359	cat6000-env	VSS standby Power-Capacity Watts display is incorrect
CSCuz03015	cat6000-env	EARL Recovery Patch triggered! Reason:[Firmware Fatal Int]
CSCuy25743	cat6000-env	C6880-X-LE: Contiguous 4 10G ports goes down and cannot be brought up
CSCux51666	cat6000-firmware	GLC-T ports may stay in down / notconnect state on standby VSS chassis
CSCur45930	cat6000-firmware	Standby ICS crashes at pyramid_lbc_err_interrupt_handler upon reload
CSCuv73899	cat6000-firmware	TestErrorCounterMonitor can generate false positive on 67XX cards.
CSCux06662	cat6000-firmware	Drops ower macsec in case od IPSEC traffic
CSCuy31847	cat6000-firmware	Flapping GLCT link results in VSL link going down
CSCut23413	cat6000-filesys	Sup2t may crash while executing more system:running-config cmd
CSCuz10094	cat6000-hw-fwding	Sup2T - Need CLI to modify earl patch recovery module reset threshold
CSCva26388	cat6000-hw-fwding	show plat software e8-recovery config is blank
CSCuz08070	cat6000-hw-fwding	EARL Patch Recovery logs are not sent to syslogs server
CSCup87407	cat6000-l2-infra	Quad Sup720 VSS unicast flooding on orphaned ports
CSCuz96214	cat6000-l2-infra	MK51 : PO is not coming up after remove/add
CSCva59171	cat6000-l2-infra	device going to rpr mode after config "fc recieve desire" and sso

Identifier	Component	Description
CSCuz02973	cat6000-mcast	Multicast drops due to incorrect FPOE mask - EDC has duplicate entries
CSCut57054	cat6000-mcast	sup2t-ha,2-sup-vss:ltl is not synced to standby
CSCus68990	cat6000-netflow	Crash when configuring NDS sender version 5
CSCuu55288	cat6000-netflow	Mechanism to throttle NDE export
CSCuu18398	cat6000-netflow	NDE interface seen in the "show cdp neighbors" output in the NBR switch
CSCuz77753	cat6000-sw-fwding	Follow up of CSCuz28618
CSCux81232	cat6000-sw-fwding	6500 performance High CPU when receive unknown LLC frame
CSCux28695	cat6000-snmp	Mk41: SNMP CPUHOG seen and terminator crashes after deleting/adding fex
CSCuy47777	cat6000-svc	NAM 6.2(1) does not boot successfully in VSS standby chassis
CSCuu18019	cat6000-qos	Memory leak at ccm_populate_feature_intf_list+34
CSCuy48491	cat6k-vs-infra	"SATVS reg_invoke Assertion Failed: " errors/TB's followed by a crash.
CSCuu43892	dhcp	switch crash on qpair_full after executing dhcpd_* functions
CSCum03685	dot1x-ios	memory leak symptoms in session manager accounting
CSCux43058	flexible-netflow	SUP2T NetFlow / DFC flow issues / timeout issues
CSCuz17235	ha-issu-infra	Crash with issu negotiation if any module is Up or Down
CSCuw48118	ip	ASR920 - crash in bcopy called from 'addnew' during reassembly
CSCuz28618	mcast-fib	sup2t: sup crashed after MFIB errors
CSCuu90695	mcast-rib	DM/SM boundary (S,G) are not repopulated: Multicast Missing Registration
CSCux87822	mpls-te	MPLS TE Missing label on midpoint when same Tunnel ID resignalled
CSCva62968	mcast-vpn	Z flag not set on *,G and S,G MDT data entry
CSCuu30091	mcast-vpn	MCP_DEV:Packet drops@Ipv4NoAdj with V6MVPN configs
CSCuv95757	nmsp	Conflict with port based features seen when nmsp enabled
CSCux46898	ntp	NTP associations vulnerability
CSCuy62478	sisf	device tracking causes duplicate address warning on Windows
CSCuy87667	ssh	Crash due to Block overrun by AAA banner

Caveats Resolved in Release 15.1(2)SY7

Identifier	Component	Description
CSCuu06523	pem	sup2t crash while doing capSidSessionInfoEntry SNMP polling
CSCun64833	cat6000-acl	Disable IPDT/ARP Snooping on RSL ports with any feature
CSCuv58471	cat6000-ltl	Upon FEX reload, Mcast trfc drops for few vlans due wrong VIF oper status
CSCus73299	cat6000-acl	Route-map Configured Inside Of NAT Packet Loss Is Seen On 6500 Sup2t
CSCuv47618	cat6000-routing	HSRP & GLBP VIP is unreachable after flapping its port-channel sub-intf
CSCuu18153	cat6000-routing	Enabling IPv6 to VRF Definition Breaks VRF to global fwding via GRE
CSCuw01019	cat6000-firmware	NVRAM_2_QUACK_failed on OIR
CSCuv48062	fex-infra	Some fex's stuck in OFFLINE state untill controller reload

Identifier	Component	Description
CSCuu64279	cat6000-acl	Cisco IOS NX-OS Malformed LISP Packet Denial of Service Vulnerability
CSCuo71816	cat6000-cts	Not able to configure cts manual when ASA-SM is enabled on Cat6K
CSCuw28153	cat6000-acl	153-1.IE101.149_20150915 build failed - Good Code Fix for CSCur37420
CSCuv50929	cat6000-ha	fex reload due to connected/registered timeout
CSCuw57403	cat6000-firmware	comp_c6kfw_mk1c MK1C_FBE_151006 BUILD FAILED
CSCus62254	cat6000-routing	Mk21 : Traceback while removing MVPN config under VRF
CSCuv50916	fex-infra	Online fex's went down due to "HA reconciliation"
CSCuw69698	cat6000-acl	cnmk1:-Back out CSCus73299 in MK1 throttle
CSCur96442	cat6000-firmware	C6800: High CPU due to "slcp process" when 10G ports have 10G SFPs
CSCuu86026	cat6000-env	Internal USB Bootdisk is not initialized during bootup
CSCts40588	eigrp	ip authentication cli in interface mode is removed when interface shuts
CSCuw95208	cat6000-ltl	Upon FEX reload,Mcast trfc drops for few vlans due wrong VIF oper status
CSCuv71068	parser	CNMK1:-Standby reboots continuosly due to "parser view "commands
CSCuv71155	cat6000-cm	DACL with L4 ops is overwritten
CSCut42645	crypto-engine	input queue wedged on a SSLVPN enabled router
CSCuu19667	cat6000-l2-ec	Crash observed on 6880 with error-EthChnl assert failure:
CSCul01067	ntp	Memory leak in NTP client with IPv6 configuration
CSCut40188	cat6000-qos	"trust device cisco-phone" is adding "trust none remark"
CSCuw73530	flexible-netflow	Active Sup resetting when exec "sh flow monitor <> cache filter count"
CSCuu01977	parser	To address parser side changes for CSCut34452
CSCuw94348	snmp	Crash seen after configuring snmpv3 user with encryption parameters
CSCuw62546	dhcp	ip dhcp snooping detect CLI not present in SY, SXJ2 onwards on S720
CSCuo55494	cat6000-eobc	Cat6k: SP sends a lot of SCP keepalive to line cards
CSCuv47733	cat6000-firmware	WS-X6904-40G Does not pass 1-2 byte of payload when Mac Sec is enabled
CSCuv89225	cat6000-env	Ha device hangs after enabling FIPS in MK1
CSCuv02292	cat6000-hw-fwding	RF-KPA/CPUHOG seen against spl groom for 200K+ ipv4/v6 entry insertion
CSCug10024	mem	XE3.10: CPU HOG with Cheak heaps process
CSCuu94695	cat6000-l2-infra	LACP:H-Port of an Port channel moves to I-state after switchover to sdby
CSCtk83641	rsvp	RSVP authentication over DMVPN Tunnel is not working
CSCux12931	cat6000-mpls	vpn_mapper_is_right_ios_hwid traceback on applying address-family ipv6
CSCux18010	cns-agents	Cisco Networking Services Sensitive Information Disclosure Vulnerability
CSCuv47600	cat6000-ltl	6880 VSS:broadcast packets punted to standby supervisor CPU in VSS
CSCux01283	cat6000-env	sup2T - supervisors do not save info to bootdata on watchdog crash
CSCut52427	cat6000-snmp	"snmp trap enable fru-cntl' on C6880-X sends POE alerts for user ports.
CSCuv11495	cat6000-netflow	FNF: platform runs out of big buffers and mallocfail
CSCuw85826	ntp	Evaluation of Cisco IOS and IOS-XEl for NTP_October_2015
CSCuw83303	cat6000-firmware	Max MTU packets dropped when directed to CPU and received on standby VSS

Identifier	Component	Description
CSCux45230	cat6000-env	CLI “sh platform fex-debug status”
CSCuq02273	cat6000-env	c68xx platform: GDB should not be available in release images
CSCua45548	sla	Router crashes with “sh ip sla summary” on longevity testing
CSCuw71689	cat6000-acl	Memory leak at FM core functions leads to crash
CSCux55558	cat6000-netflow	Netflow records are not exported to NFC sever as expected
CSCuw91443	cat6000-firmware	C6KFW:publish (mk1c)1.0.64 to MK1 throttle
CSCus55821	dhcp	DHCPv6 process crashes when receiving malformed packet
CSCux67510	cat6000-env	C4:--(6748,6704)-CFC Modules power down bcoz of Module failed SCP DWNLD
CSCuw61322	cat6000-env	After sso Insufficient power to start HP mode, standby sup into rommon
CSCux62857	cat6000-ha	6T: ICS-Standby doesn't reload, on reloading entire VSS after Z-SSO
CSCux40275	cat6000-ltl	OSPF neighborship flaps during Standby sup reload with vsl links shut
CSCux72974	cat6000-env	Sup-720 crashing continuously while loading with the image 15.1(2)SY6.22
CSCur60653	cat6000-firmware	CSCup92134 DDTS to track from the firmware side
CSCuu96336	cat6000-firmware	OIR of GLC-T flaps other 1G links on all Nappar family cards
CSCut42244	cat6000-ltl	cat6k UDLD triggers err-disable on reload
CSCuw18797	cat6000-firmware	T1: Traffic drop with GLCT negotiating to speed less than 1000Mb
CSCuv13264	flexible-netflow	sh flow mon<mon>cache aggregate rec<rec>shws incrct flow entrie aftr SSO
CSCuv31247	cat6000-l2-ec	Crash seen while unconfigure the FEX RSL PO
CSCuw38162	cat6000-l2-ec	Mk21a: RSL inter,once Channel-group <>mode on- "fex-fabric" not applied
CSCuu55971	cat6000-env	6500 - On SSO, ports after a 'power inline never' port go down
CSCux53457	cat6000-ltl	UDLD triggers err-disable on reload of standby/standby ICS sup
CSCut56029	ipc	Sup2T - supervisor is XDR disabled
CSCux83011	cat6000-firmware	Double commit conflict because of CSCuu96336 in mk1c fw throttle(mk1.7)
CSCux55287	ipc	Address issues related to invalid port-info when processing acks
CSCuv85472	eigrp	SR 635576687 6500 EIGRP VRF MD5 AUTHENTICATION ERROR AFTER RELOAD
CSCux48029	ipc	IPC debug enhancements
CSCux05676	cat6000-l2	Spurious Memory & Align errors at l2vlanifmib_find_entry_by_vlanid crash
CSCuu70641	elam	ELAM capture caused device to crash
CSCux89231	ipc	To address the BUILD failure in MK1.x WEEKLY for 151-2.SY6.30
CSCux84856	cat6000-firmware	C6KFW:publish (mk1c)1.0.69 to MK1 throttle
CSCux90929	ha-issu-matrix	MK1.7:ISSU CM Generation Request for the inclusion of 15.1(2)SY7 ver
CSCux38417	ikev2-toolkit	IKEv2 buffer overflow vulnerability
CSCup92134	cat6000-l2	Unable to configure Speed and duplex mode on the terminator interface
CSCux81271	cat6000-ltl	10G ports goes to udld err-disabled state after redundancy reload shelf
CSCun59619	wsma	netconf User logged in with Privilege level 1 can access config mode
CSCuy00397	cat6000-ltl	Build breakage in mk1.7 due to CSCux81271
CSCui33292	cat6000-env	Bundle latest porter tar file to sup2t for v151_2_sy_throttle

Identifier	Component	Description
CSCux69214	cat6000-hw-fwding	Distributed ether channel does not work with classic linecard
CSCur08470	cat6000-l2-infra	After changing a macro a Sup720 might reload/switchover
CSCuv53498	accsw-platform	“FRU Power Supply is not responding” seen on 2960XR/6800IA
CSCuv45410	accsw-ease-of-use	Cisco Smart Install denial of service vulnerability
CSCut96662	accsw-fex	6800IA incorrect VIF (vif 0 or incorrect vif number) on PO flapping
CSCuq24202	tcl-bleeding	Cisco IOS TCL script interpreter privilege escalation vulnerability
CSCum94811	tcp	TCP Packet Memory Leak Vulnerability
CSCux59183	accsw-fex	6800IA PO member frm active are not disconnected when active is reloaded

Caveats Resolved in Release 15.1(1)SY6

- CSCuu18788

  Symptom: An error similar to the following may be observed in the syslogs of a Cisco IOS device:

  *May 4 13:40:46.760: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error, -PC= :200CD000+1502CF4 -Traceback= 1#e06f72c62c6bef347348f23bdccc4b7f :200CD000+30D51C0 :200CD000+30D5588 :200CD000+3103724 :200CD000+6F2FD4C :200CD000+1502CF4 :200CD000+15033E0 :200CD000+446FF08 :200CD000+446E0B0 :200CD000+443DA40 :200CD000+442D158 :200CD000+445C0F8

  No functional impact is observed.

  Conditions: This is currently believed to affect all released versions of IOS code which support the CISCO-ENTITY-EXT-MIB. This may occur when polling the ceExtSysBootImageList object in CISCO-ENTITY-EXT-MIB. This object returns a semicolon-separated list of boot statements on the device, similar to the following:

  CISCO-ENTITY-EXT-MIB::ceExtSysBootImageList.5000 = STRING: "flash bootflash:cat4500e-universalk9.SPA.03.04.05.SG.151-2.SG5.bin;flash bootflash:cat4500e-universalk9.SPA.03.04.02.SG.151-2.SG2.bin"

  The DATACORRUPTION error will occur under a specific corner case, where the total length of one or more complete boot variables (counted starting after the 'boot system' token) is less than 255 bytes, BUT when semicolons are added (one per boot statement) meets or exceeds this number.

  Consider the following example:

  boot system bootflash:this_is_a_128_character_long_boot_statement_xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

  boot system bootflash:this_is_a_125_character_long_boot_statement_yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy

  128 + 125 + 2 semicolons = 255 characters (bytes)

  If another boot statement is added after this, the DATACORRUPTION error will be seen and the SNMP query will return invalid data.

  Workaround: Reduce the quantity/length of configured boot variables.

  Further Problem Description: This is not known to have any functional impact outside of the (potentially alarming) error message. The error will only be printed once, but subsequent occurrences of this condition can be seen via the 'show data-corruption' command.

- CSCur43251

  Symptom: The HTTPS client only offer till SSLv3.0 which is vulnerable to poodle attack.

  Conditions: Any Application is using HTTPS client with SSL3.0

  Workaround: Disable app which use HTTPS client.

  Further Problem Description: After fixing Poodle (CSCur23656) in the ssl component, this fix in the http component is required too. After the fix, TLS 1.0 will be used. After this fix HTTPS client will only offer TSL1.0.

- CSCut55517

  Symptom: 7200 router crash during multiple session validations.

  Conditions: When two certificate validations in progress, 7200 platform is crashing.

  Workaround: None.

  Further Problem Description: This defect more visible on 7200 platform than any other platform. This is not only limited to GetVPN configuration, but also with any configurations like IKEv2.

- CSCus77875

  Symptom: Router may become unresponsive. Memory is all used up and no longer available for other processes. Router may eventually reload on its own OR would need to be reloaded manually, to restore services.

  Conditions: Normal operations.

  Workaround: Track Used memory and when it approaches 70-80% utilization levels, please schedule a reload.

  Further Problem Description: Output of show process mem sorted will show signs of increase in Used. Memory held by processes Chunk Manager and CCSIP_TLS_SOCKET will show corresponding increase. show mem all totals will show increase for List Headers

- CSCus19794

  Symptom: A vulnerability in the IPv6 snooping feature from the first-hop security features in Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to cause an affected device to reload. The vulnerability is due to insufficient Control Plane Protection (CPPr) against specific IPv6 ND packets. An attacker could exploit this vulnerability by sending a flood of traffic consisting of specific IPv6 ND packets to an affected device where the IPv6 snooping feature is configured.

  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:

  http://tools.cisco.com/security/center/cvssCalculator.x?vector=AV:N/AC:L/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C&version=2.0

  CVE ID CVE-2015-6278 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

- CSCuo04400

  Symptom: A vulnerability in the IPv6 snooping feature from the first-hop security features in Cisco IOS and IOS XE Software could allow an

unauthenticated, remote attacker to cause an affected device to reload. The vulnerability is due to insufficient validation of IPv6 ND packets that use the Cryptographically Generated Address (CGA) option. An attacker could exploit this vulnerability by sending a malformed packet to an affected device where the IPv6 Snooping feature is enabled. Cisco has released 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-20150923-fhs

Note The September 23, 2015, release of the Cisco IOS and IOS XE Software Security Advisory bundled publication includes three Cisco Security Advisories. All the advisories address vulnerabilities in Cisco IOS Software and Cisco IOS XE Software. Individual publication links are in Cisco

Event Response: September 2015 Semiannual Cisco IOS and IOS XE Software Security Advisory Bundled Publication at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep15.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:

http://tools.cisco.com/security/center/cvssCalculator.x?vector=AV:N/AC:L/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C&version=2.0

CVE ID CVE-2015-6279 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

- CSCuu82607

Symptom: This product includes a version of OpenSSL that is affected by the vulnerability identified by the Common Vulnerability and Exposures (CVE) IDs:

CVE-2015-4000, CVE-2015-1788, CVE-2015-1789, CVE-2015-1790, CVE-2015-1792, CVE-2015-1791, CVE-2014-8176

This bug has been opened to address the potential impact on this product.

Conditions: Following Cisco IOS features may invoke the affected code and might be vulnerable

- SSLVPN feature (for any platform running IOS) ("webvpn gateway")

- SSLVPN feature (for CSR1000V running IOS-XE) ("crypto ssl profile")

- HTTPS client feature ("copy https://... ...", DynDNS client, ...)

- Voice-XML HTTPS client feature

- HTTPS server feature ("ip http secure-server")

- CNS feature

- Settlement for Packet Telephony feature

- LDAPv3 client feature

- CMTS billing feature

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

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

- CSCuq74492

  Symptom: Cisco IOS and IOS-XE include a version of OpenSSL that may be affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

  CVE-2014-3505 - Double Free when processing DTLS packets

  CVE-2014-3506 - DTLS memory exhaustion

  CVE-2014-3507 - DTLS memory leak from zero-length fragments

  CVE-2014-3508 - Information leak in pretty printing functions

  CVE-2014-3509 - Race condition in ssl_parse_serverhello_tlsext

  CVE-2014-3510 - OpenSSL DTLS anonymous EC(DH) denial of service

  CVE-2014-3511 - OpenSSL TLS protocol downgrade attack

  CVE-2014-3512 - SRP buffer overrun

  CVE-2014-5139 - Crash with SRP ciphersuite in Server Hello message

  This bug has been opened to address the potential impact on this product.

  Conditions: See published Cisco Security Advisory

  Workaround: None.

  Further Problem Description: At this point the investigation is ongoing, this bug will be updated in the future to reflect better the real impact on the product.

  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/cvss?target=new&version=2.0&vector=AV:N/AC:L/Au:N/C:N/I:N/A:C/E:F/RL:OF/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

- CSCus61884

  Symptom: This product includes a version of OpenSSL that is affected by the vulnerability identified by the Common Vulnerability and Exposures (CVE) IDs:

CVE-2014-3569, CVE-2014-3570, CVE-2014-3571, CVE-2014-3572, CVE-2014-8275, CVE-2015-0204, CVE-2015-0205, CVE-2015-0206

This bug has been opened to address the potential impact on this product.

Conditions: The following Cisco IOS features may invoke the affected code and may be vulnerable:

- SSLVPN feature (for any platform running IOS) ("webvpn gateway")

- SSLVPN feature (for CSR1000V running IOS-XE) ("crypto ssl profile")

- HTTPS client feature ("copy https://... ...", DynDNS client, ...)

- Voice-XML HTTPS client feature

- HTTPS server feature ("ip http secure-server")

- CNS feature

- Settlement for Packet Telephony feature

- LDAPv3 client feature

- CMTS billing feature

Affected Versions: 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.

Further Problem Description: 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: 5.0/3.7

http://tools.cisco.com/security/center/cvssCalculator.x?version=2.0&vector=AV:N/AC:L/Au:N/C:N/I:N/A:P/E:U/RL:OF/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

- CSCut46130

Symptom: This product includes a version of OpenSSL that is affected by the vulnerability identified by the Common Vulnerability and Exposures (CVE) IDs:

CVE-2015-0286, CVE-2015-0287, CVE-2015-0289, CVE-2015-0292, CVE-2015-0293, CVE-2015-0209, CVE-2015-0288

This bug has been opened to address the potential impact on Cisco IOS and IOS-XE products.

Conditions: LIST SPECIFIC VULNERABLE CONFIGURATION INFORMATION. IF DEFAULT CONFIGURATION IS VULNERABLE, USE THE TEXT "Exposure is not configuration dependent."

Following Cisco IOS features may invoke the affected code and might be vulnerable:

- SSLVPN feature (for any platform running IOS) ("webvpn gateway")

- SSLVPN feature (for CSR1000V running IOS-XE) ("crypto ssl profile")

- HTTPS client feature ("copy https://... ...", DynDNS client, ...)

- Voice-XML HTTPS client feature

- HTTPS server feature ("ip http secure-server")

- CNS feature

- Settlement for Packet Telephony feature

- LDAPv3 client feature

- CMTS billing feature

Workaround: None.

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: 7.1/6.9

https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:H/Au:N/C:P/I:N/A:N/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

- CSCuq24202

  Symptom: A vulnerability in the TCL script interpreter of Cisco IOS Software could allow an authenticated, local attacker to escalate its privileges from those of a non-privileged user to a privileged (level 15) user. This would allow a non-privileged user to execute privileged commands

  (those under privilege level 15). The vulnerability is due to an error on resetting VTY privileges after running a TCL script. An attacker could exploit this vulnerability by establishing a session to an affected device immediately after a TCL script has been run. An attacker would need to provide valid credentials and successfully pass authentication to the device.

  Conditions: This behavior is timing dependent, as the attacker would need to log-in to the device immediately after the TCL script finishes execution.

  Workaround: None.

  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 6.6/5.5:

  http://tools.cisco.com/security/center/cvssCalculator.x?vector=AV:L/AC:M/Au:S/C:C/I:C/A:C/E:F/RL:OF/RC:C&version=2.

  CVE ID CVE-2015-4185 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

- CSCum94811

  A vulnerability in the TCP input module of Cisco IOS and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a memory leak and

  eventual reload of the affected device. The vulnerability is due to improper handling of certain crafted packet sequences used in establishing a TCP three-way handshake. An attacker could exploit this vulnerability by sending a crafted sequence of TCP packets while establishing a thee-way handshake. A successful exploit could allow the attacker to cause a memory leak and eventual reload of the affected device.

  There are no workarounds for this vulnerability.

  Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150325-tcpleak

Note The March 25, 2015, Cisco IOS Software Security Advisory bundled publication includes seven Cisco Security Advisories. The advisories address vulnerabilities in Cisco IOS Software and Cisco IOS XE Software. 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_mar15.html

- CSCur70505

  Symptom: A 6500 reloads after negotiating an IPSec tunnel with ASR9000.

  Conditions: The 6500 needs to run 12.2(33)SXJ8 and the IPsec engine must be a WS-SSC-600 WS-IPSEC-3 combination.This crash does not happen with 7600-SSC-400 IPSEC-2 combination.

  Workaround: None.

  Further Problem Description: A vulnerability in the IKE subsystem of Cisco WS-IPSEC-3 service module could allow an authenticated, remote attacker to cause a reload of the Catalyst switch. The vulnerability is due to insufficient bounds checks on a specific message during the establishment of an IPSEC tunnel. An attacker could exploit this vulnerability by successfully establishing an IKE session and sending the offending packet during subsequent negotiations. An exploit could allow the attacker to cause a denial of service by forcibly reloading the switch.

  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 4.9/4.9:

  http://tools.cisco.com/security/center/cvssCalculator.x?vector=AV:N/AC:H/Au:S/C:N/I:N/A:C/E:H/RL:U/RC:C&version=2.0

  CVE ID CVE-2015-0771 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

Identifier	Component	Description
CSCuv30872	cat6000-l2	double commit CSCuo11314 and CSCuo54095 to ma2 throttle

Caveats Resolved in Release 15.1(2)SY6

Identifier	Component	Description
CSCut29617	accsw-fex	6800IA/FEX stop forwarding multicast traffic
CSCus96216	accsw-fex	BPDU exchange over mGig port isn't proper
CSCut84834	accsw-fex	6880IA System LED lit Amber
CSCuq64670	accsw-fex	6800ia is sending SCP message with src_vslot as "0" upon exceeding VSLOT
CSCuu18020	accsw-fex	Timestamp for Syslog & Debug msgs are different b/n 6k & IA stack member
CSCur01780	accsw-platform	Cat6500 FlowControl oper is changed to on with sh/no sh interface
CSCuv66869	accsw-platform	Porter/KF : To change the offset value of the I2C mux.

Identifier	Component	Description
CSCut53599	accsw-platform	C2960X RPS is not functioning correctly, reports "RPS is not responding"
CSCuu18788	accsw-platform	DATACORRUPTION-1-DATAINCONSISTENCY when pollingceExtSysBootImageList
CSCuu30115	accsw-qos	On Congestion, PQ doesn't work on 6800 IA if pkt size > 700 Bytes
CSCun63514	ap-unknown	TCP CIP Denial of Service Vulnerability
CSCui33974	cat6000-acl	High cpu due to looping packet in Sup2t
CSCut18304	cat6000-env	Blue Beacon glows after the renumbered IA module of SA IA comes online
CSCur25406	cat6000-env	t1mk2: SCP dnld failed for cannor card
CSCuv44524	cat6000-env	QuadSupVSS:poe device flap causes ICC messages stuck and memory leak
CSCuv36076	cat6000-env	Cisco PoE phone put into wrong power class 15.1(2)SY5
CSCuv41327	cat6000-env	power supply is not correctly recognized
CSCui33292	cat6000-env	Bundle latest porter tar file to sup2t for v151_2_sy_throttle
CSCuv13982	cat6000-eobc	crash @ eobc_send
CSCut81739	cat6000-firmware	EC ports are stuck in suspended state after sso
CSCut40421	cat6000-firmware	Padding is not working for less than 64 bytes packets
CSCuq06215	cat6000-firmware	Storm-control doesn't work when 1Gig/100Mbps Transceivers on 10Gig ports
CSCuv37553	cat6000-firmware	Backout the changes of CSCut81739
CSCuv89092	cat6000-firmware	Cat6800: High CPU usage due to "slcp process" when GLC-T plugged in
CSCui91874	cat6000-hw-fwding	CPU HOG seen against spl groom for ipv4 & v6 entry insertion.
CSCus85586	cat6000-hw-fwding	Cat6880: VSS standby stuck in progress to cold-config due to snmp trap
CSCur96850	cat6000-l2-ec	LACP 1-1 port-channel instabilities
CSCuu66933	cat6000-netflow	Netflow didn't send data after reconfigure "ip flow ingress"
CSCuo76165	cat6000-qos	WS-X6816-10GE drops large size packets
CSCuq35524	cat6000-qos	Wrong port-level shaping percent under show platform software port-data
CSCus60364	cat6000-qos	Priority queue threshold programming on controller and FEX is different
CSCus18036	cat6000-snmp	c6500 IOS switches sending Module failure for module minor temp alarms
CSCug38910	cat6000-vntag	c4mk1:fex:Mem leak@vnmgr_ha_set_ucast_port_feature+AC on porter reload
CSCuu54241	cat6000-vntag	6880 crashes after a connected FEX reloads
CSCus94468	cat6k-vs-infra	Inconsistent VSL MTU values in "show interface" & "show interface mtu"
CSCuq42833	cts	Configuring " cts role-based monitor permissions " will lead to mem leak
CSCuu32493	cts	Removing possible stack corruption in Keystore Crypto
CSCur61500	cts	Cat6k MPLS VPN label not pushed for L3 unnumbered interfaces
CSCus15976	cts	%CTS-AUTHZ_ENTRY_RADIUS_FAILED should be an info and can be disabled
CSCuu24318	cts	ipv6 Packet loss with SUP2t
CSCur77994	dhcp	Cat6k:DHCPv6 relay from vrf to non-vrf
CSCub30751	dns	SIP DNS SRV Calls fails even though the DNS lookup is a Success
CSCuu12582	fex-infra	Fex goes to "registered" state on ISSU abortversion b/w MK1.4a to MK1.5
CSCus77027	flexible-netflow	linecard crashes continuously when losing connectivity to Netflow collector

Identifier	Component	Description
CSCuq52496	flexible-netflow	FNF: platform runs out of big buffers
CSCut96870	flexible-netflow	"show flow monitor <profile> cache aggregate record <name>" crashes Sup
CSCuu21449	ip-acl	IPv6 traffic classified incorrectly in software
CSCts95370	ip-acl	In ACL applied to vty wrongly filters out ssh session
CSCuv18809	ipc	Unexpected reload seen @ipc_rcv_unaccount
CSCuo67770	ipv6	Race condition in IPv6 Neighbor Discovery
CSCug75942	medianet-metadata	Cisco IOS Metadata Vulnerability
CSCut24690	mpls-te	Cat6k MPLS TE high CPU when polling SNMP mplsTunnelEntry OID
CSCub94626	ntp	Memory leak at ntp_global_config_cmd
CSCut77619	ntp	APRIL 2015 NTPd Vulnerabilities
CSCus75471	parser	MALLOCFAIL on "Shell Pipeline Process" When Issuing "Show log | tail -x"
CSCum65703	parser	Inconsistency on config "privilege" commands as seen in running-config
CSCus23013	parser	show cmd under "parser view" cause standby router to reload
CSCut36817	pem	Redirect fails incase supp sends req using multiplemac andnot all hv ip
CSCum93491	pki	SSTE: CSCum37923 still exisits after the commit to xe312 throttle
CSCus77875	pki	List Headers leak verified cert chain Held CCSIP_TLS_SOCKET & Chunk Mgr
CSCut55517	pki	Memory corruption due to crypto pki
CSCtc09913	rfs	VTY Process/Telnet connection stuck
CSCui11547	rsvp	Cisco IOS RSVP Vulnerability
CSCus25125	snmp	ICS-Standby reloads on SSO bcoz of RF timer expiry for SNMP Client
CSCtn75051	snmp	%SYS-3-TIMERNEG: Cannot start timer with negative offset
CSCsr39272	spa-infra	%DATACORRUPTION-1 due to spa sensor temp overruning buffer
CSCuq74492	ssl	IOS/IOSd Multiple Vulnerabilities in OpenSSL - August 2014
CSCus61884	ssl	JANUARY 2015 OpenSSL Vulnerabilities
CSCut46130	ssl	MARCH 2015 OpenSSL Vulnerabilities
CSCuu82607	ssl	Evaluation of all for OpenSSL June 2015
CSCuq24202	tcl-bleeding	Cisco IOS TCL script interpreter privilege escalation vulnerability
CSCum94811	tcp	TCP Packet Memory Leak Vulnerability

Caveats Resolved in Release 15.1(2)SY5

Identifier	Component	Description
CSCue86180	aaa	sl_def_acl is added by default
CSCur89529	aaa	Class attributes missing in Auth-proxy accounting
CSCus09480	aaa	sessions are stuck in IDLE state when AAA server not comeup after reboot
CSCum81043	aaa	Member crashed when power off master
CSCuq98067	accsw-ease-of-use	6880 as a director needs to support 3650 as a client

Identifier	Component	Description
CSCus42147	accsw-fex	FEX Switch number update
CSCus36409	accsw-fex	Storm-control config not removed on 6848ia local port-channel
CSCuq14827	accsw-fex	"no logging event link-status" command not working for FEX ports
CSCus96063	accsw-fex	2k-side change: Per vlan timer, and deferred vlan delete timeout 60 sec
CSCui44899	accsw-fex	Timestamp for the Syslog & Debug msgs are different b/n 6k & 2k
CSCus08830	accsw-fex	6800IA SWIDB gets depleted when FEX stack member reloads
CSCus96041	accsw-fex	2K Changes for SCP_POWER_DEVICE_MSG_VER2(v2) - related to CSCus72404
CSCus90328	accsw-fex	Need PoE+ capability to pwr up Televic PD with IA (IA side changes)
CSCup27045	accsw-platform	Tracebacks are continuously reported, switches inaccessible.
CSCul80136	accsw-platform	Link flap in the REP segment with edge no-neighbor configured.
CSCus94888	accsw-platform	To increase i2c bus tBuf time and polling time of i2c bus 0
CSCur94280	accsw-platform	2960x/6800IA: Link may go down randomly with GLC-T in uplink ports
CSCun51532	accsw-platform	Sometimes C8945 with port synchronisation lose SW link on PC link
CSCur05027	accsw-platform	Loopback error occurs when keepalive packet is looped back to the port.
CSCun84283	accsw-platform	C2960 || Copper connection interfaces || Keepalive set by default
CSCur56395	accsw-platform	2960X: Link may go down randomly with GLC-T in uplinks
CSCum02538	accsw-platform	Version id & Product id blank in "sh int tran fex" o/p for SFP-10-LRM
CSCul78520	accsw-platform	%ENTROPY-0-ENTROPY_ERROR output with link flap
CSCur54770	accsw-qos	FEX/KFEX Needs Custom QoS Policy to pass DoD APL Cert
CSCuq52009	accsw-qos	FEX reload upon SSO due to (reason: ICC channel is not UP)
CSCup52988	bgp	InterAS OptionB ASBR does not allocate label for VPNv4 prefix
CSCuo62332	bgp	CISCO-BGP-MIBv8.1 - Add support for cbgpPeer2Type in BGP traps/notif
CSCug08566	bgp	BGP does not advertize a global static route pointing to a vrf intf
CSCuq41287	bgp	BGP next-hop-unchanged cannot be configured on iBGP peer-groups
CSCuo40657	bgp	'next-hop-unchanged' is not applied to some of the peers in peer-group
CSCuq49217	bgp	Stale BGP leaked routes in destination VRF with soft-reconfig in config
CSCuq35209	bgp	BGP advertising incorrect Link Local ipv6 address
CSCuq63158	bgp	Match tag not supported in policy-list
CSCuq83441	bgp	BGP L2VPN uses default static next-hop instead of outging intf-addr
CSCup34904	bgp	BGP vpnv4 incorrect import behavior with atomic-aggregate
CSCur14401	bgp	Inter-AS VPLS Option-C /next-hop-unchanged not supported on RRs
CSCuq99797	bgp	BGP Route-Target not advertised when rtfilter address family in use
CSCur11534	bgp	Inter-AS opt B PE/ASBR does not allocate an MP-BGP label to ibgp peer
CSCur66140	bgp	Import of Global routes to VRF will fail
CSCun68322	bgp	Support BGP GR for VPN AF in platform without MPLS
CSCuo62332	bgp	CISCO-BGP-MIBv8.1 - Add support for cbgpPeer2Type in BGP traps/notif
CSCur88745	cat6000-acl	Match ipv6 Routing header in hardware

Identifier	Component	Description
CSCuq62568	cat6000-acl	ACL applied using "copy tftp: run" is not being programed in hardware
CSCus70080	cat6000-acl	crash due to invalid memory access
CSCur73025	cat6000-acl	ARP with Multicast dmac is looped within the switch causing high cpu
CSCus51750	cat6000-acl	wccp_ipv6 and wccp_ipv6_fib missing from s2t54-ipservicesk9
CSCuq66142	cat6000-dot1x	Provide a mechanism to protect mac-addresses from being secured
CSCup88060	cat6000-env	x86 crashed with empty show context
CSCuq56417	cat6000-env	standby switch- VSS falls to rommon backplane Hardware Rev is => 1.3
CSCus68580	cat6000-env	Cat6500 should power up mod in standby sup slot when enough power avlb
CSCuq64403	cat6000-env	I/O Mem crash due to SCP queue build-up by flaps seen on FEX host ports
CSCut99813	cat6000-env	Crash seen after CPUHOG due to insertion & withdrawl of ipv4 & v6 routes
CSCun06843	cat6000-env	6807: After SSO, power mode changes from Combined to Redundancy
CSCun71233	cat6000-firmware	SFPs not properly seen in outputs of "show inventory"
CSCuq04062	cat6000-firmware	1Gig port- 64 byte Padding some ports pass 60 byte
CSCuo34488	cat6000-ha	Sup720/Sup2T insertion may crash & reload existing quad sup VSS chassis
CSCun79149	cat6000-hw-fwding	sup2t running config does not show mac sync learning change
CSCun23845	cat6000-hw-fwding	snmpwalk timeout for sup2T in VSS mode when polling BRIDGE-MIB
CSCur65434	cat6000-hw-fwding	L3 IF was affected when shutdown another L3 IF in different segment
CSCut83493	cat6000-hw-fwding	6880X Unexpected reset due to CPU_MONITOR-2-NOT_RUNNING
CSCue35720	cat6000-ipv6	Sup2T crash with FNF export of IPv6 flow with wrong hw adjacency
CSCuq78959	cat6000-l2	"ISL" trunking encapsulation causing layer 2 loop in 151-2.SY3
CSCum69766	cat6000-l2-ec	[TFEX] Long Traffic Convergence Time during Active/Stdby Sync
CSCup80886	cat6000-l2-ec	ASA Cluster members evicted at VSS SSO Switchover
CSCur17071	cat6000-l2-ec	C6880-X-LE: EC cannot bundle when sh/no sh interface on peer device
CSCum69766	cat6000-l2-ec	[TFEX] Long Traffic Convergence Time during Active/Stdby Sync
CSCup80886	cat6000-l2-ec	ASA Cluster members evicted at VSS SSO Switchover
CSCur10233	cat6000-l2-infra	6500 - FEX internal SVI stuck in an up/down state + FIN IP being nvgen'd
CSCuq04573	cat6000-l2-infra	6500 SUP2T crash during boot phase-SVIs on the Internal MET are present
CSCuo26327	cat6000-l2-infra	802.1x EAP-TLS not working on FEX host ports
CSCuq00430	cat6000-l2-infra	Flow control issue with port-channel across Ringer and Estelle cards
CSCur04896	cat6000-l2-infra	Sup2T unexpected reboot after FWSM went down
CSCuo26327	cat6000-l2-infra	802.1x EAP-TLS not working on FEX host ports
CSCur89036	cat6000-mcast	High memory utilization due to mls-mld process
CSCus12745	cat6000-mpls	Sup2T: When xconnect goes down traffic sent to CPU causing high CPU
CSCus50539	cat6000-mpls	cat6k:mpls adj programming at LC issue
CSCur04989	cat6000-netflow	Rate Limit Netflow TCAM ECC error logs in CSCug86296
CSCuq06095	cat6000-netflow	Fatal interrupt NF_SE_CMD_ERR
CSCur22975	cat6000-netflow	Switch crash in fnf_mon_process_flow

Identifier	Component	Description
CSCus64795	cat6000-netflow	Excessive logging/Memory leak due to a parity error in the Netflow VRAM.
CSCuq44349	cat6000-portsecur	Traffic from 6800IA may hit 0x7FA9 & get dropped on VSS
CSCup75818	cat6000-qos	Long Named ClassMap defined under PolicyMap reloads active & crash seen
CSCur55929	cat6000-qos	FEX: QoS Certification requirements
CSCuq83129	cat6000-routing	Ignored ip redrects command on tunnel interface
CSCur54239	cat6000-routing	EARL8 - HSRP VIP unreachable after HSRP swichover
CSCuq83129	cat6000-routing	Ignored ip redrects command on tunnel interface
CSCuq58281	cat6000-snmp	Need OID in CISCO-VIRTUAL-SWITCH-MIB giving Peer Interface of VSL link
CSCus56026	cat6000-sw-fwding	Locally generated LDP packets are not queued correctly
CSCun22589	cat6000-vntag	Quadsupfex: Active crashes on resetting Estelle on active&standby
CSCut44097	cat6000-vntag	to address CSCut09976 via retry mechanism
CSCur64061	cat6k-vs-infra	Sup2T/VSS/FEX: I/O memory depletion on standby with SCP opcode 0x32B
CSCur66067	cat6k-vs-infra	6880X Active VSS switch shows "UNKNOWN" RRP state for the peer.
CSCus93563	cat6k-vs-infra	FEX host po-ch stops fwding traffic a/f SSO and then an RSL reset
CSCus76144	cat6k-vs-infra	MK1.5 Proposal for zero-touch replacement of Fex stack member
CSCuq36627	crypto-engine	WAAS Express:Failed to create SSL session. (no available resources)
CSCum90081	dhcp	Cisco IOS Software DHCPv6 Denial Of Service Vulnerability
CSCul70788	eigrp	Router crashes when calculating the best cost successor in EIGRP DUAL
CSCuf60880	ha-issu-infra	IPC error message and traceback on VSS standby when Remote ICS is down
CSCuo84660	ifs	copy command yields DATACORRPUTION error
CSCtw74339	ipc	IPC errors (RPC timeouts) were observed while polling cempMemPoolEntry.
CSCtx78552	ipc	"CR10K API Stat" causing leak in middle buffer on 5x20 LC
CSCum36951	ipsec-ikev2	Cisco IOS Software IKEv2 Denial of Service Vulnerabilities
CSCuq26103	isis	ISIS adj state trap OID value mismatch with Show snmp mib ifmib ifindex
CSCuq40996	isis	None-Cisco ISIS LSP is purged after FO if auth and NSF Cisco are used
CSCuq49073	isis	LDP breaks after defaulting an interface
CSCua01375	ldap	ldap VRF is not working with PKI
CSCus91917	mcast-pim	Auto-RP config is removed from running config when address is configured
CSCup57287	mpls-mfi	SNMP walk for packets statistics stops at MPLS interface
CSCul29557	ntp	NTP : Repeatedly losing sync with the master on 3900e routers
CSCuo29389	ntp	NTP clients of 3900 loses sync sporadically,due to high offsetvariations
CSCuj55389	ntp	ntp config removed from "sh run" when ntp broadcast done in multiple int
CSCup81878	ntp	standby reload - Line by Line Sync fail while deleting dynamic NTP peer
CSCul29557	ntp	NTP : Repeatedly losing sync with the master on 3900e routers
CSCuo29389	ntp	NTP clients of 3900 loses sync sporadically,due to high offsetvariations
CSCur57476	os-logging	EEM 4.00 syslogs generated only when logging level debug configured
CSCuq58555	ospf	OSPFv3: create unintended vrf RIB w/o cap vrf-lite after sh/no sh area0

Identifier	Component	Description
CSCur33350	ospf	me3600 OSPF Prefix-suppression not working after reload
CSCur35114	ospf	0.0.0.0/1 is not redistributed into OSPF
CSCuo75572	pki	Cisco IOS Software IKEv2 Denial of Service Vulnerabilities
CSCsc46018	rsvp	Call using RSVP agent with loopback configured with RSVP crashes router
CSCtw74132	snmp	SNMP v3 information leaking vulnerability
CSCus57661	ssh	6500 | SSH - Banner Diplays "$(hostname).$(domain)"
CSCur23656	ssl	Cisco IOS and IOSd in IOS-XE : evaluation of SSLv3 POODLE vulnerability
CSCul10482	tftp	TFEX: Image auto download fails due to "ip tftp source-interface" config
CSCur70505	ws-ipsec-3	Crash with IPsec Tunnel between 6500 w IPSEC-3 and ASR9000

Caveats Resolved in Release 15.1(1)SY5

Identifier	Component	Description
CSCum17260	accsw-ease-of-use	DATACORRUPTION-1-DATAINCONSISTENCY on vstack mgmt vlan bringup on nbr sw
CSCuo02666	cat6000-cm	EARL8 improve FM/CM label allocation logic
CSCuo34488	cat6000-ha	Sup720/Sup2T insertion may crash & reload existing quad sup VSS chassis
CSCur76459	cat6000-ha	mk2 FC1-Traceback & packet loss seen after load version - ipbasek9
CSCur04989	cat6000-netflow	Rate Limit Netflow TCAM ECC error logs in CSCug86296
CSCus48378	cns-agents	IOS : CNS feature needs to support TLS
CSCtz31420	eigrp	EIGRP Metric Calc: Unknown Delay is added
CSCul70788	eigrp	Router crashes when calculating the best cost successor in EIGRP DUAL
CSCtu56112	eigrp	EIGRP v6 crashes in MVPN Scale Environment
CSCul66738	eigrp	EIGRP routes stuck in Active Never State or stuck with U/R flag
CSCuj83458	eigrp	VNET: Route stays in topology table even after no redistribution
CSCty30694	eigrp	"show ip traffic" EIGRP sent: stat not working
CSCtq50411	eigrp'	remote' keyword not working when used with SAFv6
CSCtq46747	eigrp	EIGRP-WM:Inconsistent total delay shown in "show eigrp add ipv6 topo"ih
CSCus72738	ha-issu-matrix	ISSU Generation Request for ma2.5
CSCtw74339	ipc	IPC errors (RPC timeouts) were observed while polling cempMemPoolEntry.
CSCtx78552	ipc	"CR10K API Stat" causing leak in middle buffer on 5x20 LC
CSCtz48366	ipsec-core	Standby config is getting marked dirty during boot due to ctid/crypto
CSCum36951	ipsec-ikev2	ASR1K:RP crash @__be_ikev2_parser while running IKEv2 codenomicon suite.
CSCus48386	ldapI	IOS : LDAPv3 client : Support TLS
CSCur57476	os-logging	EEM 4.00 syslogs generated only when logging level debug configured
CSCug55683	pki	PKI trustpool certificate chain-validation fails
CSCuj37366	pki	MCP: memory leak@Stby Cnfg Parse

Identifier	Component	Description
CSCuq33617	pki	IOS RA Serever crashes in NDES and SUbCA setup
CSCur23656	ssl	Cisco IOS and IOSd in IOS-XE : evaluation of SSLv3 POODLE vulnerability

Caveats Resolved in Release 15.1(2)SY4a

Identifier	Component	Description
CSCus22014	cat6000-ssh	Console hung while generating crypto key

Caveats Resolved in Release 15.1(2)SY4

Identifier	Component	Description
CSCup99867	cat6000-env	6880 VSL link Timeout
CSCun17857	cat6000-l2-infra	Standby switch joins VSS in RPR mode after switchover
CSCun11109	cat6000-mpls	Xconnect MTU configuration is not available on C6880 or SUP2T platforms
CSCuo36172	cat6000-sw-fwding	Extra padding added for Sup2T and PVST BPDUs
CSCuj32321	flexible_netflow	Standby reload due to parse error
CSCum28609	ip	SUP2T failed to send broadcast ping packet
CSCuh49066	parser	Standby crashes due to LBL sync on "parser view li-view"

Caveats Resolved in Release 15.1(1)SY4

Identifier	Component	Description
CSCuj11720	bgp	PE does next-hop-self while sending eBGP route to iBGP vrf-lite CE
CSCuh43027	bgp	BGP route does not disappear from the RIB
CSCue68714	bgp	OVLD: BFD BGP Client Incompatibility between IOS t-train and IOSXE
CSCun68006	cat6000-ipc	15.1(1)SY1 : Quad-SUP VSS(Sup2T) : Crash During Switchover
CSCui27401	cat6000-qos	cat6000-qos Traceback and crash after linecard failure
CSCuj31321	cat6000-qos	Sup2T: Notification timer expired for RF Client: Cat6k QoS Manager
CSCuh70828	cat6000-snmp	SNMP okButDiagFailed Traps received when module status is 'ok'
CSCuj96561	cat6000-svc	wism redundancy-vlan and wism service-vlan must reject vlans in trunk
CSCua73834	pki	Incorrect rollover cert issued to clients enrolling to IOS CA via IOS RA
CSCui37358	pki	PKI: peer cert validated with different trustpoint than passed by IKE
CSCul08799	sisf	IPDT: nmsp prevents converting the port from access to trunk
CSCty92208	wccp	Ingress wccp + cts sgacl monitor + reboot results in CPU exception

Caveats Resolved in Release 15.1(2)SY3

Resolved ipv6 Caveats

- CSCui59540—Resolved in 15.1(2)SY3

  Symptom: A vulnerability in the implementation of the IP version 6 (IPv6) protocol stack in Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause I/O memory depletion on an affected device that has IPv6 enabled. The vulnerability is triggered when an affected device processes a malformed IPv6 packet.

  Cisco has released free software updates that address this vulnerability. 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-ipv6

  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

  Further Problem Description: 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-2014-2113 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

Other Resolved Caveats in Release 15.1(2)SY3

Identifier	Component	Description
CSCuc32663	aaa	IOS should not send passwords and sensitive information to ACS logs
CSCud55435	aaa	Optimization of Access-Request (Radius) path
CSCue43907	aaa	ip radius source-interface not PRC compliant
CSCtz07902	bfd	Standby RP repeated crash pointing to ipv6_bfd
CSCuc60868	bgp	Router Crash on uncfg & reconfig of VPLS BGP Signaling - Script Run
CSCuj11720	bgp	PE does next-hop-self while sending eBGP route to iBGP vrf-lite CE
CSCul96778	bgp	Router crash at bgp_topo_valid_tid
CSCum14830	bgp	IPv6/After route leak from vrf to global using BGP, next hop shows null0
CSCum58261	bgp	BGP additional paths disable config per neighbor not saved in NVgen

Identifier	Component	Description
CSCum85041	bgp	BGP Aggregate route with IPv6 VRF does not remove
CSCum98099	bgp	BGP IPv4 MDT routes are lost after reload
CSCun11782	bgp	RTfilter prefixes sent with next-hop of default static route in GRT
CSCun39038	bgp	Selective route download for ipv6 blocking all routes post reload
CSCuo02832	bgp	ASR 1001 SNMP BGP peer polling, malformed IP information
CSCug11351	c7600-system	ISIS Flap on RSP Switchover
CSCum02094	call-home	call-home would crash sending a DS message if the DS didn't contain SR
CSCun51501	cat6000-acl	Crash on active supervisor when standby is reloading
CSCuo45250	cat6000-acl	Quad SUP2T VSS: Standby supervisors appear to have memory leak
CSCug29433	cat6000-diag	6k Enh: Add "reset count" config knob for GOLD to power-down LC
CSCuo24560	cat6000-diag	I/O memory leak with active SUP due to issues with standby SUP
CSCum39766	cat6000-diag	Estelle: Add support for SFP-10G-ZR from IOS side
CSCul69259	cat6000-env	ISSU VS Power Client errors seen while ISSU from 15.1(2)SY to 15.1(2)SY1
CSCum60489	cat6000-env	System LED shows amber when power supplies are restored on sup2t VSS
CSCum82569	cat6000-env	t1mk1c: PIM neighbor with query interval 500ms flaps every 1hour
CSCun06843	cat6000-env	6807: After SSO, power mode changes from Combined to Redundancy
CSCun72660	cat6000-env	Standalone to VSS quad sup2t from mk1c to mk2 image estelle goes down
CSCuo42865	cat6000-env	Implementing ICC msg for CLI sh power fex id status ps/fan for KF
CSCuo45815	cat6000-env	Implementing console disable/enable option for fex through Socket
CSCuo99860	cat6000-env	Backout MALFRA upgrade from CSCuo53369
CSCuo53369	cat6000-env	FPGA changes required for Gigatron/G1 ASIC due to CSCun78994
CSCuj48794	cat6000-firmware	Sup2T may give false EARL temp readings
CSCul18679	cat6000-firmware	ASASM may reload on removing Active Sup
CSCun65772	cat6000-firmware	Cat6500 VSS crash due to watchdog timeout, process = slcp process
CSCuo52995	cat6000-firmware	Enable packet padding on Gigatron/G1 for 1G
CSCuh57728	cat6000-ha	Bootvar retains "version1" image after successful issu upgradation
CSCuo25812	cat6000-hw-fwding	Adjacency not updated when cause for recirculation is removed
CSCuj57692	cat6000-ipc	In scale setup, on SSO 6800 IA client may reload sometimes
CSCun62742	cat6000-l2-ec	Changing the FEX Host PO load balance method doesn't reflect on IA
CSCup03967	cat6000-l2-ec	RSL Member stuck in 'w' state after few interface flaps
CSCtq27155	cat6000-l2-mcast	'clear ip igmp snooping statistics' does not clear stats on standby sup
CSCuo84886	cat6000-ltl	Backout the changes CSCul88077
CSCug79705	cat6000-netflow	Unexpected reload if 6800IA host ports w/ dual flow monitors defaulted
CSCun30574	cat6000-qos	Wrong display order of Queue for FEX Host Ports
CSCun58476	cat6000-routing	cat6k:mls cef adjacency programmed with non-existent vlan
CSCuo51010	cat6000-snmp	Cisco C6880-X is returning incorrect OID for the MIB sysObjectId
CSCum43584	cat6000-span	6500 Ingress VLAN SPAN stops working

Identifier	Component	Description
CSCuo85141	cat6000-svc	Backing out changes of CSCun26135
CSCun20430	cat6000-sw-fwding	ospfv3 control packets entered incorrect queue
CSCun33658	cat6k-vs-infra	Cetus:remove est LC card,perform reload-MCL error msg and stdby is reset
CSCun78131	cat6k-vs-infra	FEX Module provisioning entry isn't removed completely upon unconfig
CSCun13688	clns	Device crash after "sh clns route" issued
CSCug86067	config-sync	Macros lost when ISSU from IOS XE 3.3.x to 3.4.0
CSCuh85819	config-sync	partial config lost on 2nd switchover on SUP7-E
CSCui03965	config-sync	ISSU XE392->XE310 Config-sync@commands configure include interface
CSCuh05259	config-versioning	file prompt quiet cli dont work with config replace cli
CSCun78994	connor-hw	Packets seen as runts on the neighbor when decapsulating dot1q/mpls
CSCuh37526	crypto-engine	Pseudo-random number was generated twice in succession
CSCuj99926	fib	SNAP Encapsulation not working with CEF enabled.
CSCum85813	ip	Floating static not installed on ASR901
CSCts34688	ip-acl	Switch crashed due to memory fragmentation "HACL Acl Manager"
CSCue68124	ip-pbr	PBR not work with null0 default route
CSCum95311	ip-pbr	ip next-hop recursive not forwarding traffic
CSCug47367	ip-tunnels	3900e crashes on bootup /w CDP on tunnel or traceback for non E platform
CSCuh72000	ip-tunnels	PI doesn't copy TOS from mpls header to IP/GRE header
CSCuj87667	ip-tunnels	The copy from MPLS exp bits to IP tos is done without the left shift
CSCum52676	ip-tunnels	Local packet marking is NOT copied on the Tunnel with qos pre-classify
CSCum92989	ip-tunnels	Traffic black-holed V6 tunnel encap packet over but payload less 1280
CSCul22535	ipc	VSS Quad Sup2T IPC failure causes a reload
CSCuj59816	ipmulticast	Auto-RP messages are dropped in a certain scenario
CSCui90139	ipsec-core	ASR1K : Crypto Route not getting deleted on Responder
CSCuh21969	mcast-vpn	MVPN Extranet Join(S,G) not triggered for Sparse-mode
CSCun86871	nat	Switch crashes due to nat processing Real Audio Traffic
CSCuo04983	netflow-switch	ip ingress added to interface config when ip flow ingress configured
CSCuh71381	ntp	PKI does not set renew timer upon a router reload
CSCui59004	ntp	iosd crash while configuring no ntp server
CSCuj66318	ntp	ntp allows query with access-group configured
CSCto43433	os	Router crashes while printing into tty
CSCto60263	os	PfR - ASR crashed at _be_validate_memory
CSCul54254	ospf	OSPFv3 may not flush some apparently self-originated LSAs
CSCul75876	ospf	RSP2:OSPF process - router crash on default interface
CSCul96608	ospf	%OSPF-SW2_STBY-4-CHKPT_MSG_SEQ printed on console
CSCum67697	ospf	OSPFv3 summary route via Null0 isn't installed after best route deleted
CSCun26962	ospf	Adding secondary IP address doesn't trigger OSPF update

Identifier	Component	Description
CSCun48344	ospf	SSTE: Amur: config-sync failure on address-family ipv6 unicast vrf
CSCun77010	ospf	Router crashed on executing "show ipv6 ospf rib".
CSCua73834	pki	Incorrect rollover cert issued to clients enrolling to IOS CA via IOS RA
CSCue32707	pki	PKCS12 "crypto pki export" may crash router
CSCuf93460	pki	PKI counters go into negative numbers
CSCug72874	pki	GM registers multiple times when cert is revoked due to wrong err fr PKI
CSCui07002	pki	PKI chain-validation seg fault process Crypto PKI-CRL if CRL is expired
CSCui39989	pki	PKI must handle intermediate issuer certs consistently
CSCui54042	pki	"no crypto pki certificate pool" command crashes router
CSCuj74574	pki	Router fails to delete expired ID and CA certificates after rollover
CSCuj88820	pki	Router gets into continuous cert renewal loop even after CA cert expires
CSCul40500	pki	PKCS10 in SCEP enrolment signed with MD5 not configured hash alg
CSCum12911	pki	IOS PKI auto-enrolment fails with enrollment-profile
CSCum94408	pki	IOS PKI Public Key caching fails during IKE MM6 Signature verification
CSCum96156	pki	IOS PKI fails to match certificate map if provisoned with config merge
CSCun20719	pki	IOS PKI renew timer does not start with enrollment profile
CSCui64807	ribinfra	Active RP crashes due to mem corruption after changing to Simplex mode
CSCun45471	ribinfra	RIP/OSPF config rollback fails with passive-interface default enabled
CSCtr91402	service-routing	Crash in __be_sr_api_vrf_af_deleted when removing vrf definition
CSCty21638	service-routing	Enabling SAF reloads the box setting null Q structure
CSCtd45679	sla	Removing ip sla probe (configured by SNMP) in CLI reloads Standby Sup
CSCud95329	sla	Wrong IP SLA schedule after reboot
CSCtz66347	ssh	Executing show tech over SSH session with rekey crashes the router
CSCui83823	ssh	SSHV2 session closes prematurely via telnet and putty
CSCum68602	vrfinfra	MPLS VRF MIBs are not cleaning up interface list iterators
CSCty92208	wccp	Ingress wccp + cts sgacl monitor + reboot results in CPU exception

Caveats Resolved in Release 15.1(2)SY2

Resolved tcp Caveats

- CSCtz14399—Resolved in 15.1(2)SY2

  Symptom: A vulnerability in TCP stack of Cisco IOS Software could allow an unauthenticated, remote attacker to cause an ACK storm.

  The vulnerability is due to improper closing of the established TCP connection. An attacker could exploit this vulnerability by sending a crafted sequence of TCP ACK and FIN packets to an affected device. An exploit could allow the attacker to cause an ACK storm resulting in excessive network utilization and high CPU.

  Conditions: Multiple FIN/ACK packets are received.

Workaround: Do clear' tcp tcb 0x.....' where the hex value is the address of the TCB stuck in LASTACK state in 'show tcp brief.'

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-2013-5469 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-2013-5469

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

Other Resolved Caveats in Release 15.1(2)SY2

Identifier	Component	Description
CSCtq36545	aaa	2960 %AAA-3-INVALIDPARM: invalid parameter was used when accessing AAA f
CSCuj65057	aaa	ip vrf forwarding is deleted after reloading stack master
CSCuh04989	aaa	Not Update Src IP address of Radius Packets
CSCug31122	aaa	Workaround fix for VTY hung issues
CSCul18227	bgp	ASR1K RR resets the PSMI tunnel attribute
CSCue68714	bgp	OVLD: BFD BGP Client Incompatibility between IOS t-train and IOSXE
CSCuj99819	bgp	LSM and MVPN traffic dropping after clear BGP * with TE Tunnel
CSCtw84414	c7600-l2	standby reset due to config sync "monitor session 4 source remote vlan"
CSCuh91225	call-home	Router crashes @ pki_import_trustpool_bundle while test call-home v2
CSCul29932	cat6000-acl	15.1(1)SY1
CSCul07195	cat6000-diag	active ICA will reload when HM LtlFpoeMemoryConsistency fail on standby
CSCum00653	cat6000-env	6500 - SNMP - CiscoEnvmonFanState incorrect - 15.1
CSCum76224	cat6000-env	6880x Crash due to "show plat hard capa"
CSCul39734	cat6000-env	Cat6k VSS incorrect ceDisplayState & ceDisplayColor for PS "FAN OK"
CSCuj13346	cat6000-env	VSS ciscoEnvMonRedundantSupplyNotification not sent from active chassis
CSCul21009	cat6000-env	MK1.C: Cetus: Change power redundancy model to N+1 for all combo of PSU
CSCul47658	cat6000-env	G1 image bundling with IOS image (for CSCul27866)
CSCuj28345	cat6000-env	QuadsupC2MK1b: Device crashed on reload with switching mode dcef
CSCui50773	cat6000-fabric	speed & product id blank in "sh inter trans fex-fab" o/p for SFP-10-LRM
CSCuj53393	cat6000-filesys	Trifecta: Trifecta LC hangs during bootup at rommon.
CSCuj78044	cat6000-firmware	6716-10G (Hw ver 2.0) may report inlet temperature higher than outlet
CSCui65654	cat6000-firmware	Packets are looped within chassis when WS-X6904-40G is used
CSCuj32632	cat6000-firmware	sup2t:traffic not received from 6848-SFP ports due to rx datapath stuck
CSCul77666	cat6000-firmware	Undersized frames sent with CTS static SGT
CSCui60473	cat6000-firmware	"show inventory raw" shows junk values for PID and VID for 1Gig SFP's

Identifier	Component	Description
CSCum02024	cat6000-firmware	6880-X Switch: ZR optics assert TX_FAULT
CSCun01599	cat6000-ha	MK1.C:[CAT6K NTI ERR]:NTI trace dumped for s2t54 while ISSU-up/downgrade
CSCul07387	cat6000-ha	VSS domain id change doesnt get updated on standby
CSCuh57728	cat6000-ha	Bootvar retains "version1" image after successful issu upgradation
CSCul19363	cat6000-hw-fwding	"platform sub-inter maximum-vlan enable,subinter stop forwarding traffic
CSCuj83351	cat6000-hw-fwding	Router mac not programmed in L2 table, learned as dynamic
CSCuj13109	cat6000-l2-ec	Sup2T MEC members go suspend when trunking native and trunk allowed same
CSCul64956	cat6000-l2	PVLAN association >255 char lost after reload
CSCuj30680	cat6000-l2	Continuous tracebacks @ udld_send_update upon disabling fast-udld
CSCul32006	cat6000-l2-infra	Some inconsistencies seen with mgmt port LED status
CSCum11422	cat6000-l2-mcast	Microsoft NLB disable snooping CLI needs to permit only applicable MACs
CSCul76822	cat6000-l2-mcast	Mem leak @ L2MM_PD Process seen during ISSU upgrade from mk1.0 to mk1.b
CSCul12004	cat6000-ltl	VSL included in L3 vlan flood index when both MEC legs are up
CSCui72220	cat6000-ltl	FEX Host PO ping fails on FEX reload, ARP not resolved
CSCul35053	cat6000-mcast	Crash of active supervisor during ISSU (commit) with multicast enabled
CSCul17734	cat6000-mcast	FE TCAM gets disabled which affects PIM packets
CSCul15855	cat6000-medianet	cat6k sup720- perf-mon with class-map match any affecting eigrp & ospf
CSCuj51621	cat6000-medianet	Egress traffic drop on L3 Port-channel after 2nd switchover
CSCuj48465	cat6000-medianet	cat6k sup720: perf-mon flows dropped after 2 SSO sessions
CSCug21068	cat6000-mpls	Internal vlan for egress feature assigned with IPv6 link local address
CSCui57810	cat6000-mpls	With mpls recir-agg in config New 6VPE disposition broken until reload
CSCug86296	cat6000-netflow	Sup2T: EARL8 Netflow ECC enhancement
CSCui17732	cat6000-netflow	Sup2T: show tech-support hangs VTY session on Netflow TCAM interrupt
CSCul21478	cat6000-netflow	CPU hog at CTS_CORE during env data refresh with >16k SGNames
CSCui37408	cat6000-netflow	HW inconsistency seen when ingress/egress FNF applied, removed on tunnel
CSCtg67789	cat6000-portsecur	Stdby reloads 'switchport port-security mac-address sticky <> vlan voice
CSCuj04075	cat6000-qos	Show platform Datapath on Connor shows incorrect vlaues
CSCuj96208	cat6000-routing	Crash seen @cfib_backfit_path when peer box is reloaded
CSCte53717	cat6000-svc	Need to change default SCP keepalive timeout on IOS to ACE module
CSCul14564	cat6000-svc	Supervisor Crash: due to "CAT6000_SVC_APP_HW-LC1-2-APP_..." message
CSCuj96561	cat6000-svc	wism redundancy-vlan and wism service-vlan must reject vlans in trunk
CSCul58236	cat6000-vntag	Traffic drop in FEX during ISSU b/w run and commit version
CSCul65499	cat6k-vs-infra	Sort the output of "show fex system platform usage" command
CSCuj48183	cat6k-vs-infra	Gov-Connor link shows notconnect as diag fail after switchover
CSCul22006	cts	cts environment-data SGT list become corrupted after refresh w/ 30+ SGTs
CSCul52636	cts	RBM registration with XDR IPv6 subtree is missing
CSCsv79584	dhcp	DHCP relay continuesly creates dangling 0/32 leases

Identifier	Component	Description
CSCuj72631	dns	Crash on configuring mdns
CSCuj58950	dns	mDNS traffic causes I/O memory leak
CSCui63462	dns	Bonjour/mDNS causes high CPU in unscaled setup
CSCua63182	eigrp	EIGRP min BW is calculated incorrectly for ngbrs of varying versions
CSCui23218	ethernet-lldp	NewtonCR IOS image fails UNH Test IEEE 33.1.2
CSCui98700	glbp	GLBP ip with same IPV6 link-local not allowed gives error
CSCul83053	hsrp	Unknown cHsrpStateChange trap detected when IPv6 HSRP state changed
CSCuj42862	ifs	6880-X Switch: Error in writing crashinfo "open failed (-1): I/O Error"
CSCug34404	ipsec-core	XE38 : RP_Crash seen @ __be_interface_action_remove_old_sadb
CSCug63839	ipsec-isakmp	Memory leak seen in CryptoIKMP process(crypto_ikmp_config_send_ack_addr)
CSCug38641	ipsec-switching	cTCP IPSec data packets are process switched on EzVPN server
CSCtx38121	ipv6	QoS ACL not working with IPv6 traffic on RLS12 image
CSCtw63654	ipv6	XDR-3-CLIENTISSU_PUSHFAIL: Attempting to push send XDR message (ipv6 acc
CSCuh69292	ldap	LDAP gets in stuck state even if PKI provides finite timeout
CSCuh41290	ldap	PKI with LDAP gets in stuck state due to infinite LDAP timer
CSCuh67605	nat	INVMEMINT errors related to NAT max-entries with vrf
CSCuj34455	nat	NAT Process Switches all TCP port 139 Traffic
CSCul38287	nat	NAT VRF to global not creating translations with single ip add. in pool
CSCuk59859	nat	ip_nat_anywhere miscalculated and features not removed
CSCul51526	netflow-switch	s2t crash due subinterface creation
CSCuj40804	nmsp	Fex doesn't come up after reload with "nmsp" protocol
CSCui60499	ntp	High CPU from Process NTP with "access-group serve" Configured
CSCul52741	os	C4MK1B QUADSUP:Infra ISSU Client error during LV from MK1B FC2 to MK1C
CSCul40073	ospf	OSPF interface Loopback goes DOWN after switchover on 3750 Stack
CSCtu02015	ospf	OSPF: Wrong metric in asbr-summary LSA
CSCul54254	ospf	OSPFv3 may not flush some apparently self-originated LSAs
CSCul14571	ospf	OSPFv3 NSR: crash when interface removed during delayed ack
CSCui13614	parser	Config of the interface disappears.
CSCul56726	snmp	6504 VSS Upgrade 15.1(1(SY) to 15.1(2)SY breaks SNMP
CSCuc39329	snmp	SNMP Engine Memory leak- while doing ccCopyEntry set operation

Caveats Resolved in Release 15.1(2)SY1

Identifier	Component	Description
CSCuf41477	aaa	TACACS line authorization failed when AV service=shell sent by Tacacs

Identifier	Component	Description
CSCuj99819	bgp	LSM and MVPN traffic dropping after clear BGP * with TE Tunnel
CSCsq75780	c3pl	Traceback %ALIGN-3-SPURIOUS: Spurious memory access sip-400 LC
CSCuh05334	cat6000-acl	CPU went high and standby crashed while pushing ACLs - SUP 2T
CSCuf02993	cat6000-acl	SUP2T active box crashes when reloading the standby because of FM
CSCug04222	cat6000-acl	SUP2T not forwarding unicast DHCP ACK when acting as relay agent
CSCui63768	cat6000-acl	terminator: missing sub_c6k_li subsys comapred to sup2t
CSCui70455	cat6000-acl	CSCug23641 changes for Earl8 releases (15.1(1)SY (MA2) onwards)
CSCui26454	cat6000-cm	c4mk1: Line card is getting reset while large acl is applied.
CSCue91936	cat6000-cm	FPOE not programmed properly after 3rd SSO with vacl redirect
CSCui44248	cat6000-diag	%CONST_DIAG-SW1-3-BOOTUP_TEST_FAIL: Switch 1 Mod4:TestIngressSpan failed
CSCui48359	cat6000-diag	Diag msg:GOLD EEM TCL policy TestFabricCh0Health/TestMacNotifcation fail
CSCud48400	cat6000-dot1x	External loop seen on switchport configured for dot1x/mab
CSCui96441	cat6000-dot1x	IP source guard not updating PACL entry when new DHCP client connected.
CSCtq71235	cat6000-env	"4294967295 Ethernet interfaces" in "show version" command output on c6k
CSCui25588	cat6000-env	No power enable on empty slot will not keep a new linecard powered off
CSCui68336	cat6000-env	Revisit CSCug29473
CSCuh75585	cat6000-env	system power total restricted to 2268w with 2700 PS in 7606-S chassis
CSCud57919	cat6000-env	40G SR4 Transceiver not recongnized under certain condition
CSCuh92395	cat6000-env	CFex FAN entries are lost in ENTITY-MIB after SSO
CSCul47658	cat6000-env	G1 image bundling with IOS image (for CSCul27866)
CSCuh95111	cat6000-env	Incorrect media type displayed for SFP-10G-LRM on controller.
CSCui19403	cat6000-env	%RPC-SW2-4-CORE_SAT_RPC_FAIL on raise/clear FEX env temp alarm after SSO
CSCug61422	cat6000-env	Old active & old active ICS reset after SSO
CSCui50213	cat6000-hw-fwding	LTL index mapping for NLB multicast MAC is delayed upon reload
CSCui79597	cat6000-hw-fwding	Lif entry is not getting updated on minitrunk port
CSCuj65447	cat6000-l2-ec	sup2t: crash on cat6k seen if L2 loops exists in network
CSCuh30542	cat6000-l2-infra	Traffic is blackholed when port-channel member flaps
CSCuh66052	cat6000-l2-infra	MTU of RSL links show 1500 inspite of constant value 9216
CSCue10124	cat6000-l2-infra	"%QM-SW1-4-SET_MODE: Hardware mode programming failed" @default FEX port
CSCui04115	cat6000-l2-infra	fex host ports are suspended with port in half-duplex for LACP error
CSCui27472	cat6000-l2-mcast	IGMPv3 leave reports with "Change_to_include" and "sources 0" flooded
CSCuf24777	cat6000-l2-mcast	MCVPLS: PIMSN (*,g) mroutes not removed after stops joins and source
CSCui86318	cat6000-ltl	unicast flooding because mac address not learnt correctly across DFCs
CSCuh80379	cat6000-ltl	"Total unicast VIFs used" displays wrong value after SSO.
CSCuh05923	cat6000-ltl	FEX : mem leak @ vntag_mgr_handle_ucast_add_req
CSCud45116	cat6000-mcast	MCVPLS: Traffic drop seen at other Rx when one of the Rx sends leave

Identifier	Component	Description
CSCue52201	cat6000-mcast	Output of "show mls ip multicast met detail" display incorrect OIF,MET
CSCug26395	cat6000-netflow	c4mk1: FM consistency checker found in FNF
CSCug73871	cat6000-netflow	FNF: Multicast First and last packet time stamps are incorrect
CSCuh78078	cat6000-netflow	C4QUDsup:After 2nd SSO, Reverse traffic is not flowing with ReflexiveAcl
CSCui41308	cat6000-oir	QuadSup:OIR changes for ISSU abort verion
CSCui48063	cat6000-oir	FEX continuously reloads in some conditions
CSCug63410	cat6000-portsecur	Sup2T - Inband input packet drops on IBC
CSCuh94242	cat6000-qos	Agg. policer with 'platform qos police distributed' drops all traffic
CSCui27401	cat6000-qos	cat6000-qos Traceback and crash after linecard failure
CSCui08992	cat6000-qos	Child lan-queuing policy shouldn't accept 8 classes for 1p7q8t
CSCui72775	cat6000-qos	sup2T - 'auto' CLI not listed upon a ?
CSCuj31321	cat6000-qos	Sup2T: Notification timer expired for RF Client: Cat6k QoS Manager
CSCue34550	cat6000-qos	Even with L4OP Range in ACL definition Global Policy-Map gets enabled.
CSCui08914	cat6000-qos	L2-Miss match is getting accepted on Ingress Routed-Interface also
CSCui73345	cat6000-qos	Two priority queues doesn't work when shape is configured
CSCui25364	cat6000-qos	Bulk sync failure causes continuos standby reload with cos-mutation
CSCuj17251	cat6000-qos	Port level shaper doesn't work when shape is not configured on queue
CSCuh98603	cat6000-routing	sup2t :: uRPF dropping packets
CSCui87669	cat6000-snmp	ciscoEnvMonTemperature is not always sent out after module insert
CSCui82742	cat6000-svc	c4mk1: NAM-3 on Standby fails to recover after ISSU load version
CSCuj08631	cat6000-svc	NAM:Accessing span sessions not available through GUI after SSO
CSCui19374	cat6000-sw-fwding	Sup2t forwards traffic sourced at IP 0.0.0.0 when dst MAC is broadcast
CSCui35002	cat6000-vntag	L2/L3 traffic doesn't resume after Controller SSO followed by FEX reload
CSCui75787	cat6000-wccp	Redirect ACL do not work when WCCP client asked for multiple ports
CSCuj85177	cat6k-vs-infra	catalyst 6500 VSS switch does not come up in SSO after upgrade
CSCui83552	cat6k-vs-infra	ROIR removal of fex does not always reload the fex
CSCuh68974	cat6k-vs-infra	entPhysicalVendorType returns nullOID for FEX chassis.
CSCue95010	cat6k-vs-infra	FEX : mem leak @ fexmgr_sdp_srp_pkt_handler after bootup
CSCui77236	cat6k-vs-infra	FEX Ports does not come up after SSO if standby port delay is configured
CSCuf86511	cat6k-vs-infra	System does not boot if all 4k vlans are present in startup config.
CSCse52239	clns	c2600xm with ctunnel and no destiination nsap upon reload router crashes
CSCuj29428	crypto-engine	%SYS-SW1-2-INTSCHED: 'sleep for' at level 2 -Process= "Init"
CSCug71572	dhcp	DHCPv6 relay not working over LISP
CSCuc99750	eigrp	EIGRP routes which are not FS making it to the routing table
CSCud02045	ethernet-cfm	RP crashes after applying cfm mip config to interface
CSCsy87125	ethernet-oam	EOAM:RFI DG msgs are continuosly sent to peer on redundancy RPR-->SSO
CSCuj64806	fhrp	VRRPv2 priority goes wrong with tracking tunnel

Identifier	Component	Description
CSCuh40275	fib	MCP: SNMP Engine process occupy more than 97% CPU utilization
CSCui45414	flexible-netflow	SUP2T crash due to memory corruption with alloc PC related to FNF
CSCui95880	hsrp	HSRP for IPv6 flaps when there is a loop in the network.
CSCui47386	hsrp	HSRP MIB should send traps for all groups
CSCtk00976	ifs	File descriptor leak and not getting release - readh FD limit
CSCuj08831	ipc	Crash @ ipc_compare_seats part 2
CSCui83592	ipc	Line card WS-X6816-10GE crashed in IPC code
CSCui46951	ip	"%Bad mask x.x.x.x for address x.x.x.x" output with ip account-list
CSCuk62206	ip	static arp change not notified to CEF/ADJ
CSCui94718	ip	Watchdog in IP Connected Route Background
CSCua44483	ipmulticast	ME3600X suddely stops sending multicast for all groups 151-2.EY
CSCuj27671	ip-tunnels	QUAD SUP2T VSS Failover fails with tunnel path-mtu-discovery config
CSCuc38611	ip-tunnels	TTL of inner header is decremented twice
CSCtl51688	nat	NAT Error registering with Transport Port Manager - Standby Reload
CSCui94118	nat	static NAT vrf removed upon removal of "vrf definition <vrf_name>"
CSCui52587	ntp	ntp broadcast config of the last vlan was removed after delete a SVI
CSCui23670	remote-tty	Even if show sup-bootdisk is executed, nothing is displayed.
CSCui72518	rsvp	IOS RSVP authentication problem during TE FRR
CSCuj23802	tcp	SUP2T crash after unplug/plug 4 sfp from the WS-X6724-SFP
CSCsw29816	vpdn	L2TPv2 - Enabling ip pmtu on the LAC may blackhole large packets
CSCtj44098	vpdn	SSM CM: SSM switch id 0 [0x0] allocated issue
CSCtb34814	x25	Crash after %DATACORRUPTION-1-DATAINCONSISTENCY
CSCuj65989	xdr	Active sup in crash due to process "xdr_mcast_set_max_seq_for_transmit"

Caveats Resolved in Release 15.1(2)SY

Resolved gsr-boot Caveats

- CSCsv74508—Resolved in 15.1(2)SY

  Symptom: If a linecard is reset (either due to an error or a command such as hw-module slot reload) at the precise time an SNMP query is trying to communicate with that linecard, the RP could reset due to a CPU vector 400 error.

  Conditions: This symptom occurs when the linecard is reset (either due to error or a command such as hw-module slot reload) at the precise time an SNMP query is received.

  Workaround: There is no workaround.

Resolved ios-authproxy Caveats

- CSCtz99447—Resolved in 15.1(2)SY

  Symptom: Local webauth and HTTP services stop responding on the switch.

Conditions: A **show processes | inc HTTP Proxy** lists many instances of the "HTTP Proxy" service, and these do not disappear.

Workaround: The HTTP Proxy service may experience delay due to an incorrectly terminated HTTP or TCP session. In some cases, increasing the value of **ip admission max-login-attempts** works around this issue. In others, the stuck "HTTP Proxy" service will again become available after a TCP timeout.

Some browsers and background processes using HTTP transport can create incorrectly terminated HTTP/TCP sessions. If webauth clients are under control, changing web browsers or eliminating background processes that use HTTP transport may eliminate triggers for this issue.

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 5/4.1:
https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:N/C:N/I:N/A:P/E:F/RL:OF/RC:C

CVE ID CVE-2012-4658 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

Resolved ios-firewall Caveats

- CSCtx56174—Resolved in 15.1(2)SY

  Symptoms: Cisco router hangs until a manual power cycle is done. If the **scheduler isr-watchdog** command is configured, the device will crash and recover instead of hanging until a power cycle is done.

  Conditions: This is seen with websense URL filtering enabled and with zone based firewalls.

  Workaround: Disable URL-based filtering.

Resolved ntp Caveats

- CSCtw62695—Resolved in 15.1(2)SY

  Symptoms: Packets sent by the Cisco IOS NTP server will have the IP identification field set to zero, behavior which may be flagged as a vulnerability by some security scanners.

  Conditions: NTP server configured on Cisco IOS

  Workaround: There is no workaround

  Further Problem Description: Other UDP-based services on IOS (SNMP and DHCP as two examples) set the IP ID field to a nonzero value. As CVE-2002-0510 was originally reported as a way to identify a device as running a Linux 2.4-based kernel, the actual value of using this as a method to identify the underlying OS is very low.

  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 5/4.8:

  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:F/RL:U/RC:C

  CVE ID CVE-2002-0510 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

Resolved ssh Caveats

- CSCto87436—Resolved in 15.1(2)SY

  Symptoms: In certain conditions, IOS device can crash, with the following error message printed on the console:
  "%SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = SSH Proc"

  Conditions: In certain conditions, if an SSH connection to the IOS device is slow or idle, it may cause a box to crash with the error message printed on the console.

  Workaround: None

  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 6.3/5.5: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:S/C:N/I:N/A:C/E:H/RL:OF/RC:C CVE ID CVE-2012-5014 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

Other Resolved Caveats in Release 15.1(2)SY

Identifier	Component	Description
CSCub04965	aaa	TCP Session hung causing Packet loss
CSCuc50697	aaa	Exec Authorization fail of session-timeout is greater than 2147483 image
CSCuc59858	aaa	Dynamic-Author should consider src port when detecting retransmissions
CSCue03316	aaa	EoGRE: SSS Manager Segmentation fault/RP reloaded during scale test.
CSCue13913	aaa	Incorrect password used by RADIUS automated-tester after config save
CSCue18133	aaa	[7600] Router crash at show_li_users
CSCue87815	aaa	The secret password in "setup" not saved
CSCuf17296	aaa	ASR1k ISG: Missing Class Attribute in Accounting-Request
CSCug24114	aaa	CTS env download failed on non seed device after reboot
CSCug62154	aaa	Mk1: High CPU 100% due to TPLUS with tacacs config
CSCuh43252	aaa	unable to login and high cpu when authenticating with TACACS
CSCua76157	bgp	BGP routes getting advertised even after removing send-lable from the PE
CSCuc22651	bgp	XE 38: BGP RR SIT: Doing shut on interface, crashes BGP

Identifier	Component	Description
CSCuc60297	bgp	redistribute VRF route into BGP with global NH does not work
CSCud55286	bgp	On SSO IIF int goes Null & traffic drop,mpvn: 60-90 sec traffic drop
CSCud55354	bgp	BGP_MIB: Incorrect InetAddressType being returned
CSCud79067	bgp	CISCO-BGP-MIB output presented in non-ascending order
CSCue28908	bgp	Router may crash with "show ip bgp vpnv4 vrf < >" command
CSCue65006	bgp	MPLS-VPN traffic fails in pure BGP NSR environment
CSCue72839	bgp	BGP link-bw doesn't program traffic share cnt in RT/CEF if soft-in+r_map
CSCue76102	bgp	XE39:IBGP ipv6_redistributed routes not learned in neighbour router
CSCuf09006	bgp	clear ip bgp * soft out or graceful shut on PE purges all routes on RR
CSCuf09198	bgp	vrf lock is not free up after no vrf definition vpn under AD and Croute
CSCuf82179	bgp	BGP routes not cleared from multicast RIB when address-family removed
CSCug09958	bgp	Default ipv6 routes '::/0' turn to ::/16
CSCug82964	bgp	BGP NSF forwarding state not preserved during SSO
CSCuh07657	bgp	VRF Aggregate label not re-originated
CSCuh24040	bgp	BGP routes not marked Stale nor removed when peer down w/ BFD signaling
CSCuh43027	bgp	BGP route does not disappear from the RIB
CSCuh43255	bgp	ASR route server crashes due to BGP task
CSCue27826	c6k-l3-lisp	LISP: set dscp tunnel with LISP not marking outer hdr for IPv6 traffic
CSCuf83644	c6k-l3-lisp	LISP: Traffic drop on ITR encap when destined to PETR
CSCug14851	call-home	s72033:Tracebacks seen while doing ISSU from ma2.0 to ma2.b.
CSCue61593	cat6000-acl	show acl doesn't display Ethertype configured.

Identifier	Component	Description
CSCue65728	cat6000-acl	SUP-2T--VRF NAT stops working after 24-48hrs into operation
CSCue89061	cat6000-acl	6k crashes while applying a non-existing Mac ACL on the port
CSCue93721	cat6000-acl	PPTP call not getting conn. when extendable keyword used with static nat
CSCug08012	cat6000-acl	LISP: Encap traffic drops if we unconfigure "ipv4 etr"
CSCug14796	cat6000-acl	FM INCONSISTENCY CHECk on 6500 VSS switch due to FMCC issue
CSCug27047	cat6000-acl	Config Sync: Bulk-sync failure due to PRC mismatch in ACL
CSCug34187	cat6000-acl	CSCug23641 changes for 15.1(1)SY (MA2) release onwards
CSCug56779	cat6000-acl	c4mk2:Active sup crashes @ ipnat_l3_fixup
CSCug65925	cat6000-acl	CPU hog messages after making changes to ACL
CSCug69230	cat6000-acl	HSRP Packets dropped, on applying inbound ACL with LOG statement / Sup2T
CSCuh57776	cat6000-acl	DHCP binding entry expire
CSCui44825	cat6000-acl	LIF expansion not working on voice vlan Fex host ports after reload
CSCuf81446	cat6000-cm	SUP2T reset w/ Failed TestL3TcamMonitoring w/ high adjacency utilization
CSCuh07066	cat6000-cm	Sup2T - ACL Tcam count - Malfunction - Adds additional ACL's - TCAM Leak
CSCuh60848	cat6000-cm	crash@cm_rbacl_replace_req_hdlr while enabling the enforcement
CSCug54436	cat6000-cts	After first SSO traffic drop seen on cts link with cts egress reflector
CSCue72286	cat6000-diag	MA2b:Diagnostic handler is not found for DFC card after switchover
CSCuf85528	cat6000-diag	Multiple GOLD tests disable autoboot when HW isn't at fault post failure
CSCug78833	cat6000-diag	Quadsup:online-diag take wrong action on standby-ICA when ICS SUP fail
CSCuh17586	cat6000-diag	Crash after CF/disk failure due to read/write operations involving SEA
CSCtj15915	cat6000-dot1x	Static MAC entry not removed with MAB and dot1x multi-host
CSCue31621	cat6000-dot1x	MAB fails after 6500 reload when port configured for critical voice vlan

Identifier	Component	Description
CSCuh03710	cat6000-dot1x	cat6000 dot1x in MDA - IP phone losing connectivity after few minutes
CSCue59987	cat6000-energywise	Input queue size becomes negative with energywise enabled.
CSCug69969	cat6000-energywise	Memory leak of 76 bytes in powernet pd process after OIR of a card
CSCud75039	cat6000-env	6500 with 12.2(33)SXI7 doesn't send traps on 10G low optical power alarm
CSCue93101	cat6000-env	Cat6k: "exception memory minimum ... reboot" does not work on SP
CSCuh43325	cat6000-env	Sup 720 switchover causes incorrect show power output
CSCue02511	cat6000-fabric	VSS FPOE incorrect on standby
CSCue58955	cat6000-filesys	sup2t: LC file systems are not destroyed in Active upon reset
CSCue99098	cat6000-filesys	When Dom0 mode is RPR, standby ICS RFS not created.
CSCug29473	cat6000-filesys	Crash on Sup2T when copy initated through scp/tftp
CSCue11384	cat6000-firmware	c4ma2: Estell fabric OR mask programming is not proper
CSCug28934	cat6000-firmware	Incorrect COS Map and Negative Min Threshold in hardware for WS-X6548-GE
CSCud15048	cat6000-ha	Add mini trunk support to LIF manager
CSCug21530	cat6000-ha	Active ICS fails to reload from rommon
CSCuh45404	cat6000-ha	C4 4sup: optimize time to notify VSL on switchover
CSCtt42531	cat6000-hw-fwding	Fib Exception only on multiple WS-X6908-10G of Sup2T system
CSCue49346	cat6000-hw-fwding	C6K/Sup2T: LDB Mgr should not preallocate 4K LIF for L3 Subinterfaces
CSCue58387	cat6000-hw-fwding	TCAM Exception State Should Capture Prefix Distribution
CSCue79979	cat6000-hw-fwding	MCVPLS: LIF entry on DFC is not synced.
CSCuf46062	cat6000-hw-fwding	Sup2T: MAC Address is not synced properly across DFCs
CSCug44811	cat6000-hw-fwding	SUP2T:Sub-interface does not stay down when LIF entries are exausted
CSCug94630	cat6000-hw-fwding	l3 svi ip address is not reachable with service-policy on mini-trunk

Identifier	Component	Description
CSCug94822	cat6000-hw-fwding	Host looses entry in IPDT after some time or some time post SSO
CSCuh24511	cat6000-hw-fwding	Static Mac entries create Config sync issue in VSS on reload of standdy
CSCuh43287	cat6000-hw-fwding	Cat6K: Mac entries learned on a trunk are flushed after removing vlans
CSCui65190	cat6000-hw-fwding	Incorrect policing behaviour with same policer on multiple interfaces
CSCug75365	cat6000-ipc	Crash in icc multicast code on sup720 from cmfi_process_feature_msgs_int
CSCuh45350	cat6000-ipc	C4 4sup: IPC reinit for LCs in remote chassis take over 2.5 seconds
CSCdy62921	cat6000-l2	Software forced crash when adding bridge-group to ATM subinterface
CSCug37230	cat6000-l2	System Crashes at VLAN Manager due to VTP packets looping
CSCug90305	cat6000-l2	Power deny of 6148-ge-tx-AF/AT interface with 2602 factory reset
CSCuh33725	cat6000-l2	VSS may switchover when configuring vlans
CSCui55665	cat6000-l2	STP BA can cause RSL to be stuck in BLK and Impacts FEX Image download
CSCud58772	cat6000-l2-infra	IDB gets messed up with creation/deletion of Port-channel
CSCuf36123	cat6000-l2-infra	VSS Standby crash after renaming vlan
CSCud72421	cat6000-l2-mcast	C4MA2B:VPLSoverGRE-IGMP Snping Querier pkts not send to CEs for sub-inte
CSCug75502	cat6000-l2-mcast	UDP packet to FF02::1 not flooded to the Vlan
CSCud26697	cat6000-ltl	%BIT-SW1-4-OUTOFRANGE: error on 11/17 build
CSCue84185	cat6000-ltl	C4 Quad: Distributed policing fails on switchover and reload peer
CSCuh98106	cat6000-ltl	Unable to ping the directly connected neighbour after ISSU in Qsup
CSCui35333	cat6000-ltl	LTL alloctn failre for L2 mcast bcoz LTL calbak not received + LTL shrng
CSCui64318	cat6000-ltl	LTL missing for fex host ports on double sso and fex remove/add
CSCue81201	cat6000-mcast	"ip multicast boundary <ACL> in" is blocking outbound multicast
CSCtj90838	cat6000-medianet	packet counters in "show policy-map type perf int" not working on Cat6k
CSCue77698	cat6000-medianet	MT monitoring stops when last ingress VM policy in the system is removed

Identifier	Component	Description
CSCud99759	cat6000-mpls	VPLS over GRE Scheme 2 is not working as expected on DFC /Standby Sup
CSCuf21968	cat6000-mpls	6500: SXJ5 no 802.1Q VLAN TAG in vc type 4
CSCug39407	cat6000-netflow	Middle buffer leak when netflow with cdp enabled on tunnel interface
CSCuh51188	cat6000-netflow	Big buffer leak when netflow with lldp enabled on tunnel interface
CSCue91216	cat6000-oir	VSS config causing OIR PROCESS HOGGING CPU CREATED THE CRASH
CSCug61801	cat6000-oir	Remove a LC in Quad-Sup and then a SSO could result in VSS freeze
CSCue45522	cat6000-qos	Device crashes when modifying lan-queuing policy
CSCuf20455	cat6000-qos	Table-map with mapping value greater than 63 can be created and applied.
CSCuf56153	cat6000-qos	Updation of DSCP mutation map does not take effect.
CSCug28878	cat6000-qos	c4mk1: Traceback@vs_get_pslot_switch_id
CSCug29131	cat6000-qos	Distributed Policing is not disabled on conf replace
CSCug32878	cat6000-qos	C4Quad: Cos-mutation fails on uplink after SSO or reload.
CSCug42413	cat6000-qos	Attaching lan-queueing pol on a tunnel intf results in ServPol cmd crash
CSCue02387	cat6000-routing	removing VRF causes global default route to fail
CSCug26327	cat6000-routing	sup2t : urpf incorrectly drops traffic after vrf is configured
CSCud18108	cat6000-snmp	CAT6500 SNMP timeouts polling dot1dTpFdbTable
CSCsh37045	cat6000-svc	confusing log message - SVCLC-5-FWTRUNK:
CSCuf03709	cat6000-sw-fwding	SUP2T: MPLS EXP not copied to outer dot1q CoS for locally-generated BGP
CSCuf60783	cat6000-sw-fwding	Crash seen in adj_switch_handle_fragmentation on changing the MTU size
CSCug42222	cat6000-sw-fwding	VSS VPLS: Core Switch is not forwarding DHCP request received via VPLS.
CSCuf85182	cat6000-wccp	Sup2T after removing WCCP FEATURE_TUN_x interfaces are not removed

Identifier	Component	Description
CSCug24158	cat6000-wccp	Disable LLDP on WCCP tunnel interfaces
CSCue97597	cat6k-vs-infra	c4ma2b: Switch goes to recovery mode while VSS-->SA conversion after SSO
CSCuf86245	cat6k-vs-infra	Standby does not get to RPR mode with image version mismatch
CSCug23479	cat6k-vs-infra	Switch PMK configured on slot 6 sup not synced to sup on slot 5
CSCug28704	cat6k-vs-infra	"wrr-queue" appears under fast-hello port after some config and reload
CSCug47997	cat6k-vs-infra	C4 ISSU FC3 renamed: After CV, whole quad-sup setup reloads
CSCty06243	checkpoint	After reload, 1st time none of scale IP ISG sessions syncing to stby
CSCug00938	cmts-platform-infr	CST: Single step ISSU failed at runversion
CSCud99034	crypto-ace	ISM-VPN crypto engine encaps fails in 15.3(1.11)T
CSCud54133	crypto-engine	FIPS certification : need continuous random number generator test
CSCue42714	cts	Manual cts link not coming UP after switchover
CSCue92705	device-sensor	Address memory leaks in device-sensor for cache delete case.
CSCtg57657	dhcp	Router crash at dhcp function
CSCue40955	dot1x-ios	802.1x Re-authentication timer is not cleared after CoA
CSCud95127	eap2	CAT6K crashes when cts change-password procedure is interrupted
CSCub20803	eigrp	EIGRP Wide-Metric: Unknown Delay is added for static routes
CSCud41058	eigrp	ASR / 152-4.S1 / EIGRP does not read route tags
CSCue78192	eigrp	EIGRP not withdrawing routes as a result of specific update/ack sequence
CSCug17808	eigrp	EIGRP not advertisinsg redistributed routes from BGP
CSCug72891	eigrp	EIGRP successor loop results in SIA
CSCug79541	eigrp	extended communities are lost after increasing delay metric in EIGRP
CSCud96882	ethernet-lldp	Buffer leak seen in I/O with lldp_send_update

Identifier	Component	Description
CSCtw68089	eventmgr	Routing ED is missing
CSCty55449	eventmgr	Device crashes when EEM trigger is misconfigured
CSCub40161	eventmgr	Issuance of an EEM command hogs the console
CSCud31581	eventmgr	EEM script crashes router due to memory corruption
CSCua55797	glbp	privilege exec level 0 show glbp brief command causes a MALLOCFAIL
CSCuf89251	gold	FEX: 4sup ISSU the new standby crashes due to CHUNKBADFREEMAGIC
CSCub98384	hsrp	standby ASR can not ping HSRP IP
CSCue61883	ifs	In terminator partitioning the usbflash is not working.
CSCtq84313	infra-xoslib	CPUHOG due to IP SLA followed by watchdog crash on replacing config
CSCuf56303	install	ISSU abort version should show in the status
CSCue18443	ip	Subnet mask not sent in authorization request
CSCub75883	ip-acl	Access-line numbers are NOT persistant after reload
CSCui97182	ipc	6500 RPC packet leak leading to crash
CSCud50768	ipmulticast	BSR: Incorrect timer reset for BSR during switchover
CSCud90983	ipmulticast	OTV Multihome setup: Multicast stop working when shut/no shut join int
CSCue68761	ipmulticast	Buffer leak @ ip_mforward in 15.1(4)M3
CSCue75986	ipmulticast	XE39: IOSd crash @ mvpn_pim_send_join_periodic
CSCtz87485	ipsec-core	MALLOC at interrupt level only when a crypto map configured on a GigE
CSCub05907	ipsec-core	RRI isnt propagated after failure of a link, when spoke has dual ISP
CSCub26395	ipsec-core	IOS - New VPN dynamic maps not working
CSCuc36469	ipsec-core	CSR-Crash @__be_crypto_lookup_short_handle during ezvpn tunnel bring up
CSCuc93739	ipsec-core	EzVPN client with split network does not come UP when IPSEC SA is down
CSCud42938	ipsec-core	Ident remains at DMAP side even when there are no ipsec sas

Identifier	Component	Description
CSCud59176	ipsec-core	Backout CSCub95141 in XE37
CSCud69442	ipsec-core	crypto map fails after interface flap or ip address change
CSCuc08061	ipsec-dmvpn	DMVPN spoke's crypto session was gone after removing, adding tunnel back
CSCud68178	ipsec-dmvpn	XE39: DMVPN Hub crashed after physical and tunnel interface flapping
CSCuc98855	ipsec-ezvpn	When server sends Savepwd off, client fails to establish EZVPN session.
CSCtu54300	ipsec-getvpn	fn_VRFAwareGM: KS crashed while running getvpn unconfig script
CSCtz78943	ipsec-ha	Crash after configuring a crypto map on a HSRP enabled interface 2
CSCud06887	ipsec-ha	IPSec Stateful Failover - SPIs not replicated after first switch
CSCtu02543	ipsec-isakmp	EZVPN client address leak due to peer overlap (NAT)
CSCua31157	ipsec-isakmp	One way IPsec traffic after initial isakmp contact deletes budding SA
CSCub67774	ipsec-isakmp	IKE: MM6 not re-sent if MM5 retransmitted
CSCuc31761	ipsec-isakmp	XE3.9 - KS crashes when removing GDOI groups
CSCue44587	ipsec-routing	ASR Missing RRI routes is with active SAs
CSCub83722	ipsec-switching	Tunnel interface output rate does not increment in a MPLS network
CSCuc94687	ipsec-switching	SHA256 HW crypto support on 890 Platform is missing
CSCue45934	ipsec-switching	Return traffic is not coming back in ipv4 session on c6k wit ikev2 MA2re
CSCub74272	ipsec-vti	Crypto Socket goes to closed state causing SA flaps every phase 2 rekey
CSCub89144	ipsec-vti	VTI interface is always in up/up state on HSRP standby
CSCtt96462	ip-tunnels	Packets dropped when CEF enabled under Tunnel interface
CSCua16562	ipv6	OSPFv3 External routes cannot be redistributed into BGP by route-map
CSCua21049	ipv6	ipv6 route 11::1/128 16::1 multicast fails to insert into murib
CSCuc73473	ipv6	IPv6 default route is not redistributed in BGP
CSCuc58603	isis	ciiISAdjIPAddrType reported as version 4 instead of version 6

Identifier	Component	Description
CSCuf03079	isis	UEA:IOSd crash is seen during reopt with r-lfa in the RING
CSCug91111	isis	IS-IS flaps routes when advertisement moves to a new LSP
CSCue28318	ldap	Router crashes while executing test aaa command with wrong LDAP config.
CSCug52119	lisp	LISP: existing map-cache entry, BGP route introduced, cef keeps lisp enc
CSCta48521	loadbal	%DATACORRUPTION-1-DATAINCONSISTENCY: copy error
CSCuc51879	mcast-infra	Traffic loss on ASR1K in event of RP SSO switchover
CSCue61691	mcast-vpn	Mroute shows data mdt switchover but MRIB still shows up the default MDT
CSCue69214	medianet-metadata	Memory leak @__be_fmd_get_if_fn_buffer on removing MLPPP
CSCuf20537	mpls-te	C4: New Active Sup crashes on second SSO @rrr_autoroute_add_tunnel
CSCeb77918	nat	HSRP/NAT:Continuous ARP storm after failover of active router
CSCua46304	nhrp	Seg fault at __be_nhrp_group_tunnel_qos_apply on flapping tunnel
CSCuc45115	nhrp	Crash seen at nhrp_add_static_map
CSCua14640	ntp	Change in order of configuration statement after router reload
CSCua58386	ntp	NTP MIB for Dispersion Values incorrect
CSCua80643	ntp	892J NTP Source address doesn't change after routing path change
CSCuc44629	ntp	NTP crash during bootup
CSCuc90999	ntp	CISCO1921 snmp cntpSysPeer does not reset after removing ntp server
CSCud72473	ntp	NTP: Frequency Errors and Clock Loses Sync with 2 servers
CSCug85720	nvram	SupT2 crashes with seg fault after 'copy ftp: startup-config'
CSCug33116	os-logging	SUP2T in VSS crashes after reload if "logging origin-id ip" configured
CSCue36197	ospf	7600 Router Crashes When Exiting OSPF Helper Mode (RFC 3623)
CSCuf61469	ospf	route tag disappears by summary-address in NSSA after route flapping

Identifier	Component	Description
CSCug23453	ospf	OSPF: route not redistributed due to DBEXIST error message
CSCug85947	ospf	MK1: Post SSO, routes go missing from LSDB and RIB
CSCuh18132	ospf	OSPFv2 NSR: reboot command does not reboot the router
CSCuh32177	ospf	OSPFv3 no passive-int <if-name> incorrectly added for ipv6 int
CSCuh40329	ospf	OSPFV3 shamlink locks up GRE tunnel
CSCub17971	pas-ipsec	GETVPN Adv: No re-registration after switching from hw to sw crypto eng
CSCud66669	pas-ipsec	VSA: GRE with TP - Packet is not decrypted into the correct ivrf
CSCug78098	pim	SUP crash in pimv2_show_rp_hash
CSCty94210	pki	ENH FlexVPN: CERTREQ improvements in IKEv2 exchange
CSCub98357	pki	OCSP validation with disable nonce is causing crashes.
CSCue44706	qos	cbQosQueueingCfgBandwidth - CISCO-CLASS-BASED-QOS-MIB - Incorrect Value
CSCuf14343	redundancy-rf	MPLS-TP traffic restore in about 10 seconds after RP switchover
CSCud80688	rmon	rmon alarm configuration is lost during upgrading from SXF to SXJ,SXI
CSCue40304	rsvp	could not find some sender in cli o/p of show ip rsvp sender vrf ivrf1
CSCuc82551	sla	Segmentation fault(11), Process = SNMP ENGINE on ASR1001
CSCug97383	sla	Switch crashes with EOAM and IP SLA configurations
CSCee55603	snmp	SNMP ACL does not work for VRF interfaces
CSCts75438	snmp	multicast hardware forwarding doesn't work after commit of CSCtn50281
CSCue80816	snmp	Crash while routine config push through SNMP
CSCuf43525	snmp	Dom1 SNMP RF client times out when Dom0 mode is RPR
CSCue37342	spa-eth-ge-5	"no snmp trap link-status" command is removed after reboot
CSCug34877	ssh	crash during ssh connections establishment / resume

Identifier	Component	Description
CSCub36403	tftp	VSS peer reloads for Line-by-Line sync verifying failure
CSCue74612	tftp	Fts Client fails to perform ftp transfer
CSCsl19590	usb-flash-filesys	Crash at usbflash_open set_device_type
CSCug89598	vtp	"no vtp" interface configuration leads to unexpected pruning

Caveats Resolved in Release 15.1(1)SY3

Resolved aaa Caveats

- CSCue95644—Resolved in 15.1(1)SY3

  Symptom: This is the Cisco response to research performed by Mr. Philipp Schmidt and Mr. Jens Steube from the Hashcat Project on the weakness of Type 4 passwords on Cisco IOS and Cisco IOS XE devices. Mr. Schmidt and Mr. Steube reported this issue to the Cisco PSIRT on March 12, 2013.

  Cisco would like to thank Mr. Schmidt and Mr. Steube for sharing their research with Cisco and working toward a coordinated disclosure of this issue.

  A limited number of Cisco IOS and Cisco IOS XE releases based on the Cisco IOS 15 code base include support for a new algorithm to hash user-provided plaintext passwords. This algorithm is called Type 4, and a password hashed using this algorithm is referred to as a Type 4 password. The Type 4 algorithm was designed to be a stronger alternative to the existing Type 5 and Type 7 algorithms to increase the resiliency of passwords used for the enable secret password and username username secret password commands against brute-force attacks.

  This Cisco Security Response is available at
  http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20130318-type4

  Conditions: See published Cisco Security Response

  Workaround: See published Cisco Security Response

  Further Problem Description: PSIRT Evaluation: The Cisco PSIRT has evaluated this issue and a Cisco Security Response is available at
  http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20130318-type4

  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/web/about/security/psirt/security_vulnerability_policy.html

Resolved ios-authproxy Caveats

- CSCtz99447—Resolved in 15.1(1)SY3

  Symptom: Local webauth and HTTP services stop responding on the switch.

  Conditions: A **show processes | inc HTTP Proxy** lists many instances of the "HTTP Proxy" service, and these do not disappear.

Workaround: The HTTP Proxy service may experience delay due to an incorrectly terminated HTTP or TCP session. In some cases, increasing the value of **ip admission max-login-attempts** works around this issue. In others, the stuck "HTTP Proxy" service will again become available after a TCP timeout.

Some browsers and background processes using HTTP transport can create incorrectly terminated HTTP/TCP sessions. If webauth clients are under control, changing web browsers or eliminating background processes that use HTTP transport may eliminate triggers for this issue.

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 5/4.1: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:N/C:N/I:N/A:P/E:F/RL:OF/RC:C

CVE ID CVE-2012-4658 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

Resolved ipsec-ikev2 Caveats

- CSCub93641—Resolved in 15.1(1)SY3

  Symptom:

  The load balancing feature of the flex-vpn solution of Cisco IOS does not provide authentication facilities to avoid non authorized member to join the load balancing cluster. Thus, an attacker may impact the integrity of the flex-vpn system by inserting a rogue cluster member and having the load balance master to forward VPN session to it. A number of secondary effect, including black-holing of some of the VPN traffic may be triggered by this issue.

  Conditions:

  Flex-VPN with Load Balancing feature active

  Workaround: Using CoPP and interface access-list may be used to allow only trusted router to join the load balancer cluster

  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 4.3/3.9: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:P/A:N/E:F/RL:W/RC:C CVE ID CVE-2012-5032 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

Resolved tcp Caveats

- CSCtz14399—Resolved in 15.1(1)SY3

  Symptom: A vulnerability in TCP stack of Cisco IOS Software could allow an unauthenticated, remote attacker to cause an ACK storm.

  The vulnerability is due to improper closing of the established TCP connection. An attacker could exploit this vulnerability by sending a crafted sequence of TCP ACK and FIN packets to an affected device. An exploit could allow the attacker to cause an ACK storm resulting in excessive network utilization and high CPU.

  Conditions: Multiple FIN/ACK packets are received.

  Workaround: Do clear' tcp tcb 0x.....' where the hex value is the address of the TCB stuck in LASTACK state in 'show tcp brief.'

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-2013-5469 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-2013-5469

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

Further Problem Description:

Resolved udp Caveats

- CSCuh09324—Resolved in 15.1(1)SY3

  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.

  Further Problem Description: 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/web/about/security/psirt/security_vulnerability_policy.html

Other Resolved Caveats in Release 15.1(1)SY3

Identifier	Component	Description
CSCsh43036	aaa	ip radius source-int gets NVGEN'ed as ip radius source-int vrf default
CSCug31122	aaa	Workaround fix for VTY hung issues
CSCtw84414	c7600-l2	standby reset due to config sync "monitor session 4 source remote vlan"
CSCul29932	cat6000-acl	15.1(1)SY1
CSCug69230	cat6000-acl	HSRP Packets dropped, on applying inbound ACL with LOG statement / Sup2T

Identifier	Component	Description
CSCuf02993	cat6000-acl	SUP2T active box crashes when reloading the standby because of FM
CSCug04222	cat6000-acl	SUP2T not forwarding unicast DHCP ACK when acting as relay agent
CSCui70455	cat6000-acl	CSCug23641 changes for Earl8 releases (15.1(1)SY (MA2) onwards)
CSCui26454	cat6000-cm	c4mk1: Line card is getting reset while large acl is applied.
CSCuh17586	cat6000-diag	Crash after CF/disk failure due to read/write operations involving SEA
CSCui34949	cat6000-diag	Crash at quad/VS system boot-up if sub card diag monitor config exists
CSCui96441	cat6000-dot1x	IP source guard not updating PACL entry when new DHCP client connected.
CSCue59987	cat6000-energywise	Input queue size becomes negative with energywise enabled.
CSCui68336	cat6000-env	Revisit CSCug29473
CSCuj78044	cat6000-firmware	6716-10G (Hw ver 2.0) may report inlet temperature higher than outlet
CSCui90022	cat6000-firmware	High CPU seen when ingress pkts w/ dMAC of 0000.0000.0000 on 6904 LC
CSCug28934	cat6000-firmware	Incorrect COS Map and Negative Min Threshold in hardware for WS-X6548-GE
CSCui65654	cat6000-firmware	Packets are looped within chassis when WS-X6904-40G is used
CSCul77666	cat6000-firmware	Undersized frames sent with CTS static SGT
CSCui17608	cat6000-firmware	VACL unable to capture the routed traffic on 6500 coming from FWSM
CSCuj83351	cat6000-hw-fwding	Router mac not programmed in L2 table, learned as dynamic
CSCuh24511	cat6000-hw-fwding	Static Mac entries create Config sync issue in VSS on reload of standdy
CSCug75365	cat6000-ipc	Crash in icc multicast code on sup720 from cmfi_process_feature_msgs_int
CSCdy62921	cat6000-l2	Crash after BDPU is mishandled at the interrupt level
CSCuj65447	cat6000-l2-ec	sup2t: crash on cat6k seen if L2 loops exists in network
CSCuh30542	cat6000-l2-infra	Traffic is blackholed when port-channel member flaps
CSCui27472	cat6000-l2-mcast	IGMPv3 leave reports with "Change_to_include" and "sources 0" flooded
CSCul12004	cat6000-ltl	VSL included in L3 vlan flood index when both MEC legs are up
CSCul35053	cat6000-mcast	Crash of active supervisor during ISSU (commit) with multicast enabled
CSCul17734	cat6000-mcast	FE TCAM gets disabled which affects PIM packets
CSCuf21968	cat6000-mpls	6500: SXJ5 no 802.1Q VLAN TAG in vc type 4
CSCug73871	cat6000-netflow	FNF: Multicast First and last packet time stamps are incorrect
CSCug86296	cat6000-netflow	Sup2T: EARL8 Netflow ECC enhancement
CSCui17732	cat6000-netflow	Sup2T: show tech-support hangs VTY session on Netflow TCAM interrupt
CSCui37408	cat6000-netflow	HW inconsistency seen when ingress/egress FNF applied, removed on tunnel
CSCuh78078	cat6000-netflow	C4QUDsup:After 2nd SSO, Reverse traffic is not flowing with ReflexiveAcl
CSCtg67789	cat6000-portsecur	Stdby reloads 'switchport port-security mac-address sticky <> vlan voice
CSCuj83551	cat6000-qos	C2: IPv6 bridge rate limiter support, new feature
CSCuh94242	cat6000-qos	Agg. policer with 'platform qos police distributed' drops all traffic
CSCug26327	cat6000-routing	sup2t : urpf incorrectly drops traffic after vrf is configured
CSCug47095	cat6000-snmp	vlanTrunkPortDynamicStatus is wrong for members of PO
CSCte53717	cat6000-svc	Need to change default SCP keepalive timeout on IOS to ACE module

Identifier	Component	Description
CSCui82742	cat6000-svc	c4mk1: NAM-3 on Standby fails to recover after ISSU load version
CSCuj08631	cat6000-svc	NAM:Accessing span sessions not available through GUI after SSO
CSCug47997	cat6k-vs-infra	C4 ISSU FC3 renamed: After CV, whole quad-sup setup reloads
CSCuj85177	cat6k-vs-infra	catalyst 6500 VSS switch does not come up in SSO after upgrade
CSCun13688	clns	Device crash after "sh clns route" issued
CSCud99034	crypto-ace	ISM-VPN crypto engine encaps fails in 15.3(1.11)T
CSCub56842	crypto-engine	"show cry eli' active IPSec counters keep increasing lead to VPN failure
CSCud87915	crypto-engine	ZBF with IP CEF drops EzVPN traffic to the client when client behind PAT
CSCuf61640	crypto-engine	%SYS-2-INTSCHED seen when calling random_fill()
CSCuj29428	crypto-engine	%SYS-SW1-2-INTSCHED: 'sleep for' at level 2 -Process= "Init"
CSCud54133	crypto-engine	FIPS certification : need continuous random number generator test
CSCua63182	eigrp	EIGRP min BW is calculated incorrectly for ngbrs of varying versions
CSCuc99750	eigrp	EIGRP routes which are not FS making it to the routing table
CSCuh94035	eigrp	Watchdog crash while EIGRP updates Topology Table
CSCud02045	ethernet-cfm	RP crashes after applying cfm mip config to interface
CSCuh40275	fib	Very High SNMP Engine utilisation when polling cefFESelectionTable
CSCui95880	hsrp	HSRP for IPv6 flaps when there is a loop in the network.
CSCtk00976	ifs	File descriptor leak and not getting release - readh FD limit
CSCts34688	ip-acl	Switch crashed due to memory fragmentation "HACL Acl Manager"
CSCue68124	ip-pbr	PBR not work with null0 default route
CSCum95311	ip-pbr	ip next-hop recursive not forwarding traffic
CSCuj27671	ip-tunnels	QUAD SUP2T VSS Failover fails with tunnel path-mtu-discovery config
CSCuc38611	ip-tunnels	TTL of inner header is decremented twice
CSCuj08831	ipc	Crash @ ipc_compare_seats part 2
CSCul22535	ipc	VSS Quad Sup2T IPC failure causes a reload
CSCuj59816	ipmulticast	Auto-RP messages are dropped in a certain scenario
CSCue68761	ipmulticast	Buffer leak @ ip_mforward in 15.1(4)M3
CSCui46593	ipmulticast	CPU hog crash due to Mwheel Process
CSCue93229	ipmulticast	crash when polling ipMRouteEntry during "clear ip mroute"
CSCua44483	ipmulticast	ME3600X suddely stops sending multicast for all groups 151-2.EY
CSCud90983	ipmulticast	OTV Multihome setup: Multicast stop working when shut/no shut join int
CSCud50768	ipmulticast	BSR: Incorrect timer reset for BSR during switchover
CSCuc38120	ipmulticast	OTV: Multicast traffic dropped after shut/noshut of Join Interface
CSCue75986	ipmulticast	XE39: IOSd crash @ mvpn_pim_send_join_periodic
CSCui90139	ipsec-core	ASR1K : Crypto Route not getting deleted on Responder
CSCuc25995	ipsec-core	Crash with %ALIGN-1-FATAL in IPsec
CSCud69442	ipsec-core	crypto map fails after interface flap or ip address change

Identifier	Component	Description
CSCud83835	ipsec-core	crypto map on VT with negotiated ip address fails to initiate VPN tunnel
CSCuc93739	ipsec-core	EzVPN client with split network does not come UP when IPSEC SA is down
CSCud88483	ipsec-core	GETVPN with IPSEC redundancy: Registration failure on standby GM
CSCug28904	ipsec-core	IKEv2 CRYPTO-4-RECVD_PKT_MAC_ERR with peer nonce length 256 Bytes
CSCub26395	ipsec-core	IOS - New VPN dynamic maps not working
CSCue47940	ipsec-core	IPsec MTU has been changed automatically after rebooted
CSCue14418	ipsec-core	L2TP IPSEC NAT DEMUX Functionality is broke
CSCub46423	ipsec-core	L2TP/IPSec: Can not connect to HSRP Virtial IP
CSCtz87485	ipsec-core	MALLOC at interrupt level only when a crypto map configured on a GigE
CSCua35161	ipsec-core	removing tunnel protection doesn't clear up crypto-map on dmvpn HUB
CSCub05907	ipsec-core	RRI isnt propagated after failure of a link, when spoke has dual ISP
CSCuc47356	ipsec-core	RRI route is leaked when unconfiguring the RRI Static
CSCug83538	ipsec-core	RRI Route leaked when map is applied on multiple interfaces
CSCub28997	ipsec-core	segmentation fault @ __be_wavl_do_walk_threaded with IKEv2
CSCud59176	ipsec-core	Backout CSCub95141 in XE37
CSCud42938	ipsec-core	Ident remains at DMAP side even when there are no ipsec sas
CSCue65405	ipsec-core	SAs NOT all active after clear crypto gdoi
CSCug34404	ipsec-core	XE38 : RP_Crash seen @ __be_interface_action_remove_old_sadb
CSCuc36469	ipsec-core	CSR-Crash @__be_crypto_lookup_short_handle during ezvpn tunnel bring up
CSCue77265	ipsec-core	XE39: memory leak in aux_msg_acl_destroy_yourself *
CSCud02391	ipsec-dmvpn	EIGRP routes are not coming up after removing tunnel interface
CSCuc08061	ipsec-dmvpn	DMVPN spoke's crypto session was gone after removing, adding tunnel back
CSCud68178	ipsec-dmvpn	XE39: DMVPN Hub crashed after physical and tunnel interface flapping
CSCue45952	ipsec-ezvpn	"retransmitting phase 2 QM_IDLE" is sent after Phase2 setup
CSCuf51539	ipsec-ezvpn	EzVPN Server- improved resiliance for IKEv1 SA lifetime config to client
CSCuc98855	ipsec-ezvpn	When server sends Savepwd off, client fails to establish EZVPN session.
CSCtu54300	ipsec-getvpn	fn_VRFAwareGM: KS crashed while running getvpn unconfig script
CSCtz78943	ipsec-ha	Crash after configuring a crypto map on a HSRP enabled interface 2
CSCud06887	ipsec-ha	IPSec Stateful Failover - SPIs not replicated after first switch
CSCty26035	ipsec-ha	Multiple issues, while testing ipsec_ha spt, for ha_test_rekey subtest
CSCud69110	ipsec-ikev2	IKEv2:Support IKE_CP_ATTR_SPLIT_EXCLUDE attribute for anyconnect client
CSCue59967	ipsec-ikev2	VPN LED is not on in ISR when IKEv2 tunnel is up
CSCub93442	ipsec-ikev2	FlexVPN Tunnel not coming up when using "ipsec:addrv6 " radius attribute
CSCtu02543	ipsec-isakmp	EZVPN client address leak due to peer overlap (NAT)
CSCud85342	ipsec-isakmp	IKE responder fails to accept RSA-SIG auth if no trustpoints configured
CSCub67774	ipsec-isakmp	IKE: MM6 not re-sent if MM5 retransmitted
CSCue37523	ipsec-isakmp	IOS IPSEC negotiation fails with missing ID pyld in QM1 message (racoon)

Identifier	Component	Description
CSCug63839	ipsec-isakmp	Memory leak seen in CryptoIKMP process(crypto_ikmp_config_send_ack_addr)
CSCua31157	ipsec-isakmp	One way IPsec traffic after initial isakmp contact deletes budding SA
CSCuc31761	ipsec-isakmp	XE3.9 - KS crashes when removing GDOI groups
CSCue44587	ipsec-routing	ASR Missing RRI routes is with active SAs
CSCub94825	ipsec-routing	RRI does not happen in a VRF aware IPSec with stateless HA scenario
CSCub18622	ipsec-switching	Auth proxy on 15.x IOS does not apply DACL on tunnel interface
CSCug38641	ipsec-switching	cTCP IPSec data packets are process switched on EzVPN server
CSCug34507	ipsec-switching	Decrypted traffic is process-switched when tunnel is NAT-T udp-encap
CSCue36387	ipsec-switching	Interface Counters do not increment with IPSEC IPv6
CSCuc94687	ipsec-switching	SHA256 HW crypto support on 890 Platform is missing
CSCub83722	ipsec-switching	Tunnel interface output rate does not increment in a MPLS network
CSCub56064	ipsec-switching	Ping failed after clearing the crypto isakmp and sa with EZVPN client
CSCue45934	ipsec-switching	Return traffic is not coming back in ipv4 session on c6k wit ikev2 MA2re
CSCub74272	ipsec-vti	Crypto Socket goes to closed state causing SA flaps every phase 2 rekey
CSCub89144	ipsec-vti	VTI interface is always in up/up state on HSRP standby
CSCuc51879	mcast-infra	Traffic loss on ASR1K in event of RP SSO switchover
CSCue61691	mcast-vpn	Mroute shows data mdt switchover but MRIB still shows up the default MDT
CSCuh67605	nat	INVMEMINT errors related to NAT max-entries with vrf
CSCuj34455	nat	NAT Process Switches all TCP port 139 Traffic
CSCui94118	nat	static NAT vrf removed upon removal of "vrf definition <vrf_name>"
CSCug18685	nhrp	NHRP resolution request does not follow routed path
CSCud67105	nhrp	VA's are not getting deleted in FlexVPN after clearing cache entries
CSCuc45115	nhrp	Crash seen at nhrp_add_static_map
CSCua46304	nhrp	Seg fault at __be_nhrp_group_tunnel_qos_apply on flapping tunnel
CSCua14640	ntp	Change in order of configuration statement after router reload
CSCuc90999	ntp	CISCO1921 snmp cntpSysPeer does not reset after removing ntp server
CSCui60499	ntp	High CPU from Process NTP with "access-group serve" Configured
CSCuc44629	ntp	NTP crash during bootup
CSCud72473	ntp	NTP: Frequency Errors and Clock Loses Sync with 2 servers
CSCug38011	ntp	router crash after configuring NTP peer
CSCul71047	os	RF Client Cat6k Platform First Client(1319) notification timeout
CSCug33116	os-logging	SUP2T in VSS crashes after reload if "logging origin-id ip" configured
CSCud63381	pas-ipsec	7200: On demand DPDs don't work intermittently causing VPN FO to fail
CSCue39518	pas-ipsec	C7200 : VSA : Encryption Failure with IPSec SSO
CSCud66669	pas-ipsec	VSA: GRE with TP - Packet is not decrypted into the correct ivrf
CSCub17971	pas-ipsec	GETVPN Adv: No re-registration after switching from hw to sw crypto eng
CSCuj09023	pim	On Dialer interfaces pim joins are sent as unicast instead of 224.0.0.13

Identifier	Component	Description
CSCug78098	pim	SUP crash in pimv2_show_rp_hash
CSCty94210	pki	ENH FlexVPN: CERTREQ improvements in IKEv2 exchange
CSCub98357	pki	OCSP validation with disable nonce is causing crashes.
CSCuh80510	sea-log	SEA roll back to the default bootdisk after reload
CSCuj23802	tcp	SUP2T crash after unplug/plug 4 sfp from the WS-X6724-SFP
CSCub36403	tftp	VSS peer reloads for Line-by-Line sync verifying failure
CSCue74612	tftp	Fts Client fails to perform ftp transfer
CSCuj65989	xdr	Active sup in crash due to process "xdr_mcast_set_max_seq_for_transmit"

Caveats Resolved in Release 15.1(1)SY2

Resolved dhcp Caveats

- CSCug31561—Resolved in 15.1(1)SY2

  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

Resolved gsr-boot Caveats

- CSCsv74508—Resolved in 15.1(1)SY2

  Symptom: If a linecard is reset (either due to an error or a command such as hw-module slot reload) at the precise time an SNMP query is trying to communicate with that linecard, the RP could reset due to a CPU vector 400 error.

  Conditions: This symptom occurs when the linecard is reset (either due to error or a command such as hw-module slot reload) at the precise time an SNMP query is received.

  Workaround: There is no workaround.

Resolved ios-firewall Caveats

- CSCtx56174—Resolved in 15.1(1)SY2

  Symptom: A vulnerability in the Zone-Based Firewall (ZBFW) component of Cisco IOS Software could allow an unauthenticated, remote attacker to cause an affected device to hang or reload.

  The vulnerability is due to improper processing of specific HTTP packets when the device is configured for either Cisco IOS Content Filtering or HTTP application layer gateway (ALG) inspection. An attacker could exploit this vulnerability by sending specific HTTP packets through an affected device. An exploit could allow the attacker to cause an affected device to hang or reload.

  Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are not available.

  This advisory is available at the following link:
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130925-cce

Resolved rsvp Caveats

- CSCuf17023—Resolved in 15.1(1)SY2

  Symptom: A vulnerability in the Resource Reservation Protocol (RSVP) feature of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to trigger an interface queue wedge on the affected device.

  The vulnerability is due to improper parsing of UDP RSVP packets. An attacker could exploit this vulnerability by sending UDP port 1698 RSVP packets to the vulnerable device. An exploit could cause Cisco IOS Software and Cisco IOS XE Software to incorrectly process incoming packets, resulting in an interface queue wedge, which can lead to loss of connectivity, loss of routing protocol adjacency, and other denial of service (DoS) conditions.

  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-20130925-rsvp

Resolved ssh Caveats

- CSCto87436—Resolved in 15.1(1)SY2

  Symptoms: In certain conditions, IOS device can crash, with the following error message printed on the console:
  "%SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = SSH Proc"

  Conditions: In certain conditions, if an SSH connection to the IOS device is slow or idle, it may cause a box to crash with the error message printed on the console.

  Workaround: None

  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 6.3/5.5:
  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:S/C:N/I:N/A:C/E:H/RL:OF/RC:C CVE ID CVE-2012-5014 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

Other Resolved Caveats in Release 15.1(1)SY2

Identifier	Component	Description
CSCta92630	aaa	Failing PAC provisioning job does not use updated radius source intf
CSCtx20903	aaa	TACACS authenproblem between CISCO switch - errno 257((ENOTCONN))
CSCub04965	aaa	TCP Session hung causing Packet loss
CSCuc50697	aaa	Exec Authorization fail of session-timeout is greater than 2147483 image
CSCuc59858	aaa	Dynamic-Author should consider src port when detecting retransmissions
CSCue03316	aaa	EoGRE: SSS Manager Segmentation fault/RP reloaded during scale test.
CSCue13913	aaa	Incorrect password used by RADIUS automated-tester after config save
CSCue18133	aaa	[7600] Router crash at show_li_users
CSCue87815	aaa	The secret password in "setup" not saved
CSCuf17296	aaa	ASR1k ISG: Missing Class Attribute in Accounting-Request
CSCuf41477	aaa	TACACS line authorization failed when AV service=shell sent by Tacacs
CSCug24114	aaa	CTS env download failed on non seed device after reboot
CSCug52714	aaa	TACACS Single-Connect request from Switch does not failover to Secondary
CSCug62154	aaa	Mk1: High CPU 100% due to TPLUS with tacacs config
CSCuh43252	aaa	unable to login and high cpu when authenticating with TACACS
CSCuh51556	aaa	Source ip doesn't change when using '[no] ip radius source-interface'
CSCua76157	bgp	BGP routes getting advertised even after removing send-lable from the PE
CSCuc60297	bgp	redistribute VRF route into BGP with global NH does not work
CSCud55286	bgp	On SSO IIF int goes Null & traffic drop,mpvn: 60-90 sec traffic drop
CSCud55354	bgp	BGP_MIB: Incorrect InetAddressType being returned
CSCud79067	bgp	CISCO-BGP-MIB output presented in non-ascending order

Identifier	Component	Description
CSCue28908	bgp	Router may crash with "show ip bgp vpnv4 vrf < >" command
CSCue65006	bgp	MPLS-VPN traffic fails in pure BGP NSR environment
CSCue72839	bgp	BGP link-bw doesn't program traffic share cnt in RT/CEF if soft-in+r_map
CSCue76102	bgp	XE39:IBGP ipv6_redistributed routes not learned in neighbour router
CSCuf09006	bgp	clear ip bgp * soft out or graceful shut on PE purges all routes on RR
CSCuf82179	bgp	BGP routes not cleared from multicast RIB when address-family removed
CSCug09958	bgp	Default ipv6 routes '::/0' turn to ::/16
CSCuf83644	c6k-l3-lisp	LISP: Traffic drop on ITR encap when destined to PETR
CSCug14851	call-home	s72033:Tracebacks seen while doing ISSU from ma2.0 to ma2.b.
CSCue65728	cat6000-acl	SUP-2T--VRF NAT stops working after 24-48hrs into operation
CSCue93721	cat6000-acl	PPTP call not getting conn. when extendable keyword used with static nat
CSCug08012	cat6000-acl	LISP: Encap traffic drops if we unconfigure "ipv4 etr"
CSCug27047	cat6000-acl	Config Sync: Bulk-sync failure due to PRC mismatch in ACL
CSCug34187	cat6000-acl	CSCug23641 changes for 15.1(1)SY (MA2) release onwards
CSCug56779	cat6000-acl	c4mk2:Active sup crashes @ ipnat_l3_fixup
CSCuh57776	cat6000-acl	DHCP binding entry expire
CSCuf81446	cat6000-cm	SUP2T reset w/ Failed TestL3TcamMonitoring w/ high adjacency utilization
CSCuh60848	cat6000-cm	crash@cm_rbacl_replace_req_hdlr while enabling the enforcement
CSCue72286	cat6000-diag	MA2b:Diagnostic handler is not found for DFC card after switchover
CSCuf85528	cat6000-diag	Multiple GOLD tests disable autoboot when HW isn't at fault post failure
CSCug78833	cat6000-diag	Quadsup:online-diag take wrong action on standby-ICA when ICS SUP fail

Identifier	Component	Description
CSCue31621	cat6000-dot1x	MAB fails after 6500 reload when port configured for critical voice vlan
CSCuh03710	cat6000-dot1x	cat6000 dot1x in MDA - IP phone losing connectivity after few minutes
CSCue02511	cat6000-fabric	VSS FPOE incorrect on standby
CSCue11384	cat6000-firmware	Sup2T/15.1SY: WS-X6904-40G fabric OR mask programming is not correct
CSCuh45404	cat6000-ha	C4 4sup: optimize time to notify VSL on switchover
CSCtt42531	cat6000-hw-fwding	Fib Exception only on multiple WS-X6908-10G of Sup2T system
CSCue49346	cat6000-hw-fwding	C6K/Sup2T: LDB Mgr should not preallocate 4K LIF for L3 Subinterfaces
CSCue58387	cat6000-hw-fwding	TCAM Exception State Should Capture Prefix Distribution
CSCuf46062	cat6000-hw-fwding	Sup2T: MAC Address is not synced properly across DFCs
CSCug94630	cat6000-hw-fwding	l3 svi ip address is not reachable with service-policy on mini-trunk
CSCui65190	cat6000-hw-fwding	Incorrect policing behaviour with same policer on multiple interfaces
CSCuh45350	cat6000-ipc	C4 4sup: IPC reinit for LCs in remote chassis take over 2.5 seconds
CSCug90305	cat6000-l2	Power deny of 6148-ge-tx-AF/AT interface with 2602 factory reset
CSCuh33725	cat6000-l2	VSS may switchover when configuring vlans
CSCuf36123	cat6000-l2-infra	VSS Standby crash after renaming vlan
CSCue84185	cat6000-ltl	C4 Quad: Distributed policing fails on switchover and reload peer
CSCue81201	cat6000-mcast	"ip multicast boundary <ACL> in" is blocking outbound multicast
CSCud99759	cat6000-mpls	VPLS over GRE Scheme 2 is not working as expected on DFC /Standby Sup
CSCug39407	cat6000-netflow	Middle buffer leak when netflow with cdp enabled on tunnel interface
CSCuh51188	cat6000-netflow	Big buffer leak when netflow with lldp enabled on tunnel interface
CSCue91216	cat6000-oir	VSS config causing OIR PROCESS HOGGING CPU CREATED THE CRASH
CSCug61801	cat6000-oir	Remove a LC in Quad-Sup and then a SSO could result in VSS freeze
CSCui28066	cat6000-qos	Ant24CR4 and CR3 with AdmiralCR- distributed policing not working

Identifier	Component	Description
CSCue02387	cat6000-routing	removing VRF causes global default route to fail
CSCud18108	cat6000-snmp	CAT6500 SNMP timeouts polling dot1dTpFdbTable
CSCuf60783	cat6000-sw-fwding	Crash seen in adj_switch_handle_fragmentation on changing the MTU size
CSCug42222	cat6000-sw-fwding	VSS VPLS: Core Switch is not forwarding DHCP request received via VPLS.
CSCuf85182	cat6000-wccp	Sup2T after removing WCCP FEATURE_TUN_x interfaces are not removed
CSCug24158	cat6000-wccp	Disable LLDP on WCCP tunnel interfaces
CSCue97597	cat6k-vs-infra	c4ma2b: Switch goes to recovery mode while VSS-->SA conversion after SSO
CSCuf86245	cat6k-vs-infra	Standby does not get to RPR mode with image version mismatch
CSCug23479	cat6k-vs-infra	Switch PMK configured on slot 6 sup not synced to sup on slot 5
CSCuh42552	cat6k-vs-infra	4supsso: optimize vslp swover time
CSCue92705	device-sensor	Address memory leaks in device-sensor for cache delete case.
CSCtg57657	dhcp	Router crash at dhcp function
CSCud95127	eap2	CAT6K crashes when cts change-password procedure is interrupted
CSCub20803	eigrp	EIGRP Wide-Metric: Unknown Delay is added for static routes
CSCud41058	eigrp	ASR / 152-4.S1 / EIGRP does not read route tags
CSCue78192	eigrp	EIGRP not withdrawing routes as a result of specific update/ack sequence
CSCug17808	eigrp	EIGRP not advertisinsg redistributed routes from BGP
CSCug72891	eigrp	EIGRP successor loop results in SIA
CSCug79541	eigrp	extended communities are lost after increasing delay metric in EIGRP
CSCud96882	ethernet-lldp	Buffer leak seen in I/O with lldp_send_update
CSCue25526	flexible-netflow	router crash on fnf
CSCue67873	flexible-netflow	High cpu utilization with Flexible Netflow (FNF)

Identifier	Component	Description
CSCui45414	flexible-netflow	SUP2T crash due to memory corruption with alloc PC related to FNF
CSCuf89251	gold	FEX: 4sup ISSU the new standby crashes due to CHUNKBADFREEMAGIC
CSCuk62206	ip	static arp change not notified to CEF/ADJ
CSCub75883	ip-acl	Access-line numbers are NOT persistant after reload
CSCua99969	ipmulticast	MLD CPU goes high on FHR, RP is located in other router in v6 vrflite
CSCtt96462	ip-tunnels	Packets dropped when CEF enabled under Tunnel interface
CSCua16562	ipv6	OSPFv3 External routes cannot be redistributed into BGP by route-map
CSCua21049	ipv6	ipv6 route 11::1/128 16::1 multicast fails to insert into murib
CSCuc73473	ipv6	IPv6 default route is not redistributed in BGP
CSCuf03079	isis	UEA:IOSd crash is seen during reopt with r-lfa in the RING
CSCue28318	ldap	Router crashes while executing test aaa command with wrong LDAP config.
CSCue85804	lisp	MA2b: Mem Alloc failure msg is seen once on every SSO
CSCug52119	lisp	LISP: existing map-cache entry, BGP route introduced, cef keeps lisp enc
CSCta48521	loadbal	%DATACORRUPTION-1-DATAINCONSISTENCY: copy error
CSCue69214	medianet-metadata	Memory leak @__be_fmd_get_if_fn_buffer on removing MLPPP
CSCud31716	mpls-mfi	Traceback seen after 2nd SSO
CSCtl51688	nat	NAT Error registering with Transport Port Manager - Standby Reload
CSCue36197	ospf	7600 Router Crashes When Exiting OSPF Helper Mode (RFC 3623)
CSCuf61469	ospf	route tag disappears by summary-address in NSSA after route flapping
CSCug23453	ospf	OSPF: route not redistributed due to DBEXIST error message
CSCtr91402	service-routing	Crash in __be_sr_api_vrf_af_deleted when removing vrf definition
CSCty21638	service-routing	Enabling SAF reloads the box setting null Q structure
CSCuc82551	sla	Segmentation fault(11), Process = SNMP ENGINE on ASR1001
CSCee55603	snmp	SNMP ACL does not work for VRF interfaces

Identifier	Component	Description
CSCtx05449	snmp	snmp ifindex persist command gets applied to all the Port-Channels
CSCue80816	snmp	Crash while routine config push through SNMP
CSCug34877	ssh	crash during ssh connections establishment / resume
CSCtb34814	x25	Crash after %DATACORRUPTION-1-DATAINCONSISTENCY

Caveats Resolved in Release 15.1(1)SY1

Resolved aaa Caveats

- CSCtk15666—Resolved in 15.1(1)SY1

  Symptoms: IOS password lentgh is limited to 25 characters.

  Conditions: IOS password lentgh is limited to 25 characters on NG3K products.

  Workaround: N/A

  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/web/about/security/psirt/security_vulnerability_policy.html

Resolved accsw-ease-of-use Caveats

- CSCub55790—Resolved in 15.1(1)SY1

  The Smart Install client feature in Cisco IOS Software contains a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device.

  Affected devices that are configured as Smart Install clients are vulnerable.

  Cisco has released free software updates that address this vulnerability. There are no workarounds for devices that have the Smart Install client feature enabled.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-smartinstall

Resolved ipsec-core Caveats

- CSCua21166—Resolved in 15.1(1)SY1

  Symptoms: Unable to form IPSec tunnels due to error: "RM-4-TUNNEL_LIMIT: Maximum tunnel limit of 225 reached for Crypto functionality with securityk9 technology package license."

  Conditions: Even though the router does not have 225 IPsec SA pairs, error will prevent IPSec from forming. Existing IPSec SAs will not be affected.

  Workaround: Reboot to clear out the leaked counter, or install hsec9 which will disable CERM (Crypto Export Restrictions Manager).

  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 2.8/2.3:

https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:M/C:N/I:N/A:P/E:U/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/web/about/security/psirt/security_vulnerability_policy.html

Resolved ipsec-ikev2 Caveats

- CSCub39268—Resolved in 15.1(1)SY1

  Symptom: Cisco ASR 1000 devices running an affected version of IOS-XE are vulnerable to a denial of service vulnerability due to the improper handling of malformed IKEv2 packets. An authenticated, remote attacker with a valid VPN connection could trigger this issue resulting in a reload of the device. Devices configured with redundant Route Processors may remain active as long as the attack is not repeated before the affected Route Processor comes back online.

  Conditions: Cisco ASR1000 devices configured to perform IPSec VPN connectivity and running an affected version of Cisco IOS-XE are affected. Only authenticated IKEv2 connection is susceptible to this vulnerability.

  Workaround: None.

  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 6.8/5.6:

  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:S/C:N/I:N/A:C/E:F/RL:OF/RC:C CVE ID CVE-2012-5017 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

Resolved mpls-te Caveats

- CSCtg39957—Resolved in 15.1(1)SY1

  The Resource Reservation Protocol (RSVP) feature in Cisco IOS Software and Cisco IOS XE Software contains a DoS vulnerability.

  Cisco has released free software updates that address this vulnerability. There are no workarounds available to mitigate this vulnerability.

  This advisory is available at the following link:
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-rsvp

  Note: The March 27, 2013, Cisco IOS Software Security Advisory bundled publication includes seven 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 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_mar13.html

Resolved nat Caveats

- CSCtg47129—Resolved in 15.1(1)SY1

  The Cisco IOS Software implementation of the virtual routing and forwarding (VRF) aware network address translation (NAT) feature contains a vulnerability 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 this vulnerability. Workarounds that mitigate this vulnerability are not available.

This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-nat

Note: The March 27, 2013, Cisco IOS Software Security Advisory bundled publication includes seven 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 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_mar13.html

Other Resolved Caveats in Release 15.1(1)SY1

Identifier	Component	Description
CSCtc72940	aaa	ip vrf forwarding command not being executed under aaa
CSCty74859	aaa	ISG PWLAN: Memory leaks@ cpf_get_unbundle_pak_buffer with latest image
CSCua01641	aaa	NAS-IP address in Accounting-on packet is 0.0.0.0.
CSCua18679	aaa	Framed-IP-Address is not included in Acct-Start for Dual-Stack sessions
CSCua30053	aaa	Client failing to authenticate with dot1x authentication
CSCua58100	aaa	SYS-2-NOTQ TBs with EAPSIM Roaming at Scale
CSCua83073	aaa	ASR 1000 route processor failure
CSCua85934	aaa	SessProvisioning fail in ISG-SCE interface
CSCub33045	aaa	ASR1k: Memory leak in XE3.6
CSCub69350	aaa	aaa accounting suppress null-username doesn't work with domain-stripping
CSCub91677	aaa	Accounting interim update gets delayed after RP switchover
CSCuc48245	aaa	Impossible to remove vrf command "ip radius source-interface" from conf
CSCty57476	bgp	BGP-GSHUT: Need to support formats NNNN AA:NN
CSCua61330	bgp	NSF traffic loss during switchover for prefixes with BGP learnt NH
CSCua75069	bgp	BGP PIC: Update/Withdraw are not sent correctly

Identifier	Component	Description
CSCua96958	bgp	BGP PIC with confederations require next hop self configuration
CSCub30577	bgp	Incorrect RTs are attached to redistributed routes
CSCub48495	bgp	BGP RTC:BGP RT Filter using route-map causing crash
CSCub70336	bgp	BGP Task crash on bgp hard reset
CSCub73177	bgp	ASR1K crash with Watchdog Process: BGP Router
CSCub78143	bgp	clear ip bgp vpnv4 unicast damp rd cli doesn't clear damp info in VRF
CSCub86706	bgp	XE3.7.1: router crash with BGP HA SSO while switch-over on pE
CSCub92997	bgp	BGP Route Server crashes when GR-supported client session flaps
CSCuc87208	bgp	Router Crashed while configuring 'inherit peer-session'
CSCud03273	bgp	BGP nexthop is not resolved marked inaccessible though route is availab
CSCud70041	bgp	Make BGP NH unchanged for IPv6 LLA
CSCud88983	bgp	<min-holdtime> NOT written in running with default "timers bgp 60 180"
CSCtc60463	c7600-l2	RSP720/Sup720 crash on "traceroute mac <src_mac> <dst_mac>" command
CSCso63807	c7600-mpls	vpn-num is 0 in vlan-ram after moving int to a new vrf
CSCek74844	c7600-snmp	sysObjectID is wrong for 7603-S and 7609-S
CSCue05681	call-home	ISSU XE381->MCP_DEV:Traceback @ fsm_execute_internal after loadversion
CSCub07847	cat6000-acl	High CPU seen on receiving DHCPINFORM on SVI with pbr enabled
CSCuc00098	cat6000-acl	Crash occurs with two Sup2Ts while standby Sup is initializing
CSCuc91306	cat6000-acl	MEM LEAK seen with DHCP SNOOPING on MA1.3
CSCud97653	cat6000-acl	IP device tracking is not working.
CSCue33266	cat6000-acl	SUP2T: DHCP relay not working after configuring secondary IP address
CSCuc02668	cat6000-cfm	Script cat6k_me_cfmosvlanbd_d8_y1731 fails for some 21 TCS

Identifier	Component	Description
CSCuc81745	cat6000-cm	TCAM error for interface with QOS policies
CSCuc67656	cat6000-diag	"show diagn result"causing high CPU issue when bad LC is power down.
CSCub23671	cat6000-dot1x	Authentication loop in dot1x->mab->guest vlan for supplicantless PC
CSCub60449	cat6000-dot1x	Switch starts second authentication after port in guest vlan
CSCud22789	cat6000-dot1x	IGMP joins when port is in auth-fail state not forward to mrouter
CSCua50391	cat6000-env	C6KENV-SW2_SPSTBY-2-MAJORTEMPALARM msg seen in 150-1.IA273.330_120613
CSCub54653	cat6000-env	Many entSensorThresholdNotifications for the Cat6500 down interfaces
CSCub86068	cat6000-env	PCIe error print on console but not log
CSCud41173	cat6000-env	Console problem seen in Mfg side during MA2 software modeling
CSCud53949	cat6000-env	ME-C6524 crashes after "%MLSCEF-SP-4-FIB_EXCEPTION_THRESHOLD:" error
CSCue76640	cat6000-env	No service password-recovery on sup2t doesn't work
CSCud22843	cat6000-fabric	supervisor module crash
CSCud68540	cat6000-fabric	VSS may log 'VSLP Hello Packets dropped'
CSCue18618	cat6000-fabric	Cat6500 not reporting Optical Power Level for X6904 40G Linecard
CSCuc10919	cat6000-firmware	WS-X6904-40G power on leads to control-plane traffic loss on Cat6K
CSCtz53188	cat6000-ha	Multiple Traceback @ ipc_locate_port after switchover
CSCuf20989	cat6000-ha	MA2b: ICS also goes for a reload on sso saying "Active not responding"
CSCsj97387	cat6000-hw-fwding	show mls cef hardware does not honour pager
CSCub46713	cat6000-hw-fwding	Migrating mls rate-limit config to sup2t sets burst size to 1 packet
CSCub82035	cat6000-hw-fwding	C2 4SUP: After triggering Port-Sec err-dis, sh mac-add o/p hangs console
CSCuc76227	cat6000-hw-fwding	SUP2T - packet forward to the wrong dest index
CSCuc43594	cat6000-ipc	VSS NTI_AGENT_STATUS_TIMED_OUT: IPC sessions not cleared on sup failover
CSCua16716	cat6000-l2-ec	Stdby supervisor crashes with PO secondary aggregator

Identifier	Component	Description
CSCty86250	cat6000-l2-infra	Sup2T Failover Changes DLY Value
CSCub72971	cat6000-l2-infra	inrerface resets counter shows 4294967295 after module OIR/switchover
CSCub94484	cat6000-l2-infra	Mem leak is seen in pool_grow_cache
CSCud43211	cat6000-l2-infra	6500 Switch Crash / Port channel configration on SXI3 Image
CSCuc00432	cat6000-l2-mcast	memory leak seen in mcast_etrack_locate_stats
CSCuf34043	cat6000-ltl	C4 Quad: On Z-Switchover remote link is going to UDLD err-disabled state
CSCud67557	cat6000-mcast	MVPN feature not available in advipservices image
CSCud83152	cat6000-mcast	MVPN traffic punted to RP due to misprogrammed MTU
CSCue52637	cat6000-mcast	Multicast traffic blackholed after deleting a vlan
CSCug10856	cat6000-mcast	s72033-ipbasek9:ISSU from ma2.0 to ma2.b old active sp crashes & reloads
CSCue21282	cat6000-netflow	SUP2T I/O Memory Leak Due to CDP
CSCuc84396	cat6000-oir	Missing modules in CISCO-STACK-MIB
CSCud60412	cat6000-oir	reset of the stdby chassis Estelle causes CPU_MONITOR, KPA & VSL msg
CSCsq15198	cat6000-qos	EPC:SRD:RSP720:OSPF/BFD flaps when Gi5/2 (RSP gi link) is no shutted
CSCub81771	cat6000-qos	Revert support to allow multiple ace's in class-map
CSCub93731	cat6000-qos	Cat6K Sup2T crash in QoS policy
CSCuc06115	cat6000-qos	C2-Quad: Aggregate policy programming inconsistent after each SSO
CSCuc28707	cat6000-qos	MLS QoS statistics Export not exporting all statisticS
CSCud36335	cat6000-qos	Certain queuing functionality not configurable in slot 1 cards
CSCud98850	cat6000-qos	Sup2T: Crash when execute sh platform datapath last multiple times
CSCue57638	cat6000-qos	LC 6904 expects priority queue limit in rcv-queue cli
CSCue82604	cat6000-qos	'TCAM label capacity exceeded' may log with low TCAM utilization
CSCua84226	cat6000-routing	LISP: "earl_lif_free_entry failed for LISP0" seen on del router lisp

Identifier	Component	Description
CSCud49596	cat6000-routing	secondary pvlan traffic fails urpf strict check
CSCud96150	cat6000-routing	6500 15.1(1)SY VRF vpn-num misprogammed causes connectivity issues
CSCue03296	cat6000-routing	Build errors due to CSCud49596
CSCue03531	cat6000-snmp	6500-Transceiver/SFP SNMP polling interrupted when changing port config
CSCub65063	cat6000-span	standby sup crashed when "no ipv6 pim rp-address" is configured
CSCub12941	cat6000-svc	Etherchannel of IDSM goes 'W' state after SSO
CSCub94085	cat6000-svc	SXJ: CSM/CSM-S/SSLM modules should be powered down
CSCud15384	cat6000-svc	Vlan-Based Qos fails for Wism module
CSCue06000	cat6000-svc	Boot device statements are lost after reload on a VSS.
CSCuf39348	cat6000-svc	C4MA2B: %OIR-SW1_STBY-3-SOFT_RESET_SSO Error for FWSM on SUP SSO
CSCud16543	cat6000-sw-fwding	IBC TX Freeze on Sup2T with CTS/MACsec
CSCuc31256	cat6k-vs-diag	Sup2T Quad Sup: Active sup crashes and does not recover
CSCub45763	cdp	crash following SYS-2-FREEFREE and SYS-6-MTRACE messages
CSCub72198	config-sync	DUT getting crash while upgrading from Zave-SG7 to Texel
CSCud24601	config-sync	dC4MA2B:ics_cs_nego_open_active_port: ERROR seen on SSO in Quad-SUP
CSCtz74540	cpu	2 Sup VSS - Mistral interrupt on SP : old active remains in RP Rommon
CSCto39849	cts	"cts dot1x" intfs in startup-config lead to long bootup time in VSS
CSCub85948	device-sensor	Memory leak caused by CDP, LLDP or DHCP traffic
CSCub65395	dhcp	Sup720 crashes at dhcpd_forward_reply
CSCud51025	dhcp	DHCP relay crash @dhcpd_relay_remove_info_option
CSCud52349	dot1x-ios	Abnormal role selection when aaa is unreachable from seed device
CSCud62199	eigrp	IOS EIGRP Speaker Fails to Install Routes from ASA Peer after CSCtt17785
CSCtq91063	fib	Crash while fragmenting a tunnel packet

Identifier	Component	Description
CSCub15402	fib	VRF is not getting deleted for a long time.
CSCuc37047	fib	VSS crashes on reconfiguring "ipv6 unicast-forwarding" couple of times
CSCue31321	fib	Crash while running "show ip cef ... detail"
CSCuc19862	flexible-netflow	Flexible Netflow on cellular int cause spurious mem access and CPU HOG
CSCud16764	flexible-netflow	Traceback@ async_fastsend upon reload
CSCud86954	flexible-netflow	Flexible Netflow with DMVPN: Lost cache entry
CSCud71233	ha-ifindex-sync	c4ma2: Notification timer Expired for RF Client: IfIndex(139)
CSCue61332	ha-issu-infra	MA2B : Active sup hangs during boot up after 2nd SSO in IPBASE image
CSCuc54300	ha-red-mode-client	Standby crashes, Notification timer Expired for RF Client
CSCsw74926	idb	show interface <int name> dampening command is broken
CSCtx43599	idb	Backup Interface does not go into backup state
CSCud57852	ifs	c4ma2b: Startup-config is erased when i copy to nvram and reload on ICS
CSCue93416	ifs	c4ma2b: Startup-config is erased when i copy to nvram and reload on ICS
CSCub12694	ip	%SYS-2-INTSCHED: 'may suspend' -Process= "IP SNMP" logs seen
CSCuc88846	ip	Extend Unicast Multitopology Routing (MTR) support to Cat6k
CSCuc93361	ip	"ip" protocol is not accepted in ping command
CSCud94939	ip	IP ICMP debugs needs to print MTU Value
CSCee23195	ipc	Spurious memory access in show ipc queue .
CSCud11731	ipc	c2ma2b: ALIGN-1-FATAL: Corrupted program counter
CSCue55377	ipc	Module (WS-X6816-10GE) crash @ ipc_compare_seats
CSCub17584	ipmulticast	IOSD crash ipmulticast pim when flapping LNS sessions
CSCuc19046	ipmulticast	Crash in pmt_mrib_delete_entry following "clear ip mroute *"

Identifier	Component	Description
CSCuc22217	ipmulticast	PIM Registration Delay after Link Flap
CSCud08166	ipmulticast	ASR1K Crashes on mvrf delete when RP ACL is extended (unsupported cfg)
CSCud36723	ipmulticast	RPF updates not working for IPv6 multicast on t_base_3
CSCtu28696	ip-rip	ASR1k RP exception @ rip_process_mgd_timers on clear ip route*
CSCua91473	ipsec-api	crypto_kmi_add_data_to_pyld memory leak at IPSEC key engine process
CSCuc71706	ipsec-api	show run command runs for minutes
CSCtr45287	ipsec-core	3900 router crashes when the dvti tunnel count reaches 2500+
CSCts08224	ipsec-core	Expected Inspect ACL/Sessions are not found for most of the protocols,
CSCtz50204	ipsec-core	Crash seen while applying "vrf ivrf2" on Server
CSCtz69527	ipsec-core	RRI: Route not found on UUT for RRI testcases
CSCtz94286	ipsec-core	Router with ISM-VPN module requires GRE permit entry on outside ACL
CSCua15292	ipsec-core	router crashed at be_crypto_check_acl
CSCua21201	ipsec-core	RP2 reloaded in 8k tunnel overnight traffic test
CSCua33821	ipsec-core	crypto_acl: CPU utilization shoots up to 99% after config crypto maps
CSCua55423	ipsec-core	"security-association lifetime" not reflected in configs
CSCua78782	ipsec-core	EzVPN Connection down due IPSEC SA nego failure on Inception
CSCub49291	ipsec-core	DMVPN IPv6: Static tunnels failed to build between hub and spokes
CSCub95141	ipsec-core	FP pending message refs on removing 'crypto local-address loopback'
CSCub99756	ipsec-core	ASR1K GETVPN GM uses wrong SPI after rekey until old SA expires.
CSCuc25529	ipsec-core	Incorrect mask being applied when route is added
CSCud03877	ipsec-core	XE371: after volume rekey, ipsec pd flow set soft/hard traffi limit to 0
CSCua45206	ipsec-dmvpn	Hub crashed while removing Stale Cache entry
CSCub10809	ipsec-dmvpn	NHRP commands removed when using EEM script to unshut the interface
CSCuc45528	ipsec-dmvpn	Incremental leaks at :__be_nhrp_recv_error_indication

Identifier	Component	Description
CSCua39107	ipsec-flexvpn	iprib_first_hop not returning NHO route added by NHRP
CSCub07382	ipsec-flexvpn	FlexVPN : Spoke to Spoke : NHRP cache entry expires even with traffic
CSCub20385	ipsec-getvpn	GETVPN SNMP: Rekey failure trap not sent on installation failure
CSCub42920	ipsec-getvpn	GETVPN: KS fails to validate hash in rekey ACK from previous GM versions
CSCub99778	ipsec-getvpn	ASR1K GETVPN GM does not attempt registration after reload interface up
CSCuc77704	ipsec-getvpn	GETVPN Suite-B: esp-sha2-hmac TEK policy not downloaded to COOP-KS Sec
CSCua51991	ipsec-ikev2	Inconsistency for IPSec SA count between IKEv2 and IPSec PI database
CSCuc47399	ipsec-ikev2	IKEv2-Accounting Wrong values in STOP Records when locally cleared
CSCty48712	ipsec-isakmp	DMVPN/EZVPN Hub can't tell difference between endpoints with the same IP
CSCua15759	ipsec-isakmp	IOS crashed in function construct_phase2_hash
CSCua18823	ipsec-switching	DMVPN tunnel on 7200 pltfm encaps packets with TTL=1 on MPLS-VRF setup
CSCub45054	ip-tunnels	OQD Counter issue:Packet Drops seen on mGRE tunnel.
CSCub96618	ip-tunnels	[RLS14]idb creation failed: XDR updates arrived before parser updates
CSCuc39148	ipv6	PPP-Prefix delegatation - IPv6 /128 route not installed to routing table
CSCuc50764	ipv6	Removing ND Prefix doesn't remove the associated connected route
CSCud22222	isis	ISIS IP FRR crash upon interface/neighbor up event
CSCud38297	isis	IPv6 ISIS summary-prefix advertised as inter-area route
CSCud38774	ldap	Router get stuck at 100% CPU while doing scale testing with curl-loader
CSCud89244	ldap	IOS LDAP w/ Win 2008 Server : Intermittent Failure w/ socket write error
CSCts75737	lisp	Traceback @ swidb_if_index_link_identity on standby RP
CSCua37873	mcast-vpn	LSM: MCAST traffic drops at th3 rx PE upon VSS SSO when VSL come back up
CSCub38559	mcast-vpn	MVPNV6:Recursive RPF lookup fails on egress PE w/static route/mroute

Identifier	Component	Description
CSCua18166	medianet-metadata	Need to support sub-app-id
CSCua60785	medianet-metadata	Metadata class-map matches only the first match statement for mediatype
CSCua86620	medianet-metadata	Metadata App-ID for vmware incorrect
CSCud33159	mpls-mfi	C3925: MPLS traffic is Process switched over ATM interface
CSCuc13805	mpls-te	MPLS-TE leak; explicit ID path options; high#failed activation
CSCud71211	mpls-te	reoptimization cleanup delay does not work for path protection
CSCua12396	mrib	MFIB Linecard Sync Fails across stack in IPV6 Multicast Routing
CSCed01880	nat	Not able to configure NAT tcp timeouts beyond 4194 sec
CSCub18395	nat	PAT not working when shut/no shut nat+hrsp config interface
CSCub78079	nat	NAT per VRF: parser fail with route-map applied to static nat
CSCud08682	nat	NAT not translating Traceroute's ICMP Unreachables
CSCud09626	nat	NAT PPTP use_count 1 entry not removed if TCP data segment with FIN flag
CSCud95251	nat	static nat with vrf looses vrf name after nat translations expire
CSCue21223	nat	Intermitant HSRP hellos not sent w/ IP NAT redundancy configured on SVI
CSCua31934	nhrp	Crash seeen at __be_address_is_unspecified
CSCub99216	nhrp	ASR: hub should not fwd resolution req for an authoritative cache entry
CSCub98634	ntp	ntp access-group serve prevent proper client synchronization
CSCud70205	nvram	VSS - Standby Reload when NVRAM accessed from multiple sessions
CSCue81327	oce	C4MA2B : Crash seen while hardware reset on stand-by
CSCud53872	os-logging	ASR1K sends syslogs with the wrong source address after a reboot.
CSCtw65575	ospf	get for ospfv3AreaAggregateTable objects causes router to crash

Identifier	Component	Description
CSCua47056	ospf	Seeing crash in core switch with nsf enabled
CSCub04112	ospf	Quick interface re-configuration causes removal of OSPF routes
CSCub06859	ospf	VSS quad-sup invokes standby down notification on active on switchover
CSCub80386	ospf	OSPF MANET:Mismatched hello parameters experienced with Relay IPv6 Test
CSCuc05728	ospf	7600 OSPF looses "TE MCAST" for mcast route and install it in GRT
CSCud01774	ospf	OSPFv2 : crash on router unconfig
CSCua13273	parser	RP Crash on executing 'show crypto ipsec security'
CSCua97589	parser	No service prompt config command shows incorrect prompt
CSCub83068	parser	Archive config fails if protocol sctp is defined in an IPC zone
CSCud27379	parser	WS-SUP720-3B Crashes due to parser component issue
CSCub88742	pim	MLDPv6 Scale - Ingress PE, SSO twice then flap "mpls mldp" Crash
CSCtz68776	pki	correct OCSP response invalidated due to thisUpdate field in the future
CSCtz81129	pki	OCSP revocation check uses the source interface loopback for destination
CSCua16122	pki	CRL revocation check fails when chain-validation configured
CSCua46153	pki	IOS-CA server at standby device gets disabled during autorollover
CSCua49764	pki	Https created WExp certificate - WExp went to offline after upgrade
CSCua65639	pki	IOS CA Server fails to auto-grant RA CS certificate requests
CSCua93995	pki	Memory leak in PKI-CRL process - negative CRL cache size reported
CSCub91815	pki	Authentication with valid certificate fails on spoke-to-spoke DMVPN
CSCuc08964	pki	IOS PKI server updates CRL even when server is shut down
CSCuc53085	pki	PKI public key cache entries randomly deleted after manual CRL update
CSCuc43794	redundancy-rf	asr903: %PRST_VBL-3-GENERAL: Persistent general error: Is API usable
CSCty44654	ribinfra	router Crash seen with GRE+IPV6+VRF : ipmcast_lib_ipv6_rpf_lookup

Identifier	Component	Description
CSCua98902	ribinfra	Remote LFA FRR support for whales - fibidbnot getting initialized
CSCuc55634	ribinfra	IPV6 static route unable to resolve the destination
CSCud03646	ribinfra	Repair path points to drop adj with remote-LFA after 2nd SSO
CSCsr02168	rsps-time-rptr	Unexpected NO_SYNC when using microseconds precision.
CSCtx45970	rsps-time-rptr	Crash with group scheduling when freq. is not multiple of history interv
CSCuc61817	rsvp	ASR903 crashes @ rsvp_rsb_expiry while removing mpls te tunnels
CSCtg82170	sla	IP SLA destination IP/port config changes over a random period of time
CSCtz13812	sla	2960S can not receive the IP SLA control message from sender
CSCua03037	sla	IP SLA: NumOfRTT & PacketLateArrival incremented for same packet
CSCua54689	sla	Wrong source IP used in path-jitter probe configured in VRF
CSCua80784	sla	Invalid number of IP SLA configurable probes
CSCub47374	sla	Router crashes during IP SLA probe removal/reconfiguration
CSCud11078	sla	MA1.3: Crash observed with auto IP SLA probe for ethernet cfm
CSCua66481	smartoperations	SMI-Image tftp permission is deleted when one group is deleted
CSCuc55547	smartoperations	SMI Startup VLAN is tied to SVI-1's IP for becoming director
CSCth03648	snmp	Pending SNMP Informs builds up and eventually crashes 29xx/37xx switches
CSCts87275	snmp	Cat4k with sup7e : same snmp engineID on different cat4k switches
CSCub80710	ssl	SSL handshake failure with ASR 3.7
CSCud79481	udp	Crash on 6500 on executing "show ip helper address"

Caveats Resolved in Release 15.1(1)SY

Resolved AAA Caveats

- CSCsv06973—Resolved in 15.1(1)SY

  Symptom: Router crashes For Authentication RESPONSE with GETUSER and when getuser-header-flags is modified and sent.

  Conditions: TACACS single-connection is configured. When authorization is configured Telnet to router and removing authorization,telnet to router again

  Workaround: Do not use TACACS single-connection option.

- CSCsv38166—Resolved in 15.1(1)SY

  The server side of the Secure Copy (SCP) implementation in Cisco IOS software contains a vulnerability that could allow authenticated users with an attached command-line interface (CLI) view to transfer files to and from a Cisco IOS device that is configured to be an SCP server, regardless of what users are authorized to do, per the CLI view configuration. This vulnerability could allow valid users to retrieve or write to any file on the device's file system, including the device's saved configuration and Cisco IOS image files, even if the CLI view attached to the user does not allow it. This configuration file may include passwords or other sensitive information.

  The Cisco IOS SCP server is an optional service that is disabled by default. CLI views are a fundamental component of the Cisco IOS Role-Based CLI Access feature, which is also disabled by default. Devices that are not specifically configured to enable the Cisco IOS SCP server, or that are configured to use it but do not use role-based CLI access, are not affected by this vulnerability.

  This vulnerability does not apply to the Cisco IOS SCP client feature.

  Cisco has released free software updates that address this vulnerability.

  There are no workarounds available for this vulnerability apart from disabling either the SCP server or the CLI view feature if these services are not required by administrators.

  This advisory is posted at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-scp.

Resolved IPServices Caveats

- CSCtl59814—Resolved in 15.1(1)SY

  Symptoms: Kerberos/Encrypted Telnet code needs to be improved. There is a potential buffer overflow condition in the code. There is no proof of an attack vector/exploit. However, the code needs to be improved.

  Conditions: Cisco IOS device configured for Kerberos/Encrypted Telnet access.

  Workaround: None

  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 5.4/4.1: 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:U/RL:U/RC:UC 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/web/about/security/psirt/security_vulnerability_policy.html

Resolved Multicast Caveats

- CSCts37717—Resolved in 15.1(1)SY

  Symptoms: Active RP may crash while processing packets. **Conditions:** Device is processing packets which are being punted to the RP at a rate faster than memory can be allocated or deallocated. **Workaround:** Implementing a CoPP policy rate-limiting packets punted to the RP may be a workaround, depending on specific circumstances and traffic pattern **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-2012-1317 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

- CSCtz28544—Resolved in 15.1(1)SY

  Symptoms: Cisco ASR 1000 Series Aggregation Services Routers configured for Multicast Listener Discovery (MLD) tracking for IPv6 may reload after receiving certain MLD packets. The following traceback will be shown in the logs.

  Exception to IOS Thread: Frame pointer 4081B7D8, PC = 1446A878

  ASR1000-EXT-SIGNAL: U_SIGSEGV(11), Process = MLD

  Conditions: Cisco ASR 1000 Series Aggregation Services Routers configured for Multicast Listener Discovery (MLD) tracking for IPv6.

  Workaround: The only workaround is to disable MLD tracking.

  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 6.1/5.8:

  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:U/RC:C

  CVE ID CVE-2012-1366 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

Resolved Routing Caveats

- CSCin14467—Resolved in 15.1(1)SY

  Symptoms: A router may forward IP packets even when IP processing is disabled on the incoming interface.

  Conditions: This symptom is observed on all Cisco routers running Cisco Express Forwarding (CEF).

  Workaround: Configure an inbound access-list denying all traffic on the interface without IP address. Example :

  access-list 100 deny ip any any

  int x no ip address ip access-group 100 in

- CSCti33534—Resolved in 15.1(1)SY

  Symptoms: After launching a flood of random IPv6 router advertisements when an interface is configured with "ipv6 address autoconf", removing the IPv6 configuration on the interface with "no ipv6 address autoconf" may cause a reload. Other system instabilities are also possible during and after the flood of random IPv6 router advertisements.

  Conditions: Cisco IOS is configured with "ipv6 address autoconf".

  Workarounds: Not using IPv6 auto-configuration may be used as a workaround.

  Further Information: Cisco IOS checks for the hop limit field in incoming Neighbour Discovery messages and packets received with a hop limit not equal to 255 are discarded. This means that the flood of ND messages has to come from a host that is directly connected to the Cisco IOS device.

  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 6.1/5.5:

  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-2010-4671 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

- CSCts16133—Resolved in 15.1(1)SY

  Symptoms: Cisco IOS Software on the Catalyst 6500 and 7600 may crash after removing/readding object-group configuration.

  Conditions:

  – Ie: Initial config:

```
object-group ip address foo_obj
  10.1.1.0 255.255.255.0
  10.1.2.0 255.255.255.0
  10.1.3.0 255.255.255.0
  10.1.4.0 255.255.255.0
  10.1.5.0 255.255.255.0
```

  – **Then configure:**

```
no object-group ip address foo_obj
object-group ip address foo_obj
 10.1.1.0 255.255.255.0    <<< Sup may crash here
```

  Workarounds:

  – Workaround is to perform object-group changes in this order:

  • First remove the ACLs which are referencing the object-group

  • Then remove/rebuild the object-group

  • Then reconfigure the ACL

  Ie:

```
config t
no ip access-list extended foo_acl
no object-group ip address foo_obj

object-group ip address foo_obj
 10.1.1.0 255.255.255.0
 10.1.2.0 255.255.255.0
 10.1.3.0 255.255.255.0
 10.1.4.0 255.255.255.0
 10.1.5.0 255.255.255.0
!
ip access-list extended foo_acl
 permit tcp addrgroup foo_obj any log-input
<...re-configure rest of ACL>
```

  Further Problem Description:

  Cisco IOS Software on the Catalyst 6500 and 7600 series contains a vulnerability that could allow an authenticated, local attacker to cause a reload of an affected device.

  The vulnerability issue is due to logic processing in the ACL code. An attacker could exploit this vulnerability by editing the ACLs on the device.

  An exploit could allow the attacker to reload the affected device.

  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 4.6/3.8: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:L/AC:L/Au:S/C:N/I:N/A:C/E:F/RL:OF/RC:C

  CVE ID CVE-2012-5037 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

- CSCtt35379—Resolved in 15.1(1)SY

  Summary Cisco IOS Software contains a vulnerability in the Border Gateway Protocol (BGP) routing protocol feature.

  The vulnerability can be triggered when the router receives a malformed attribute from a peer on an existing BGP session.

  Successful exploitation of this vulnerability can cause all BGP sessions to reset. Repeated exploitation may result in an inability to route packets to BGP neighbors during reconvergence times.

  Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability. This advisory is available at the following link: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-bgp

  Note: The September 26, 2012, Cisco IOS Software Security Advisory bundled publication includes 9 Cisco Security Advisories. Eight of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses a vulnerability in Cisco Unified Communications Manager. 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 2012 bundled publication.

  Individual publication links are in "Cisco Event Response: Semi-Annual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep12.html **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-2012-4617 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

- CSCty58300—Resolved in 15.1(1)SY

  Summary Cisco IOS Software contains a vulnerability in the Border Gateway Protocol (BGP) routing protocol feature.

  The vulnerability can be triggered when the router receives a malformed attribute from a peer on an existing BGP session.

  Successful exploitation of this vulnerability can cause all BGP sessions to reset. Repeated exploitation may result in an inability to route packets to BGP neighbors during reconvergence times.

  Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability. This advisory is available at the following link: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-bgp

  Note: The September 26, 2012, Cisco IOS Software Security Advisory bundled publication includes 9 Cisco Security Advisories. Eight of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses a vulnerability in Cisco Unified Communications Manager. 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 2012 bundled publication.

Individual publication links are in "Cisco Event Response: Semi-Annual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep12.html

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-2012-4617 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

- CSCty89224—Resolved in 15.1(1)SY

  Symptom: IOS router may crash under certain circumstances when receiving a mvpnv6 update

  Conditions: Receive mvpnv6 update

  Workaround: None

  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 6.8/5.6: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:S/C:N/I:N/A:C/E:F/RL:OF/RC:C CVE ID CVE-2012-3895 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

Resolved Security Caveats

- CSCsu73525—Resolved in 15.1(1)SY

  Symptom: Traceroute output becomes incorrect because VSA does not do a TTL decrement on the packet after decryption.

  Conditions: The symptom is observed when configured IPSec with C7200 NPE-G2 VSA.

  Workaround: Disable HW crypto engine - Use VTI

- CSCta79031—Resolved in 15.1(1)SY

  Symptom: If a cert map is changed of added to the trustpoint, the pub key cache for the peers is not cleared. This makes it possible for a client which was connected in the past to reconnect again even if it's cert was banned by the cert map.

  Updated the 'Configuring Authorization and Revocation of Certificates in a PKI' module with notes to indicate - If a certificate map is changed or added to the trustpoint, the public key cache for the peers is not cleared.

  The link to the latest document is: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/15-sy/sec-usr-aaa-15-sy-book/sec-cfg-authentifcn.html

  Workaround: N/A

- CSCth82164—Resolved in 15.1(1)SY

  Symptom: A peer's key is cached indefinitely in the key cache.

  The following messages indicate bypassing the revocation check.

```
*Jul 13 18:43:18.095: ISAKMP:(1002): peer's pubkey is cached
*Jul 13 18:43:18.095: CRYPTO_PKI: Found public key in hash table. Bypassing
certificate validation
```

Conditions: A method (OCSP, CDP, etc.) to check for certificate revocation is used, then it is changed to "none" ("revocation check none"), and finally it gets changed to some revocation method again.

This configuration transition "revocation check -> no revocation check -> revocation check" is what causes a problem.

Workaround: None.

Further Information: The problem is independent of which revocation method is used (OCSP, CDP). The problem will happen when revocation check is disabled with the command "revocation none". This would cache the peer's key infinitely into the cache. After this, turning on any revocation method will have no efect; validation will always succeed since the keys are cached.

The problem will only happen if someone turns off revocation and then later realizes that it was a mistake and turns it back on. If remote peer's key is cached within that period then that cache entry will never be deleted. End Result: If the same remote peer tries to establish the tunnel again we would bypass validation and would not check if it is still a valid peer or not.

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 5.0/4.1:

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

CVE ID CVE-2011-0935 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

- CSCtl59829—Resolved in 15.1(1)SY

  Symptom: Login success and failure messages only display the first 32 bits of the IPv6 source address in IPv4 format.

  Source Address FC00::1

  *Aug 5 19:39:07.195: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: cisco] [Source: 252.0.0.0] [localport: 23] [Reason: Login Authentication Failed - BadPassword] at 19:39:07 EST Wed Aug 5 2009

  Conditions:

  – Telnet or SSH from IPv6 enabled device to IPv6 address on router or switch.

  – Have login success and failure logging enabled.

  ```
  login on-failure log
  login on-success log
  ```

  Workaround: None

  Further Problem Description: The IPv4 address is derived from the first 32 bits of the IPv6 address.

  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:

  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:S/C:N/I:P/A:N/E:F/RL:OF/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/web/about/security/psirt/security_vulnerability_policy.html

- CSCto00318—Resolved in 15.1(1)SY

  Symptoms: SSH session that is initiated from a router that is running affected Cisco IOS software may cause the router to reboot.

  Conditions: Occurs when performing a SSH client session from the router.

  Workaround:

  Do not initiate a SSH session from the device.

  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 4.6/4: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:L/AC:L/Au:S/C:N/I:N/A:C/E:H/RL:OF/RC:C

  CVE ID CVE-2012-4638 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

- CSCtq61128—Resolved in 15.1(1)SY

  Symptom: Router crash with Segmentation fault(11)

  Conditions: It was observed on routers acting as IPSEC hub using certificates.

  Workaround None 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 6.3/5.2: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:S/C:N/I:N/A:C/E:F/RL:OF/RC:C CVE ID CVE-2011-4231 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

- CSCts68262—Resolved in 15.1(1)SY

  Symptoms: Certain SSH version 2 packets may cause a memory leak on a Cisco IOS device configured for SSH. Authentication is needed in order to exploit this vulnerability.

  Conditions: This issue is observed on a Cisco IOS device configured for SSH version 2 after it has received malformed SSHv2 packets. Successful, exploitation may cause system degradation or a partial denial of service condition on an affected device.

  Workaround: The only workaround is to disable SSH version 2.

  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 4/3.6: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:S/C:N/I:N/A:P/E:POC/RL:U/RC:C

  CVE ID CVE-2011-3312 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

- CSCtt28703—Resolved in 15.1(1)SY

  Symptom: VPN client with RSA-SIG can access a profile where his CA trustpoint is not anchored

  Conditions: Use of RSA-SIG

Workaround: Restrict access by using a certificate-map matching the right issuer.

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 3.5/3: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:S/C:P/I:N/A:N/E:POC/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/web/about/security/psirt/security_vulnerability_policy.html

- CSCth99104—Resolved in 15.1(1)SY

  Symptom: Certificate that should not be allowed bypasses validations checks.

  Conditions: This happens when the PKI validation test command is used.

  Workaround: Do not use the PKI validation test command.

  Further Information: The PKI validation test command invokes the pubkey insert api which erroneously adds pubkey entries when at times it should not. this results in all subsequent validations bypassed for the same certificate.

  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 1.7/1.4:

  https://intellishield.cisco.com/security/alertmanager/cvss?target=new&version=2.0&vector=AV:L/AC:L/Au:S/C:P/I:N/A:N/E:F/RL:OF/RC:C/CDP:ND/TD:ND/CR:ND/IR:ND/AR:ND

  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/web/about/security/psirt/security_vulnerability_policy.html

Resolved Cisco IOS Caveats

- CSCta11223—Resolved in 15.1(1)SY

  Symptoms: A Cisco router may crash when the **show dmvpn** or **show dmvpn detail** commands are entered.

  Conditions: This symptom is observed when the device is running Cisco IOS and configured with DMVPN. The crash occurs when the **show dmvpn** or **show dmvpn detail** commands are entered two or more times.

  Workaround: There is no known workaround.

- CSCtc49782—Resolved in 15.1(1)SY

  Symptoms: Upgrade from 12.2(18)SXF6 to 12.2(33)SXH5 introduced additional vty lines to the running-configuration (vtp line 5 - 15). These new lines do not inherit the security ACL or transports configured by the customer on the old lines (0-4). Switch upgrade caused device to be non-compliant with network security policy defined by customer.

  Condition: Software upgrade from 12.2(18)SXF6 to 12.2(33)SXH5.

  Workaround: We have to manually configure the ACL for those newly introduced vty lines.

- CSCtd35382—Resolved in 15.1(1)SY

  Symptom: Smart Install is a plug-and-play configuration and image-management feature that provides zero-touch deployment for new switches. This means that a customer can ship a switch to a location, place it in the network and power it on with no configuration required on the switch.

  When a vulnerability scanner such as NMAP, Nessus, Retina or other is run against the Smart Install port (TCP port 4786) the switch may display some memory error messages such as the following:

```
14w1d: %SYS-2-MALLOCFAIL: Memory allocation of 1633771873 bytes failed from 0x1BB2EE8,
alignment 0
Pool: Processor  Free: 5159776  Cause: Not enough free memory
Alternate Pool: None  Free: 0  Cause: No Alternate pool
 -Process= "SMI IBC server process", ipl= 0, pid= 185
-Traceback= 29AF8E4 29B1E04 29B2068 2C3D198 1BB2EEC 1BB3144 1BB32D4 1BB35E8 1BB1EF0
1B2EDA8 1B25878
14w1d: VSTACK_ERR:
!! smi_socket_recv_read_data : Malloc Failed for msg_data
14w1d: VSTACK_ERR:
!! smi_socket_recv_read_data : Malloc Failed for msg_data
14w1d: VSTACK_ERR:
```

These messages do not cause any operational impact to the affected device (switch).

Conditions: Switch configured with the Smart Install feature (client or director).

Workaround: In Smart Install implementations the client switches are served by a common director. The switch selected as the director provides a single management point for images and configuration of client switches. hen a client switch is first installed into the network, the director automatically detects the new switch, and identifies the correct Cisco IOS image and the configuration file for downloading.

Switches that are clients have the Smart Install feature enabled by default and it cannot be disabled. The only way to workaround this issue is to apply an access control list (ACL) blocking TCP port 4786, if smart install is not needed.

- CSCtd95386—Resolved in 15.1(1)SY

  Symptom: An IPSec tunnel can be torn down if the router receives a replayed QM (Quick Mode) packet.

  Conditions: This is only a problem when a replayed QM packet is received on an IPSec endpoint.

  Workaround: None at this time.

- CSCtg09360—Resolved in 15.1(1)SY

  Symptom: Dot1x or port-security violation with RSPAN configured was observed.

  Conditions: RSPAN should be configured.

  Workaround:

  – Disable RSPAN

  Or

  – For Dot1x - change dot1x authentication mode on interface to multi-host

  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 2.9/2.9: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:A/AC:M/Au:N/C:N/I:P/A:N/E:H/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/web/about/security/psirt/security_vulnerability_policy.html

- CSCti54173—Resolved in 15.1(1)SY

  Symptoms: A Cisco7200 w/VAM2 2 configured for GETVPN may experience a memory leak for every packet that is fragmented at high CPU. This may cause system stability and the device to potentially reload. These packets are received from a trusted and configured GETVPN peer.

  Conditions: The symptom is observed on a Cisco 7200 series router.

  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 4.9/4: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:H/Au:S/C:N/I:N/A:C/E:F/RL:OF/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/web/about/security/psirt/security_vulnerability_policy.html

- CSCti99869—Resolved in 15.1(1)SY

  Symptom: Middle buffer iomem leaks seen with dhcp snooping in relay agent environments alongwith the following error messgaes (error messages are seen when the free iomem goes very low and is unable to service a request for a buffer from it)

  %SYS-2-MALLOCFAIL: Memory allocation of 1748 bytes failed from 0x42275FC0, alignment 32 Pool: I/O Free: 1264736 Cause: Memory fragmentation Alternate Pool: None Free: 0 Cause: No Alternate pool -Process= "Pool Manager", ipl= 0, pid= 9

  Conditions: DHCP snooping configured on the switch and snooping is operating in a relay agent environment. Problem is seen in 12.2SXI-12.2SXI4.

  Problem not present in 12.2SXF, 12.2SXH, 12.2SRC,SRB,SRD based releases

  Workaround: Force process switching of software switched packets on the dhcp server facing interface on the cat6k by configuring the no ip route-cache command on the router facing interface.

  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/web/about/security/psirt/security_vulnerability_policy.html

- CSCtj90091—Resolved in 15.1(1)SY

  Symptom: When an ICMPv6 ACL is applied to an interface on PFC3C system, fragment entry may not be created in TCAM.

  Conditions: None

  Workaround: No workaround

  Further Problem Description: None

  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 5/4.1: 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:F/RL:OF/RC:C CVE ID CVE-2011-4012 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

- CSCtj95182—Resolved in 15.1(1)SY

  Symptom: When using a network scanner to check the network components if there have security issues or are woundable on a 3750, it apears that CPU goes high and there is a memory leak in SMI IBC server process

  Conditions : Network scanner run on a 3750 running 12.2.55.SE

  Workaround: None

- CSCtk54650—Resolved in 15.1(1)SY

  Symptoms: After modifying the IPv6 ACL it can happen that some lines in the ACL get multiply indefinitely. Once we try to save such a config it will generate the following error:

  ```
  %SYS-SP-4-CONFIG_NV_NEED_OVERRUN: Non config data present at the end of nvram
  needs to be overwritten to fit the configuration into nvram
  ```

  and the VTY line will hang.

  Reloading the box in this state will result in empty configuration.

  Conditions: Modifying the IPv6 ACL

  Workaround: Remove and reapply the ACL

  Further Problem Description: Upgrade to a release that has Cisco Bug ID: CSCts16133 integrated.

- CSCtl88673—Resolved in 15.1(1)SY

  Symptom: Enhancements to GDOI processing

  Conditions: N/A

  Workaround: N/A

- CSCtn22376—Resolved in 15.1(1)SY

  Symptoms: A memory leak occurs when processing specific packets, when ikev2 debugging is enabled.

  Conditions: ikev2 debugging must be enabled

  Workaround: Disable ikev2 debugging.

  Further Problem Description: None.

  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 5/3.9: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:N/C:N/I:N/A:P/E:POC/RL:OF/RC:C CVE ID CVE-2012-0360 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

- CSCto10165—Resolved in 15.1(1)SY

  Summary A vulnerability exists in the Smart Install feature of Cisco Catalyst Switches running Cisco IOS Software that could allow an unauthenticated, remote attacker to perform remote code execution on the affected device.

  Cisco has released free software updates that address this vulnerability.

  There are no workarounds available to mitigate this vulnerability other than disabling the Smart Install feature.

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-smart-install.

- CSCto72927—Resolved in 15.1(1)SY

  Symptoms: Configuring an event manager policy may cause a cisco Router to stop responding.

  Conditions: This issue is seen when a TCL policy is configured and copied to the device.

  Workaround: There is no workaround.

- CSCtq36327—Resolved in 15.1(1)SY

  Symptom: A loop between a dot1x enabled port and another a)dot1x enabled port configured with open authentication or b) non-dot1x port, will create a spanning-tree bpdu storm in the network.

  Workaround: Avoid creating a loop.

  Further Problem Description: This is a day-1 issue and the fix is available in SXI7, SXJ2 and MA2.

  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 6.1/5.8: 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:U/RC:C CVE ID CVE-2011-2057 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

- CSCtt03207—Resolved in 15.1(1)SY

  Symptom: Traffic flows through unauthorized supplicant switch

  Conditions: Authenticator Switch should have established auto-config with authorized supplicant switch. Now bring up, unauthorized supplicant switch by physically connecting to hub placed between ASW & SSW. Though wrong dot1x credential is used, ASW allows network access for unauthorized SSW.

  Workaround: None

  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 2.9/2.4: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:A/AC:M/Au:N/C:N/I:P/A:N/E:F/RL:OF/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/web/about/security/psirt/security_vulnerability_policy.html

- CSCtt16051—Resolved in 15.1(1)SY

  Cisco IOS Software contains a vulnerability in the Smart Install feature that could allow an unauthenticated, remote attacker to cause a reload of an affected device if the Smart Install feature is enabled. The vulnerability is triggered when an affected device processes a malformed Smart Install message on TCP port 4786.

  Cisco has released free software updates that address this vulnerability. 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-20120328-smartinstall

- CSCtw80533—Resolved in 15.1(1)SY

  Symptom: Error message in the logs: %SYS-4-CHUNKSIBLINGSEXCEED: Number of siblings in a chunk has gone above the threshold. It is a result of a slow memory leak.

  Conditions: Observed on ASR1000 running 15.1(2)S when polling crypto statistics

  Workaround: Avoid stressing the box with multiple SNMP requests. Reload if the memory is completely depleted.

- CSCty90293—Resolved in 15.1(1)SY

  Processing Improvements for GREv6 over IPv6 Currenlty requires IP CEFv6 to be disabled

  Workaround: use "tunnel protection" instead

- CSCty96049—Resolved in 15.1(1)SY

  Summary Cisco IOS Software contains a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. An attacker could exploit this vulnerability by sending a single DHCP packet to or through an affected device, causing the device to reload.

  Cisco has released free software updates that address this vulnerability. A workaround that mitigates this vulnerability is available. This advisory is available at the following link: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-dhcp

  Note: The September 26, 2012, Cisco IOS Software Security Advisory bundled publication includes nine Cisco Security Advisories. Eight of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses a vulnerability in Cisco Unified Communications Manager. 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 2012 bundled publication.

  Individual publication links are in "Cisco Event Response: Semi-Annual Cisco IOS Software Security Advisory Bundled Publication" at the following link: http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep12.html

  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-2012-4621 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

- CSCte83104—Resolved in 15.1(1)SY

  Conditions: When an ipv6 RACL is confiured on an interface. All packets containing ipv6 optional headers are punted to RP. But if any packets that are sent with no L4 header are also hitting this punt entry present at the top of tcam.

  Workaround: No Workaround:

- CSCtr88193—Resolved in 15.1(1)SY

  Symptom: Either High CPU or Crash resulting from large number of ipv6 hosts.

  Conditions: This has been seen while sending Multicast Listener Discovery packets with IPv6 and mld snooping enabled.

  Workaround: none

  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-2012-3062 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

- CSCtq39602—Resolved in 15.1(1)SY

  Symptom: DMVPN Tunnel is down with IPSEC configured. The show dmvpn from Spoke shows the state is IKE.

Conditions: After heavy traffic was pumping from DMVPN Hub to Spoke for some time, from a few minutes to a couple of hours.

Workaround: Configure “set' security-association lifetime kilobytes disable” to disable volumn based rekeying will reduce the problem.

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-2012-3915 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

- CSCtz02622—Resolved in 15.1(1)SY

  Symptoms: FlexVPN spoke crashed while passing spoke to spoke traffic.

  Conditions: Passing traffic from spoke to spoke or clearing IKE SA on the spoke

  Workaround: None

  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:N/AC:L/Au:M/C:N/I:N/A:C/E:F/RL:OF/RC:C CVE ID CVE-2012-3893 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

Other Resolved Caveats in Release 15.1(1)SY

Identifier	Technology	Description
CSCec79136	—	Crypto Isakmp key adds subnet /24bits
CSCef95765	—	RIP offset-list interface option not saved in AF VRF context
CSCsg78501	—	IKE should not delete established tunnel upon RSA key regeneration
CSCsj19194	—	SP crashes after %PM-3-INTERNALERROR due to switchport flapping
CSCsj38112	—	High CPU due to interrupts on WS-X6704-10GE
CSCsk29975	—	Tunnel not up, invalid local address after modify the local address .
CSCsk62032	—	DHCP snooping support to detect rogue dhcp servers
CSCsm63524	—	SUP32 crashes due to SP hang when it recovers from errdisable
CSCsm70924	—	Radius accounting STOP contains zero output for short sessions, on C10k
CSCso63459	—	Unallowed RADIUS attributes in CoA Ack/Nak in LI cases
CSCso93708	—	IPsec-HA:RFclient timingout on7200 running 12.4(15)Tx, AdvSecurity fse
CSCsq15994	—	C10K BBA: Low CPS seen with all PPPoA, PPPoE sessions
CSCsu01846	—	Authentication Per Realm with VRF fails on HA4.0
CSCsu29301	—	C2W21: Ingress SPAN on Sup - ACE module duplicates packets
CSCsu84927	—	c2w2:allow DIVC to negotiate red mode when matrix overide check is yes

Identifier	Technology	Description
CSCsu92000	—	Inconsistency in configurations on a secured port with aging timer
CSCsv20595	—	An invalid input detected error message on bootup
CSCsv21770	—	PAC re-provisioning fails, AAA generates endless number of Prov Requests
CSCsv24908	—	L2 Fwd Broken on other modules when int flaps
CSCsv36306	—	BFD: Removing BGP on the router makes the neigh router crash
CSCsv63040	—	EzVPN server does not apply group attributes when per-user attr present
CSCsv80230	—	Red zone block overruns & mallocfails lead to LC and stby RP crashes
CSCsv82285	—	Cat6k: UDP port 10000 is opened by default
CSCsv90904	—	Cat6k: UDP port 2228 is opened by default
CSCsv97424	—	router crashes due to memory corruption in IO pool running 12.4(22)T
CSCsw89720	—	CPU-HOG error messages are seen when we query cbQosPoliceStatsTable.
CSCsx08671	—	Service Logon for subnet session is failing
CSCsx24934	—	CPU Monitor not heard and ipc TBs on Active VSS switch on issuing Reload
CSCsx56011	—	Switch may crash when issuing "show mac-address-table"
CSCsx62864	—	GETVPN: GM reloads while crypto map is removed and re-applied to interfa
CSCsx66105	—	GET_VRF::Chunk memory leak at "SADB SA Header" for clear crypto gdoi
CSCsy69914	—	Some lines are omitted when Copy and paste of TCL script in TCL shell
CSCsy82679	—	Memory leak at fh_dup_policyQ_for_nvgen when using a policy description
CSCsy89677	—	"% Ambiguous command" returned in the TCLSH for all commands
CSCsy89795	—	ASR1K: IOSd crash after running clear counters
CSCsz00865	—	GETVPN: cannot configured loopback as registration interface
CSCsz12460	—	Cron timer may execute EEM policies twice in the same minute
CSCsz29564	—	Traffic loss between ASR and IOS GM if IOS GM missed REKEY.
CSCsz86894	—	GETVPN: %CRYPTO-4-RECVD_PKT_MAC_ERR: does not print src and dst IP's
CSCta02570	—	IPSec dVTI: iosd crash at crypto_ipsec_clear_cryptomap_sas during PBR dv
CSCta17587	—	VRF + RHI combination does not work on FWSM
CSCta20590	—	GETVPN: GM pseudotime [TBAR] gets desynchronized after re-registering
CSCta22746	—	ASR1k: RP crashes at crypto_ipsec_delete_sibling_sas()
CSCta23902	—	DMVPN P3: seeing pkt drops due to Type: incomplete entry in NHRP Cache
CSCta25824	—	Normal Buffers Leaking
CSCta27279	—	WCCP s/w switching with Ingress redirection & interface ACL
CSCta30298	—	CHKPT-SP-3-NOMEM: Memory leak seen and later the box crashed
CSCta32902	—	IPSEC HA should support the "set nat demux" option on the crypto map
CSCta32922	—	SP crash due to heartbeat failure.
CSCta50110	—	GETVPN1.4::GM does not register if crypto map is applied to only tunnel
CSCta55574	—	Once in a while catalyst fails to apply to proxyACL with auto mac-check
CSCta56305	—	Detector data port operation status not OK after boot

Identifier	Technology	Description
CSCta93316	—	Memleaks are seen in Coop testing
CSCta94179	—	Recirculated MPLS packets becasue of egress service policy are dropped
CSCta95295	—	IOMEM depleted when PKI servers unavailable for CRL checking
CSCta97714	—	%SYS-2-SHARED: Attempt to return buffer with sharecount 2
CSCta98108	—	With NAT, on Netflow database cleanup timer expiry, CPU spikes on 7600
CSCtb05792	—	sh event manager environment all displays only 30 chars for variables
CSCtb13421	—	KS registration fails if one of the gdoi interfaces on GM is down
CSCtb28712	—	SPAN Reflector not enabled for WS-SVC-ADM-1-K9
CSCtb42862	—	GETVPN_SCALE: GM 3845 router crashed due to illegal memory access
CSCtb43009	—	GETVPN_SCALE: GM 3845 router crashed when key server removed from list
CSCtb49373	—	Route Watch Does Not Notify Client for one route loop
CSCtb50678	—	Crash @ registry_add_case with VSS when change from RPR to SSO
CSCtb55858	—	No qos rewrite on untrusted port in SXI2
CSCtb56183	—	ASR does not use the lowest MTU for crypto SA after reboot
CSCtb56607	—	GETVPN: GM does not perform PMTUD correctly with TBAR
CSCtb58724	—	GETVPN: to commit additional seqnum/PST checking code
CSCtb60330	—	VTI: Missed DPD ACK on phase 1 expiry causing phase 2 deletion.
CSCtb65406	—	QoS ACL May Not Program L4 ports Correctly In TCAM
CSCtb66273	—	EZVPN+DVTI: Ping through EZVPN tunnel fails with Split-tunneling
CSCtb74547	—	DMVPN- ASR1k reloads at process IPSEC key engine
CSCtb76774	—	IPSec does not handle PMTU updates properly
CSCtb76775	—	QoS on NM-1A-T3/E3 + NME-IPS Promiscous mode causes large IO mem leak
CSCtb87454	—	DHCP Rogue Server Detection
CSCtb89745	—	RRI breaks when devices are running in HA pair
CSCtc02012	—	GETVPN: KS sends port 500 in his ID payload instead of 848
CSCtc03011	—	GETVPN KS Crash in unicast_rekey
CSCtc04351	—	RP Crashes @ crypto_ipsec_process_gdoi_multicast_rekey
CSCtc06486	—	VTI: Headend routes are removed when ezvpn client reboots and reconnects
CSCtc06629	—	crash/tracebacks seen @ crypto_ident_count_ipsec_sas_to_peer
CSCtc17058	—	VC stops sending traffic due to duplicate vpn id in port based EoMPLS
CSCtc17083	—	Tunnel decap not programmed, hence traffic RP switched
CSCtc17162	—	Ezvpn - SegV crash at ikmp_profile_vrf_set while clearing int dialer 0
CSCtc32207	—	Need better accuracy in RP crash reporting
CSCtc38771	—	12.2SXH: Intermittent BPDU drop over Dot1Q tunnel.
CSCtc38905	—	Disabling IPv6 MLD Snooping breaks IPv4 IGMP and PIM Snooping
CSCtc39052	—	svclc module command adds firewall module command to configuration
CSCtc39592	—	Classification is broken after applying crypto on ATM PVC bundle

Identifier	Technology	Description
CSCtc40420	—	Basic packet forwarding failed when GRE tunnel is configured
CSCtc52655	—	GetVPN KS/GM report sequence number failures after several weeks
CSCtc53375	—	C2W2B : pagp_switch_sp2mp:idbman_update_mp_delete_agport
CSCtc54878	—	NDE direct export packets are checked by egress ACL
CSCtc67457	—	ASR1k - RP2 Crash seen on process Crypto IKMP with getvpn vrf-lite
CSCtc70462	—	port-security Line-by-Line sync verifying failure
CSCtc71996	—	SSO : Bulk-sync failure at "ip flow-export source"
CSCtc72699	—	OSPFv3 neighbor cannot be established by using IPSec authentication.
CSCtc73441	—	CPUHOG in GETVPN Key Server when doing "show crypto gdoi ks members"
CSCtc78951	—	C2W2C: port's not recovering from "s" state with non-default native vlan
CSCtc87183	—	Crash by bus error in software with adjacency errors
CSCtc88424	—	Could not set values for certain 3G OIDs
CSCtc90469	—	Supervisor module crashes just after boot up with ACL Deny Test Failure
CSCtc95423	—	RLS6:ASR RP crash observed @ ipsec_bug_main during config/unconfig
CSCtd11886	—	Memory leak was observed at Hub at "nhrp_forward" function
CSCtd13970	—	'ip cef accounting per-prefix non-recursive' breaks hw-based PBR
CSCtd17586	—	Kron policy cli show tech removed from configuration after occurrence.
CSCtd18573	—	EARL-SPSTBY-2-SWITCH_BUS_IDLE: & PF_ASIC dump with 'clear mls qos'
CSCtd27511	—	Crypto map on a tunnel interface with vrf, sadb in global table
CSCtd27768	—	CISCO-ENTITY-FRU-CONTROL-MIB reports missing module 12.2.(33)SXI2a
CSCtd49232	—	rx packets dropped on protected GRE tunnel in a vrf in MPLS/VPN setup
CSCtd55638	—	Standby Getvpn hsrp router tries to register with key server and fails
CSCtd59027	—	Crypto crash in association with EzVPN client disconnection
CSCtd60194	—	Global MLD snooping disable does not reset snoop condition registers
CSCtd61443	—	GETVPN Key Server may crash after modifying group ACL
CSCtd62858	—	Standby resets due to Event Manager client timeout during SSO switchover
CSCtd68627	—	memory leak @ ikev2_profile_set_laddr
CSCtd68951	—	Crash occurs as a flurry of ingress IKEv2 sessions begin
CSCtd69074	—	VSS: No resv vlan assigned after del-add VRF after SSO.
CSCtd74965	—	DSCP marking on VTP packets needs to be changed
CSCtd75076	—	EzVPN: Client might initiate double renegotiation causing tunnel to fail
CSCtd92196	—	show crypto maps cmd lead to Unexpected exception to CPU: vector 1400
CSCtd92821	—	SSH + SSO crashes with large RSA keys
CSCtd94789	—	PFS setting not used for the dynamic crypto map on standby HA for rekey
CSCtd94947	—	Multicast traffic breaks crypto engine
CSCte01303	—	KS Policy Change not allowed on new Primary KS after a failover
CSCte05199	—	EEM syslog event detection failure due to logger queue getting full

Identifier	Technology	Description
CSCte08785	—	mac notification change history log not seen for deleted mac entries.
CSCte14561	—	L2 port's mac-address is not same as the BIA after reload
CSCte19413	—	EzVPN on sub-interface doesnt come up after reload
CSCte19478	—	crypto isakmp xauth timeout doesn't seem to work
CSCte20914	—	SPAN Reflector not enabled for WS-SVC-ADM-1-K9 : 2nd Commit
CSCte37412	—	after deleting isakmp profile and certificate-map, cert-map still in use
CSCte39051	—	EzVPN NEM VTI with secondary IP address fails to send primary ip route
CSCte40472	—	FWSM: Private vlan association not syncing on VSS systems from switch
CSCte42041	—	DMVPN crypto socket stuck on peer router
CSCte65688	—	"Client_type=CISCO_SW_VPN_CLIENT" should show up instead of "—"
CSCte72214	—	ME6500 - Traffic may be dropped on applying cos-map.
CSCte74909	—	Modifying crypto ACLs causes crash
CSCte78562	—	Regexp action may generate %SYS-2-BADFREE
CSCte81230	—	IP Source Guard feature goes into an incorrect state
CSCte83779	—	dmvpn2mpls:mgre interface cleanup causes iosd crash
CSCte85669	—	qos state in TM = 0 and QM = 1 is different msg on toggling qos
CSCte90261	—	6500 PoE issues with 1120 and 1230 line of APs when using dot1x
CSCte90427	—	In-correct\>Mis-leading **%CRYPTO-6-IKMP_NO_PRESHARED_KEY:** Message
CSCte90818	—	MPLS Label to GRE traffic stops on toggling 'mls mpls tun-recir'
CSCte91203	—	Bus error crash when executing 'show crypto sessions'
CSCte94156	—	ASR1k TBAR does not update PST upon GM Re-Register
CSCte97511	—	IKEv1-PKI non-blocking Interaction
CSCtf13942	—	GETvpn manual certificate import deletes ISAKMP SA
CSCtf15479	—	VSS: TestMatchCapture failure causing Sup Minor error after manual failo
CSCtf16330	—	DHCP Rogue Server Detection : Multiple DHCPDISCOVER's issue
CSCtf18061	—	Modify warning message when removing "crypto ipsec client ezvpn"
CSCtf25141	—	Mem leak seen msc_create_met_set, msc_update_met_set & hal_send_met_job
CSCtf26923	—	Error reading DOM printed when configured L2 port on non DOM capable LC
CSCtf36117	—	Crash occurs on executing 'Show crypto session brief'
CSCtf39056	—	RRI routes not deleted
CSCtf41721	—	Dmvpnv6 hub crashes @ ifs_lookup_prefix_common
CSCtf42209	—	show crypto ipsec sa count displays incorrect SA counts
CSCtf43071	—	IBC crash - seen on 2960 and 3560v2
CSCtf45755	—	EEM software forced crash when unregistering an applet if poll-interval
CSCtf48179	—	AH drops - Bad IP header checksum with ah-md5-hmac transform-set
CSCtf50155	—	CDP neighbors aren't seen on layer2 subinterface
CSCtf51541	—	System controller reset due to TM_DATA_PARITY_ERROR error

Identifier	Technology	Description
CSCtf52407	—	Sup720 may reload when passing GRE traffic
CSCtf53433	—	Knob 'platform ipv6 acl punt extension-header' default should be false
CSCtf56107	—	Software forced crash
CSCtf61757	—	4sup: Power to module in slot 7 set off (Module Failed SCP dnld)
CSCtf70959	—	ip address check on dialer intf does not complete before initiating ezvp
CSCtf71010	—	Trafic doesnt flow through HUB(3900) in vrf aware tunnel protection
CSCtf79637	—	3750X -- VSTACK_ERR: smi_ibc_dl_handle_events : invalid messag
CSCtf83906	—	W2.Clix: after apply/remove/re-apply v6 ACL's, TCAM full
CSCtf83910	—	Event Manager SNMP action snmp-trap incorrectly nvgens
CSCtf87039	—	Device crashes in crypto_ikmp_process_xauth_reply
CSCtf91692	—	Insertion of 6708/6716 linecard into the chassis resets another linecard
CSCtf93876	—	"sh plat hardware capacity multicast" does not work after switchover
CSCtg01020	—	IPSec tunnel fails to establish on ASR due to invalid SPI (SPI leak)
CSCtg08496	—	After merge KS deletes all GMs, send rekey fails and all GM reregister
CSCtg08509	—	Failed to decrement IPSec Client connection
CSCtg09000	—	GETVPN - Old SAs not cleared on GM after modifying ACL on KS
CSCtg09619	—	Web Auth host gets dropped after DHCP renewal with DHCP snooping enabled
CSCtg11344	—	PPPoA sessions fail to sync up with stand-by after SSO in a scaled setup
CSCtg17979	—	vs_ltl_set_ucast_source_indices slot 19 num_ports 8 fail msgs on bootup
CSCtg19546	—	Incorrect TAG ADJ post encap on tunnel interface
CSCtg30383	—	vif int address change causing vlan/vpn programming mismatch in sp
CSCtg32797	—	c6k long failover issue with multicast MVPN
CSCtg41606	—	RRI configuration drops egress traffic due to incomplete adjacency
CSCtg42904	—	Crash in fnf_cache_unlock_entry_internal when apply FNF to EasyVPN
CSCtg44108	—	informer Bus error bad pointer crash in ipsec
CSCtg50024	—	Router crash in NHRP multicast packet replication due to freed pointer
CSCtg50990	—	6500 DHCPv6 relay does not forward on layer 3 vlan interfaces.
CSCtg54691	—	Met2 is not programmed when p2p gre tunnel is IIF for service reflect gr
CSCtg55338	—	Crypto socket not created after a reload on GRE interface
CSCtg55435	—	"show crypto route" unusable with clients using multiple subnet support
CSCtg55447	—	Secondary KS TEK Seq number out of synch after primary KS failure
CSCtg60424	—	Fast-UDLD:Some ports connecting to VSS stby getting err-disalbed on boot
CSCtg62986	—	A Cisco router may crash reporting a software forced crash
CSCtg65763	—	"Clear crypto gdoi" on KS does not clear the KS Policies
CSCtg75452	—	SDH POS VC-4c interface config replace to base config causes RP crash
CSCtg76885	—	ISR drops encrypted fragmented packets failing post decrypt checking
CSCtg79262	—	EEM: policies can get stuck in the active queue

Identifier	Technology	Description
CSCtg79692	—	W2C: Multicast traffic duplicated when OIR card comes back up
CSCtg92327	—	MET entries are not deleted properly
CSCtg93243	—	QOS+Crypto::Tunnel Protection on VSA is broken with 15.0(1)M2.8
CSCtg94316	—	IKE SA does not rekey after lifetime expires with DPD & active IPsec SA
CSCtg95940	—	dh-group2 KE generation fails in the following scenario.
CSCtg98525	—	ISSU MLS MSC Client(6036) incompatible while issu btn SXI2a->SXI4.FC2
CSCth04998	—	[VSS] DFC installs drop index for MAC-address
CSCth05533	—	memory leak in IPSEC key engine
CSCth12206	—	6500 with 12.2(33)SXI3 May Not Forward Multicast With SLB Configured
CSCth15109	—	Flowmask conflict between "Intf full flow" and "full flow least"
CSCth15924	—	RRI routes remains after disconnection if connecting from local LAN
CSCth16962	—	GETVPN KEK timer gets stuck to zero after GDOI policy change and rekey
CSCth20862	—	asr1k:RLS7:ios crash on changing gre ipsec tunnel destination on PE
CSCth26920	—	TCL: ungraceful exit from tclsh can leave the Tcl Server running
CSCth29511	—	EEM policy execution cannot be fully disabled
CSCth36114	—	crash after executing "write memory" via sdm
CSCth36813	—	VSL PO goes down while changing the switch fabric mode
CSCth37830	—	12.2(33)SXI3 - xconnect traffic stops when neighboring xconnect removed
CSCth37905	—	The value of ifType for logical lacp ports should be ieee8023adLag
CSCth40213	—	multiple pre-shared keys with address 0.0.0.0 not supported
CSCth43911	—	active crash when configuring subscribe-to-alert-group.
CSCth46251	—	encryption ipsec w/ esp 3des on ipv6 ospf can't form neighbor 2800 3845
CSCth47686	—	ASR1K:Crash seen on EXEC process on GM with psuedotime configured on KS
CSCth61317	—	Noc Payload Crc Error Logged
CSCth64271	—	Routers are staying stuck in manual swact disabled
CSCth64507	—	" event manager policy multiple_ed_8.tcl type user" causes bulk sync fa
CSCth67788	—	sVTI broken when 'ip local policy route-map' configured
CSCth69504	—	7600 - Small buffer leak on SP due to IGMP snooping
CSCth70437	—	876 - Crypto Fails with %SYS-2-QCOUNT and %SYS-2-BADSHARE
CSCth73553	—	dot1x phone unregistered during SSO switch-over
CSCth74294	—	ASR1K ezvpn accounting missing Octets and Packets information
CSCth74527	—	Cat6K: Timing issue with diagnostics corrupt data-forwarding registers
CSCth74953	—	SPI Value shown incorrectly as zero for ipsec sa with crypto profiles
CSCth78343	—	Fetching PSK from keyring should not be restricted to local addr config
CSCth80298	—	Encrypted specific size packet does not go through over MLP
CSCth83455	—	C2WA1b: set default interface <serial interface> is not working
CSCth83634	—	RSTP: Shut/No shut on unrelated neighbour causes root flap

Identifier	Technology	Description
CSCth85618	—	KS Trace@%SYS-3-MGDTIMER@Process= "Crypto IKMP"@gdoi_init_rekey_timer
CSCth87937	—	Crash after configuring 'ip multicast boundary'
CSCth92629	—	On Bootup/SSO or traffic, few S,G are not installed completely in Hrdwar
CSCth92828	—	TACACS key is not blanked out
CSCth93066	—	IPV6 mcast traffic is SW forwded over standby uplink with DCEF-only mode
CSCti01426	—	Switch crashes after configuring 'auto qos voip trust'
CSCti06901	—	SMI:director not sent dhcp option3 when configure vstack dhcp-localserve
CSCti15448	—	C4HD1: Traffic loss due to ACE intra-chassis failover on VSS setup
CSCti15990	—	EZVPN not up immediately after Virtual-access interface up
CSCti16649	—	ASR1K: GM re-registers with KS when ACL is add/remove in KS.
CSCti23872	—	traceroute double hop with set vrf due to double ttl decrement
CSCti32358	—	linkup is detected earlier than that of the connected device
CSCti36423	—	ASR memory leaks when configured with NHRP, SNMP and DMVPN
CSCti37172	—	Ingress SPAN on Sup duplicates packets to ACE module
CSCti39902	—	RRI: Route still seen on UUT via router1 after deletion of ipsec SA
CSCti41891	—	Traceback@verrmsg and stanby continuosly reboots
CSCti42958	—	IKEv2 should not select ESN amongst proposal until supported
CSCti47250	—	MVPN: S,G entry not created in mroute table for default-MDT group
CSCti48407	—	Incorrect TTL handling in MPLS traceroute if TTL=1
CSCti49472	—	System acct off fails to work on suppress CLI enabled for SSO
CSCti51196	—	SSH [ipv6] to any link-local address connects to itself
CSCti57096	—	6500 OIR causes crash w/ service policty on Distributed Etherchannel
CSCti59656	—	After tp tunnel cutover OCE chain is inconsistent between RP and LC
CSCti60740	—	crash after disconnect command
CSCti64429	—	Bus Error Crash at fm_process_nf_dbase_clr_timer
CSCti66454	—	Crash in TunPro_v4_fivrf ipsec sanity test case
CSCti71807	—	cnfTopFlowsOutputIfIndex returns value 0, instead of destIf
CSCti72095	—	c2wa1: Switch crashed after ISSU runversion from latest sierra to SXI2a
CSCti84025	—	VRFs hardware re-mapping causing MLS/CEF inconsistencies
CSCti93310	—	With static IGMP outgoing port not programmed in hardware after reload
CSCti94107	—	c2wa1:BOOTUP_TEST_FAIL: Switch 2 Module 1: TestQos failed
CSCtj01235	—	Crash after "debug crypto isakmp" during isakmp profile selection
CSCtj04195	—	Additional bridge asic registers need to be removed from TestErrorCounte
CSCtj04278	—	IPv6 forwarding fails post encap in Multipoint GRE tunnel (DMVPN IPv6)
CSCtj04562	—	PBR with 'set interface null' causes incorrect tcam programming
CSCtj06067	—	Chunk memory leak on the process MallocLite @__be_pdb_distance
CSCtj06432	—	Crash seen @ msc_destroy_met_set during SSO

Identifier	Technology	Description
CSCtj07133	—	Incorrect switchover to SPT with Multipath configured
CSCtj10515	—	Exnet: Mrib and Mroute entry goes out of sync after a routing loop
CSCtj14921	—	IOS_INTR_OVER_LIMIT and crypto map memleak with dVTI & DynCMAP stress.
CSCtj15088	—	c2w2:MDEBUG tracebacks @ qm process while applying service policy.
CSCtj17637	—	MF: HTTPS generates a new self-signed cert on reboot even if one exists
CSCtj22529	—	some mcast shortcut are process switched in ISSU RV.
CSCtj27523	—	On Standby Sup SP, Memory leak seen related to MET
CSCtj30297	—	System returned to ROM by address error at PC 0x10B81BC, address 0x0
CSCtj38057	—	QOS ACEs with 'eq' for dst ports not programmed when LOUs/label exceeded
CSCtj40564	—	crypto keyring binding with local address is broken in some scenarios;
CSCtj46927	—	MF:Access Vlan is removed when 802.1x is enabled on port
CSCtj48039	—	ikev2 account send out 2 Acct-Session-Id attribute
CSCtj52347	—	Span confg removed from PO span dest causes L3 protocols to not work
CSCtj55624	—	Router crash with show crypto ruleset CLI with v6 crypto maps
CSCtj58219	—	Standby switch crashes when repl mode is changed to egress in ISSU RV
CSCtj59721	—	%PM_SCP-2-LCP_FW_ERR_INFORM: module 8 is experiencing the following err
CSCtj61261	—	DFC has misprogrammed i2k_slvan for private vlan after reload
CSCtj63031	—	SNMP syslog trap for OER_MC-5-NOTICE msg is not sent
CSCtj66392	—	IPSec Stateful Failover: TP doesn't open crypto socket on standby router
CSCtj66981	—	MET2 is not programmed for new SR translation rules added in ISSU RV
CSCtj76176	—	Port-Channel members go to w state (Up Mstr Not-in-Bndl) after SSO
CSCtj76788	—	Bulk-sync failure @ set ip next-hop recursive vrf in route-map
CSCtj91384	—	IPC Crash Seen In SXH
CSCtj91928	—	C6K PBR set ip nexthop verify-availability w/ tracking & nexthop tunnel
CSCtj94510	—	Crypto_SS_process crashed at sessions setup
CSCtj94589	—	Crash happened at unconfig vrf under crypto isakmp profile
CSCtj96837	—	Blank occurred on show run when the system switchover.
CSCtj99724	—	SXI1: Memory leak in "mls-msc Process"
CSCtk00198	—	Stack master crashed on defaulting ASw interface
CSCtk03526	—	Segmentation fault at Crypto IKEv2 process while scaling static CMs
CSCtk05747	—	TCAM remerge seen on interface up/down, causing 100% CPU
CSCtk10279	—	LISP crash when receiving map-reply with IPv6 RLOC without IPv6 routing
CSCtk10374	—	Crash @ cts_dot1x_authc_supp_info.
CSCtk12122	—	Tracebacks @crypto_ipsec_sa_lifetime_expiry,crypto_ipsec_key_engine
CSCtk14496	—	WA1: system crash when issue {red reload peer} on VS setup and non-VSS
CSCtk14941	—	Memory leak seen @ fh_applet_config_entry_proc
CSCtk16232	—	MVPN traffic software switched due to mtu failure

Identifier	Technology	Description
CSCtk31978	—	c2wa1: VSS Act (SW2) reloads after ISSU LV and AV if NAM card is in SW1
CSCtk32622	—	WS-X6748-GE-TX May Reset If All Ports Are Shutdown With Interface Range
CSCtk59012	—	Deprecate LSD HA
CSCtk60169	—	config sync not happening after setting crcSpanDstPermitListEnabled obj
CSCtk61460	—	Set vlanPortVlan on a port to diff access vlan disconnect IP phone
CSCtk63049	—	Bulk-sync failure due to PRC mismatch due to mls sampling interface
CSCtk65429	—	Traffic crossing MPLS passes in clear and does not hit crypto map
CSCtk66648	—	Traceback Spurious memory access pm_get_bcast_supp_discard_counters
CSCtk68647	—	ASR1K: DMVPN Shared TP - crypto sockets not cleared + exhaust resources
CSCtk69114	—	RP rest @crypto_ipsec_clear_endpt with crypto config
CSCtk76633	—	Wrong FPOE programing after replacing the chassis with different type
CSCtk84116	—	GETVPN ks crash during split and merge happening between the key servers
CSCtk99699	—	GETVPN : Rekey functionality is broken if you remove and add crypto Key
CSCtl00995	—	ikev2: ASR1K with 1897 svti tunnels & ikev2 reloads @ IPSEC Key Engine
CSCtl03781	—	ISSU:ONLINE-SW1_SPSTBY-6-INITFAIL: Module 6: Failed to bring up DFC
CSCtl05514	—	IDSM etherchannel fails after SSO
CSCtl05684	—	XAUTH user remains if authenticated by different user during P1 rekey
CSCtl08594	—	EZVPN client fails when outside interface is fastethernet and NAT config
CSCtl23179	—	Incorrect TCAM Programming when new DHCP address received.
CSCtl23439	—	Need to increase CRYPTO_IPSEC_TRANSIENT_SPI_AGING_INTERVAL timer value
CSCtl23748	—	EoMPLS over GRE (DMVPN) with IPSec protection not working after reboot
CSCtl24871	—	GLBP virtual mac not programmed in tunnel internal vlan
CSCtl45122	—	CSCsv76509 seen again in SXI4
CSCtl46816	—	DMVPN spoke should not init. invalid SPI recov while already negotiating
CSCtl54046	—	Standby Sup crashes@dot1x_get_supp_sb with cts dot1x/manual
CSCtl58505	—	sa connection id created are out of the permissible range of <1-32766>
CSCtl58612	—	Stby Sup resets with "boot bootldr", but file doesn't exist on stby
CSCtl58831	—	small buffer leak on WS-X6708-10GE
CSCtl59710	—	Multicast traffic process switched if nat outside configured on FWD intf
CSCtl73660	—	c2wa1: IP ACL TCAM doesn't get reset after removing ACL filter from MPA
CSCtl75972	—	CPUHOG for "Virtual Exec" seen when removing/adding ACL on VSS
CSCtl76189	—	On inserting JIAN the SVC ips of all WISMs/JIANs in the system flushed
CSCtl83517	—	C2WA1: ISSU cycle from sierra->SXI with 256PO not working - red_mode
CSCtl88070	—	IPv6 VRF configuration causes software punt for global uRPF
CSCtl92049	—	IPSec memory leak was observed after simulating smurf attack on UUT
CSCtl98884	—	Crashes noticed in AAA create user (kron /console buffer got corrupted)
CSCtn00835	—	Traceroute via mpls cloud does not show egress PE in 3C mode

Identifier	Technology	Description
CSCtn02208	—	ISG: Old peruer acl not removed on applying new acl
CSCtn03582	—	TTL Failure rate-limiter not working
CSCtn05007	—	ip multicast boundary command not filtering in both directions
CSCtn09789	—	Traceback seen after fixing this ddts CSCtk58012
CSCtn12119	—	Add support for dual signing
CSCtn12243	—	T/b @ icc_send_mcast_request upon bootup
CSCtn16303	—	The notification was generated incorrectly by ME-C6524GT-8S.
CSCtn18654	—	Mem corruption @ checkheaps after remove and insert LC on diff. slot
CSCtn18962	—	ospf :s72033-lanbase-mz image missing subsystems
CSCtn22325	—	ikev2-ra access-request radius should contains a calling-station-id
CSCtn22339	—	Pre-shared-key lost after router reload
CSCtn25253	—	command in EEM script gone missing after router reload
CSCtn31309	—	"int g0" command on ASR1000 creates unwanted GMPLS0 interface
CSCtn39632	—	Unable to configure RSA key under crypto keyring
CSCtn39950	—	Reventon not working with BRI-PRI connection
CSCtn42811	—	"Template name contains one or more illegal characters[OK]" while bootup
CSCtn46263	—	mem leaks seen for ikev2 sanity on 152-3.22.2.PIB16
CSCtn46329	—	IKEV2 should send an authentication failed after an auth timeout
CSCtn47119	—	Crash @ ipsecv6_check_if_icmp_embedded
CSCtn49482	—	CONFIG_NV_NEED_OVERRUN and config lock after configuring IDS module
CSCtn51740	—	Memory leak found in 2800 router "ezvpn_parse_mode_config_msg"
CSCtn52417	—	IKEV2-RA some Radius accounting attributes are missing
CSCtn55187	—	pak is not freed in crypto_ipv6_udp_write if tunnel i/f is shut
CSCtn55847	—	Mem leaks seen at crypto_isakmp_save_qm in DVTI scenario
CSCtn57039	—	Memory leak in RADIUS and EAP Framework processes with dot1x configs
CSCtn61834	—	Transport nat overload flow process test failed in ipsec_nat_wrapper
CSCtn62033	—	VA fails to come up, when loopback int is used as IKE end pt
CSCtn64575	—	Notification of multicast alternate next hop updates is delayed
CSCtn65137	—	mem leaks found in NHRP
CSCtn65393	—	MPLS imposing in-correct TTL when using sVTI Encryption
CSCtn67577	—	SIP-400 is crashing while modifying cell-packing values
CSCtn68317	—	Cat6500/SXI: DHCP snooping removed from vlan on module OIR
CSCtn68537	—	GETVPN: "Registering to" field might not be present
CSCtn68643	—	OSPFv3 hellos are not processed w/IPsec authentication or encryption
CSCtn72884	—	IKEv2 - ASA to IOS cert based fails - Interop Issue
CSCtn74249	—	Post-Frag behavior is changed to pre-frag when changing the IPSEC SA MTU
CSCtn91337	—	mem leaks found @ nhrpSnmpAddr2OctetStrAdd

Identifier	Technology	Description
CSCtn95395	—	VTEMPLATE Background Mgr crashed after clear crypto session on CES
CSCto10485	—	Locally generated traffic may fail IPSec replay check w/ GRE over IPSec
CSCto11025	—	Packet drop on crypto engine with Buffer Unavailable if QoS is applied
CSCto14268	—	Crypto ruleset corrupted during the initial configuration of a getvpn GM
CSCto15371	—	system crashed at [crypto_check_acl]
CSCto16601	—	EzVPN input feature disappears with "flow restrict" enabled
CSCto29645	—	DHCP SNOOPING: Dhcp relay information option (Option 82) replace
CSCto33424	—	After SSO "mls cef error action reset" cli gets added on standby
CSCto43776	—	"shared" keyword does not work as expected on second tunnel interface
CSCto47294	—	Router crash while configuring EzVPN dVTI client
CSCto53119	—	ES40:EoMPLS for a vlan X not progmd on LC after allowing&removing frm VE
CSCto53332	—	%AAA-3-BUFFER_OVERFLOW: Radius I/O buffer has overflowed
CSCto56052	—	MPLS Forwarding not working on PPPoA Dialer Interface
CSCto60399	—	GETVPN:having icmp/ip acl's in KS, ping is not working IN 15.2(0.7)T
CSCto61098	—	chunk leaks observed @IPToOctetString "SNMP SMALL CHUN" in 15.2(0.9)T
CSCto61485	—	High CPU Util seen on LNS after PPPoX session disconnect with scaling
CSCto63954	—	Router continuously crashing with GETVPN configs
CSCto64858	—	rate limiter cli not sync on unconfiguring port-security and perform SSO
CSCto69916	—	Apply ACL in order of IPv4 then IPV6 disables TCAM screening on int.
CSCto73345	—	Router Crashed while reloading
CSCto73878	—	Intermittent PAT Order-of-Operations problem
CSCto76018	—	ASR1000-WATCHDOG crashed after clear crypto session on CES
CSCto76700	—	Multihop bfd session goes DOWN with TE-FRR cutover
CSCto80719	—	Crash seen using "tunnel protection ipsec profile tunpro" on IPv6 tunnel
CSCto81814	—	Router crash when SSH over IKEv2 tunnel to manage the router
CSCto89922	—	GetVPN KS sends a Rekey ,even when the KS ACL is un-supported
CSCto90252	—	Standby RP stuck to "init, standby" for about 10 hours after reload
CSCto92123	—	continuous tracebacks at ce_sw_encrypt_ipsec_packet
CSCto92529	—	%OSPFv3-3-IPSEC_POLICY_ALREADY_EXIST:Unable to configure ipv6 ospf auth
CSCto92586	—	chunk leak seen at ipsec_dp_init
CSCto92891	—	MFIB_IPC-3-MFIB_RP_FAILED_IPC_SEND: IPC message for stats or rates fails
CSCto95484	—	XDR interrupt client can't guarentee no-interrupt msg send
CSCto95687	—	Failure to aquire sem (l2_se_get_ps_sem) for a long time leads to crash
CSCto98855	—	Supervisor crashes in VS mode when VSL LC crashes
CSCto99234	—	LACP Auto Interleaved HA issue
CSCtq06060	—	LACP config re-appeares after PO detele/recreate sequence
CSCtq06105	—	MPLS FRR function broken

Identifier	Technology	Description
CSCtq07413	—	HW Crypto may fail to decrypt with error invalid parameter
CSCtq08784	—	IKEv2 ENCR payload during IKE_AUTH doesn't conform to RFC 4868
CSCtq09354	—	VLAN counters & adjacency counter do not match at high rate of traffic
CSCtq09372	—	GRE/IPSEC with TP, ip mtu does not take ipsec overhead into account
CSCtq09426	—	Tunnel path-mtu discovery broken with GRE/IPSEC Tunnel protection
CSCtq09449	—	CMTS boot failed and PRE4 crashed for OBFL
CSCtq24006	—	DmVPN with ipv6 doesnt come up even without crypto configured
CSCtq26057	—	Multicast ping fails after manual SA was fixed
CSCtq26766	—	SUP720-3B crash due to large number of IGMP reports received
CSCtq27016	—	Qos related Memory leak is observed on ES-40
CSCtq28392	—	Fix build errors on latest t_base_2 due to CSCto80719
CSCtq31974	—	c2wa1b: multicast SR translation not happening after active sup crashes
CSCtq32282	—	Chunk Leaks @ isadb_group_allocate, isadb_user_allocate
CSCtq33932	—	%ERROR: Standby doesn't support while configuring atm subinterface
CSCtq37579	—	UUT crashed @snmp_free_variable_element
CSCtq46279	—	Standby crashes on authz failure when voice and critical vlan are same
CSCtq47531	—	Shortcut count on active fluctuates when standby chassis is reset
CSCtq47856	—	GM fail to free ident/SA and crashes in subsequent rekey
CSCtq48160	—	cbQosPoliceCfgRateType not set to 2 (Precent) when configured via CLI
CSCtq50438	—	c2wa1b: JIAN ports not detected on SIERRA 0523 Image
CSCtq56225	—	Multiple Authorized types seen for dot1x supplicants
CSCtq56256	—	DVTI: Correct route next-hop to be like for a standard virtual-template
CSCtq61665	—	c2wa1b: %BIT-STBY-4-OUTOFRANGE: bit 32767 is not in the expected range
CSCtq61884	—	DHCP snooping for unicast not working to HSRP DMAC
CSCtq63225	—	Dropped classified packets on IPSec tunnel
CSCtq63487	—	with Multi-action ipv4/ipv6 pbr, Deletion of vrf causes issues
CSCtq64820	—	6500 SP crash at cmfi_frr_process_stats_counters
CSCtq65072	—	Crypto related segmentation fault crash in 15.1(1)S2
CSCtq69083	—	Nested IPSec Tunnels Support - GRE / IPsec as outside tunnel
CSCtq74345	—	Gre mode (no) / tunnel tos x shows incorrect behavior
CSCtq75008	—	LNS router for L2TP over IPSec crashes
CSCtq75045	—	FlexVPN connection gets stuck in NEGOTIATING state
CSCtq77024	—	Route change on ATM/FR intf causes dvmc to fail
CSCtq79767	—	IPSEC key engine crashed after clear crypto session on CES
CSCtq80394	—	mroute entry not create for sparse default-MDT group
CSCtq86573	—	Processor memory leak due to crypto_pki_keyring_pki2keyring_subj
CSCtq87937	—	slow leak in Crypto SS

Identifier	Technology	Description
CSCtq88437	—	RLS10:ikev2 iosd crash when test with 4K Crypto Map
CSCtq93623	—	Perf. degradation with copy funcs when using large acl and mcast config
CSCtr01421	—	cont standby reset "ip source binding <#> vlan <#> <ip> int fa3/8" if L3
CSCtr03012	—	On SSO, Mcast RPF-MFD fails only with static join @ RPF i/f
CSCtr07142	—	Memory leak seen at crypto_ss_open
CSCtr15483	—	Tunnel interface support of GDOI cryptomap is broken in latest T
CSCtr16857	—	IKEv2 windowing is broken in flexvpn_phase2
CSCtr17317	—	Mem Leak in mld_etrack
CSCtr19129	—	VSS - need to suppress "SIBYTE-SW2_DFC2-3-SB_TX_FIFO_UNDRFL" msgs
CSCtr20300	—	SA negotiation test failed.
CSCtr21296	—	multiple issues after disabling hardware crypto engine
CSCtr22434	—	IPv6 crypto map gets leaked and unable to remove OSPFv3 policy
CSCtr23134	—	"debug crypto ikev2 internal" causes a crash/printsgarbage.
CSCtr24889	—	Static route in vrf causes %MPLS_IPRM-3-INTERNAL:
CSCtr25103	—	Revert the changes for CSCso98512
CSCtr25127	—	Traceback observed with switching between ATM and 3G interface
CSCtr26398	—	vslor ERROR !! may be observed on VSS when member port is down.
CSCtr31153	—	Packet decryption fails while using crypto maps
CSCtr31638	—	Continuous traceback & crash due to 'RF Interdev reload process'
CSCtr39973	—	c2w2: Diag failure after second sso with arp policing
CSCtr40279	—	CTS interface is stuck in "OPEN" though nei port is not CTS configured
CSCtr41990	—	Router crash after the "Crypto IKMP" process had been hogging the CPU
CSCtr42913	—	Stale crypto maps left behind for shared tunnel protection
CSCtr52081	—	packet storm with external loop on dot1x/mab ports in singlehost mode
CSCtr59314	—	ASR: DVTI ikev2 headend crashes for clear crypto session
CSCtr59775	—	proxy map-reply setting R bit to zero causing the locator to be down
CSCtr61289	—	FlexVPN connection gets stuck in NEGOTIATING state
CSCtr61390	—	Standby SUP crash @ when its booting with SXI and SXJ image
CSCtr61623	—	FlexVPN : ASR(Server) reload at process IPSec key engine
CSCtr64482	—	Vlan 1 is getting allocated as internal vlan
CSCtr67276	—	PBR within a VRF with object tracking not working on Cat6k
CSCtr67852	—	RRI injects invalid entries at failover when Stateful IPSec HA is used
CSCtr67921	—	Memory Leak At crypto pki
CSCtr68112	—	SW installed NF entry does not get updated when next-hop sends garp
CSCtr82360	—	%EARL_L2_ASIC-DFC4-4-DBUS_HDR_ERR: EARL L2 ASIC #0: Dbus Hdr.
CSCtr85457	—	MA2:Memory Leaks with QoS Configurations
CSCtr87740	—	Crash seen at crypto_check_acl due to freed postdecrypt_check ACL

Identifier	Technology	Description
CSCtr93412	—	XE35 GETVPN - IGMP/PIM Crash Seen on Mwheel Process
CSCtr95194	—	VSS 2T - TX SPAN fails for mcast traffic after oir/reload/shut no shut
CSCtr96204	—	TE Tnl: MPLS VC down as Tunnel app ignored while inferring implicit null
CSCtr96541	—	ASR1k EZVPN - OU attributes chosen incorrectly for client authorization
CSCts02018	—	Memory leak in Spanning Tree process on SP
CSCts02779	—	Local PBR broken on ASR
CSCts05277	—	Miscalculation of IPSec overhead for ESP-GCM
CSCts10254	—	VTI: Tunnel mtu is set to improper value if using loopback as source
CSCts14799	—	XE35 - Memory leak on IPSEC key engine
CSCts18404	—	Duplicate IKEv2 SA deletion removes mode-config configuration
CSCts19088	—	programmed metadata acl got removed unexpectly
CSCts22336	—	Bus error crash with NHRP
CSCts27161	—	VSS:standby reloads due to parser return error command: duplex full
CSCts27379	—	Mem leak @ fm_cm_dynamic_policy_update+1BC upon defaulting 4k EFP intf
CSCts29515	—	CTS: Peer policy is not updated after reauth.
CSCts32963	—	ACL in distribute-list/distance should be created with ACL_UNDEFINED
CSCts34693	—	Crash in syslog_pubinfo_enqueue
CSCts37446	—	c7600: traceback seen @ zamboni_create_flow_cmd
CSCts38007	—	Query Interval mismatch msg appears on a sw where no querier configs
CSCts42154	—	ASR Fails to Register after the Initial Attempt Failing
CSCts43808	—	TB seen on config replace and subinterface po on vnet trunk down.
CSCts44718	—	crash found on fnf_cache_remove_from_free_list
CSCts49137	—	show tech redirect command fails in SXJ1
CSCts49769	—	CVV: crash @ auth_mgr_ctx_destroy when unconfiguring CVV
CSCts63501	—	Explicit Null Configuration, in a *not EOS* case is set to Dropa
CSCts66142	—	Reconfiguring "mls ip multicast stub" config does not program tcam
CSCts66625	—	VRRP master mac-address with Xtag=0 causing high cpu
CSCts68322	—	Multicast traffic blackholing and elif points to cpp
CSCts68541	—	ipsec key engine crash @be_crypto_ipsec_preferred_peer_lookup
CSCts69973	—	Spoke with 100 tunnels crashed at "nhrp_process_delayed..."
CSCts76410	—	VTI: tunnel interface stays up/down even with active SA and socket.
CSCts81583	—	Internal vlan acl denying - causing vrf connectivity failure
CSCts82932	—	Incorrect dscp-q mapping on trusted interface
CSCts84327	—	IDSM/NAM will not come up when power off followed by power on
CSCts85459	—	C881GW : On Reload, cellular int won't negotiate if crypto map applied
CSCts89599	—	EEM ED routing events fail but should have matched pattern specification
CSCts96040	—	VSL configuration check before reloading a VSS switch with FIPS

Identifier	Technology	Description
CSCts98336	—	unconfiguring ikev2 profile is causing a crash
CSCts98410	—	Standby going to RPR mode after Switchover
CSCtt04093	—	VC is not coming up after unshutting the preferred path/Tunnel
CSCtt04914	—	Span stops working and must be re-configured to continue working.
CSCtt11748	—	RP crashes @ route_map_ip_info_remove
CSCtt15401	—	dIOU image is crashing in rf_slave_is_present during bootup
CSCtt16102	—	Traceback seen on unconfig ACL @ pfm_protofltr_acl_configured
CSCtt16732	—	SP memory display in wrong on SUP720-3B when running 12.2(33)SXJ1
CSCtt17490	—	%GDOI-5-COOP_KS_REACH is shown too early
CSCtt18651	—	cat6000-qos and Traceback after a no shut of a port system crash
CSCtt23038	—	IOSD core @flow_lock_lock when issuing show command during HA tests
CSCtt23358	—	RP crash @ __be_tunnel_protection_remove_idb_for_connection
CSCtt24777	—	net_background crash @ be_crypto_ipsec_update_peer_path_mtu
CSCtt26063	—	c2ma2:sdby rebooting continuously due to "mls qos trust cos" config sync
CSCtt27490	—	Policer does not work on dialer interface with crypto map
CSCtt27583	—	c4ma2:Adjacency fields is not programmed in fm interface with gre tunnel
CSCtt33433	—	(S,G) MAC with missing ports blocks egress traffic with PIM snooping
CSCtt36513	—	FlexVPN : ASR(Server) reload at process IPSec key engine
CSCtt41807	—	GOLD Traffic Stress test needs improvement to catch bad fabric port
CSCtt45654	—	Virtual-Access is not deleted when tear down ipsec session
CSCtt46730	—	c3945e platform crash at crypto_check_metadata with version 15.2(1.14)T
CSCtt70133	—	RP crash @ __be_ikev2_bin2hex_str due to crypto_engine: no resources err
CSCtt94440	—	RLS3.6 eToken: RP reloaded when issue "show cryp eli all" with IKEv2
CSCtt94484	—	Overwriting default keyword is ignored in set peer command
CSCtt96152	—	VSS: corrupted Portchannel: LTL missing VSL-link
CSCtt97950	—	3rd set peer statement in crypto map not being used
CSCtu00699	—	IOS processor pool memory fragmentation due to Crypto NAS Port ID
CSCtu01035	—	OIR heathland module on newly active during standby bootup crash both
CSCtu03447	—	Mem leak @ ltl_set_sw_status_cb with MEC,VSL,rxvr ports on same linecard
CSCtu03867	—	switch crash when polling energywise mib and energywise disabled
CSCtu03945	—	%LINK-SP-3-UPDOWN and %LINEPROTO-SP-5-UPDOWN message does not read out
CSCtu07968	—	ISR 890: Perf mon reports incorrect loss packets/percent with 0 loss
CSCtu17134	—	ASR IOSd process memory pool fragmentation due to BigNumAlloc
CSCtu22335	—	On a 6500 after a sup switchover arp inspection fails to forward arp
CSCtu25952	—	1 multicast packet is forwarded on RP-tree even though (S,G) exists
CSCtu31096	—	Unexpected mcast traffic copied to SPAN destination port in MVPN setup
CSCtu32929	—	DMVPN tunnel does not come up when TrustSec is enabled in the Hub

Identifier	Technology	Description
CSCtu35116	—	VPDN sessions doesn't come up with "mpls mtu" more than 1500 byte
CSCtu36321	—	CVV: Phone mac gets deleted in MATM on CDP 2nd port up/down for MA mode.
CSCtu36562	—	Missing or improper mapping of IKEv1 failure reasons
CSCtu37676	—	On FWSM insertion, standby sup may crash or active report not enough mem
CSCtu38244	—	GetVPN GM can't register to GDOI after bootup
CSCtu42675	—	%SYS-2-BADSHARE: Bad refcount in datagram_done, ptr=, count=,-Traceback=
CSCtu42798	—	Metropolis RBH filtering is wrongly programmed for Met-0 ASIC in VSS
CSCtu43731	—	Watchdog fires taking down RP on ISSU event with 4000 DVTI sessions
CSCtu75030	—	FTP of exception core dump after crash times out
CSCtv28434	—	GETVPN: tracebacks during GM re-registration
CSCtw46061	—	Irremovable IPSec Sessions in "show crypto eli"
CSCtw46793	—	Primary Key Server Uses Wrong Rekey Sequence Number upon Split&Merge
CSCtw49735	—	load-defer config is not syncing after SSO while load-defer running
CSCtw49851	—	show ipv6 mld snooping explicit-tracking cli o/p changed
CSCtw50375	—	NF entry does not get dmac updated after next-hop device sends garp
CSCtw50952	—	ASR crashes due to memory exhaustion after issuing "clear ip ospf"
CSCtw52097	—	RG state does not progress to STANDBY HOT - broken in 15.2(2.6)T
CSCtw58586	—	default ikev2 profile should be anchored to the default ipsec profile
CSCtw61876	—	IGMPv3 leave results in MCAST packet loss for other receivers
CSCtw69374	—	ISR G2+ISM: "crypto map" command removed after disabling HW acceleration
CSCtw71447	—	ipsec:route-set=prefix is parsed but not included in the config-response
CSCtw73530	—	Metadata: flow gen fail to clear created flows with 100 or more flows
CSCtw78451	—	ASR1k May reload when multiple users are issuing show commands
CSCtw79510	—	Cant force VPN client users to change their passwords in the nxt login
CSCtw86793	—	IKEV2 DVTI sends KMI KEY_ENG_REQ_SAS on ikev1 instead of ikev2
CSCtw91041	—	Convergence time for bgpv4/v6 on sup4 degrading from sierra to ma2_pi
CSCtw93140	—	On 'wr mem' command noticed "% VRF table-id 0" message
CSCtw93788	—	MDA port during reauth goes to error disabled state on SSO.
CSCtw98456	—	Static and dynamic RRI create incorrect route in vrf-aware IPSec case
CSCtw99035	—	PE NOT generate its local v6 type-1 route after "clear bgp ipv6 mvpn * "
CSCtw99185	—	Ipv6 Reflexive acl not working in HW for sdby CFC
CSCtx00829	—	t-train : 802.1X authentication failure reason code 23
CSCtx01329	—	Software Forced Crash due to %SYS-3-CPUHOG: <snip> process = Crypto ACL.
CSCtx01918	—	ew isakmp sa triger by invalid-spi recovery has wrong ivrf
CSCtx04712	—	removing gdoi crypto-map from interface hangs the router
CSCtx06747	—	boot failure due to TLB (Store) Exception with ASSERTION FAILED logged
CSCtx06813	—	lfd_install_local_label_for_key: installation failed for rwid type l2ckt

Identifier	Technology	Description
CSCtx15860	—	Continues t/b message in id_get when ip prefixes run out of space
CSCtx16782	—	FlexVPN Spoke to Hub, not getting UP event from crypto sock
CSCtx16977	—	TB @ mvrp_switch_port_oper_state_change upon enabling MVRP
CSCtx17098	—	HSRP/Routing protocols stops working on disabling MVRP
CSCtx21321	—	Router crashes while deleting vrf in SRE5
CSCtx23534	—	RRI Host Routes not replicated to HA peer
CSCtx23600	—	c2ma2: Auth fail vlan doest recover after giving valid credentials.
CSCtx28301	—	Call Home registration may trigger a reload when IPv6 is enabled
CSCtx30881	—	Estelle: %CONST_DIAG-3-HM_PORT_TEST_FAIL: Module 2 TestNonDisruptiveLoo
CSCtx31294	—	Ikev2 doesn't come up if headend Local auth is RSA-SIG, for AC clients
CSCtx31329	—	Memory leak in ikev2_process_config_set_attribs
CSCtx32527	—	Flexvpn: IPSEC SA on GRE tunnel should act as always-up like ipsec-ipv4
CSCtx34643	—	ping MPLS Psedowire is not working with single segment
CSCtx35036	—	MPLS static crossconnect is not working in 151-4
CSCtx35465	—	RTTY client is not created in VSL enabled Estelle LC
CSCtx38953	—	crash in IPSEC key engine code @crypto_ipsec_profile_map_val
CSCtx41296	—	xe35:memory leak @ be_variable_chunk_malloc_internal
CSCtx42175	—	flex server fails to bring up session with win7 client
CSCtx43498	—	cat6500: Some DACL entries may not be pushed to the switch TCAM
CSCtx44060	—	Flexvpn spoke to spoke tunnel doesn't come up
CSCtx48753	—	ASR1K: 10% Increase in IOS Mem in BBA Profiles in XE36
CSCtx49766	—	GETVPN tracebacks with 3g/4g HWIC
CSCtx50176	—	ASR1k :ikev2 brings up sa even with CRYPTO_ERR_RESOURCES from dh
CSCtx50235	—	SP and RP mutually resetting each other hides the actual crash reason
CSCtx52805	—	"%PARSE_RC-3-PRC_SUBRCODE_RANGE" error with mls sampling configuration
CSCtx54859	—	Display the module and port causing %PM-SP-4-BAD_COOKIE
CSCtx57073	—	ISSU:XE3.6--->MCP_DEV iosd crash @ Process = Metadata HA
CSCtx61557	—	crash after authc result 'success' from 'dot1x' for client (— MAC)
CSCtx62375	—	mem leak and cm messages with sclae config
CSCtx72339	—	platform rate-limit config for acl-drop get into invalid value
CSCtx74051	—	Unsupported subtraffic bits from XDR not ignored; ISSU downgrade breaks
CSCtx74258	—	6908 module may crash while reading registers
CSCtx76004	—	XE36: Spurious memory access at route_map_ip_info_remove
CSCtx77503	—	mls config commands crash Sup2T
CSCtx78044	—	6-8 second delay in forwarding mcast after a rapid join/leave/join
CSCtx84897	—	Wrong Default interval for HM "TestEARLInternalTables " is set to 5 secs
CSCtx86116	—	ZBFW-HA: ACTIVE router crashing when HA config is removed

Identifier	Technology	Description
CSCtx87939	—	XML output for mediatrace poll command is invalid
CSCtx90408	—	Crash after configuring a crypto map on a HSRP enabled interface
CSCtx90705	—	ISSU XE343->XE322: LDP neighbor is down after CC/SPA downgrade
CSCtx92054	—	On Creating monitor session device goes for a reset with traceback.
CSCtx92665	—	Crash at __be_sla_mt_route_data_print with show cmd after link flap
CSCtx92802	—	Packet drops with VFR and crypto tunnel
CSCtx92816	—	NDAC link with Manual Mode stops fwding packets after sometime
CSCtx92952	—	SUP crash when issuing show upgrade fpd file ftp/tftp cmd
CSCtx93598	—	ikev1 dpd config erroneously affect ikev2 flows
CSCtx98926	—	LIF expansion not requires if 'acl downloadable setup' is not configured
CSCtx99483	—	Switch crashes when removing PBR from interface
CSCty02902	—	cnma1b: FWSM RHI Routes are not withdrawn after SSO on VSS
CSCty03133	—	XE35: Memory leak in IPSEC key engine process
CSCty07538	—	Incorrect static NAT translation leads to TCP reset
CSCty21663	—	EBGP peer flap with mcast traffic cause cpu spike , ospf and ebgp flap
CSCty22100	—	Ezvpn: change phrasing in debug for http intercept
CSCty26334	—	ospfv3 neighborship fails to come up between PE routers with shamlink
CSCty27229	—	ME-6524 switch ports with CWDM-SFP go down
CSCty28813	—	mis-config "VRFa mdt_default" as "VRFb mdt_data" is not blocked
CSCty42626	—	RSA operations fail with '(malloc) at interrupt level' msg
CSCty44281	—	Commit shimming changes related to hw source entropy
CSCty47509	—	IPsec does not trigger IKE when periodic dpd is enabled.
CSCty49656	—	Crash @ ip_route_delete_common when "no ip routing" is issued on console
CSCty49824	—	MAC change on ipv6 host not propagating new MAC to CEF/TCAM from ND
CSCty52047	—	ASR1k - DPD not deleting IKE SA (release 3.5 and later)
CSCty54036	—	6k/SUP2T cannot do RSPAN if it is intermediate device
CSCty54695	—	RRI routes missing while IPsec SA is up after peer IP change
CSCty56801	—	NEAT: Bus error @ __be_cisp_client_match on Asw
CSCty61152	—	Back out fix for CSCtt66441
CSCty61212	—	Router gets hanged while unconfiguring crypto map tag
CSCty65189	—	First PIM Reg message gets dropped by ZBFW
CSCty70689	—	netflow entry to ignore ACL deny is not programmed for the SUP2T int Po
CSCty71564	—	VS-S720 gig ports can drop multicast traffic under certain conditions
CSCty72183	—	Reloading HSRP standby router impacts IPSec tunnel on active router.
CSCty80553	—	Multicast over IPSEC crashes router
CSCty84989	—	IKEv2+TP+VRF fails installing ipv6 ike routes in the ivrf
CSCty94405	—	DCP and CCP loopback ondemand tests fail without Jian LAG configured

Identifier	Technology	Description
CSCty97033	—	Duplex not changing using snmpset
CSCty97492	—	Not all ARP queries going out when port-channel (DEC) is brought back up
CSCtz01421	—	Fix SA issue in ipflow_aux_post_switch_collect()
CSCtz02829	—	IDSM: some config not getting sync'd to standby properly
CSCtz04599	—	MU: Cat4500: dot1x fail - MAB success - dot1x fail leads to High CPU
CSCtz05012	—	"responder-only"command flushing IPsec SAs before initiator starts rekey
CSCtz08037	—	OCE Handle Leak with dual tunnel encryption
CSCtz14980	—	stby RP keep reboot after SSO when configured crypto map GETVPN_MAP
CSCtz15211	—	15.ISM: Double encryption failure
CSCtz17231	—	Bulk-sync failure due to PRC mismatch when ACL is config with portgroup
CSCtz23020	—	EZVPN IOS 15.x : ISAKMP lifetime corrupt when using cert auth
CSCtz23026	—	VSL interface error after VSL-Encryption
CSCtz25953	—	LFD-3-CORRUPTED_PKT: exception packet with NULL inlabel pointer
CSCtz29869	—	Diag error on sup2T uplinks with cts dot1x enabled - ports errdisabled
CSCtz30804	—	SUP2T: crash at CM-MSG:ERR cm_icc_server error in cond
CSCtz31217	—	IPSLA HTTP probes with source-ip don't work after upgrade to 15.2(2)T
CSCtz32521	—	Need to allow configuration ofBFD min multiplier to be set to value of 2
CSCtz32627	—	Phase II does not come up on ASR for DVTI w/VRF and ASA endpoint
CSCtz35085	—	%SYS-2-BADBUFFER: Attempt to use contiguous buffer as scattered
CSCtz35247	—	HM_TEST_FAIL TestMgmtPortsLoopback consecutive failure for ASASM on OIR
CSCtz36880	—	SXJ3: ACE30 IPv6 RHI throws TB
CSCtz38080	—	Crash seen while unconfig the subint with pbr multiple tracking object
CSCtz40621	—	Crash observed when GM tries to register to KS and KS has issued rekey
CSCtz41048	—	trace mpls ipv4 is unsuccessful in latest PI19
CSCtz42708	—	Sup720 Storm control on unused port causes TestUnusedPortLoopback fail
CSCtz45901	—	show runn
CSCtz45931	—	MVPN traffic drops when a Port-Channel member module is OIRed
CSCtz47309	—	FlexVPN: smart defaults: SA negotiation fails due to mismatched mode
CSCtz47873	—	Flexvpn: "sh crypto ikev2 client flex" doesn't work as expected
CSCtz48615	—	AES encryption may cause high CPU utilization at crypto engine process
CSCtz53188	—	Multiple Traceback @ ipc_locate_port after switchover
CSCtz54207	—	After Master stack down, next hop address is duplicated on "ip next-hop"
CSCtz58941	—	Crash show_network after multiple times "show ip route x" cmd executed
CSCtz59429	—	MF: metadata not matching "application attribute category voice-video"
CSCtz61271	—	6500/7600: Ports not considered in permits in WCCP redirect-list
CSCtz69084	—	Switch crashes when trying to enable IPSec md5 authentication on the SVI
CSCtz70317	—	C6K/Sup2T: On LDB mem exhaustion, report log message

Identifier	Technology	Description
CSCtz71181	—	Sup2T mem corruption crash missing corrupted memory print out
CSCtz72044	—	EzVPN client re-transmiting wrong packet=> death by retransmission throw
CSCtz72390	—	FlexVPN: authorization by name mangler fails silently w/ diag traceback
CSCtz72735	—	Mcast traffic on vrf is dropped on shutting one of the paths to the host
CSCtz73836	—	NHRP crash due to DMVPN event-trace
CSCtz73895	—	TB & crash when default a switchport: CM hogging CPU
CSCtz78194	—	ASR 3.6 crash in IPSEC key engine w/large IKE profile names
CSCtz79703	—	PBR set vrf feature is applied also on IPv4 packets with TTL=1
CSCtz80643	—	CEF unresolved and receive adjacency for VAI using VRF PBR selection
CSCtz80907	—	TP interface goes to reset if profile-name is exactly 31 chars long
CSCtz86763	—	Session/Memroy leak in Crypto SS Process on session churn
CSCtz87383	—	Sup2T-all LDP Packets dropped on Egress
CSCtz89775	—	cnma2:span_add_port_array_to_port_list
CSCtz90154	—	GETVPN rapid re-registartion after ipsec failure during registration
CSCtz91260	—	bootup traceback @ %REGISTRY-SPSTBY-3-STUB_CHK_OVERWRITE:
CSCtz92205	—	GETVPN applying fail close after registered -> registering
CSCtz94984	—	Interop issue between WS-SVC-ASA-SM1 and xconnect
CSCua02456	—	WS-X6824-SFP Minor Error during IOS boot up (TestInbandEdit failed)
CSCua02641	—	Multicast traffic has second drop during SSO/NSF
CSCua03386	—	Sup2T egress multicast replication mode fails on service modules
CSCua06138	—	Dot1x clients are authz failed on routed ports.
CSCua08028	—	Multicast traffic drops under the VRF with IPv6 Family after MVRF upgrad
CSCua10556	—	crypto ikev2 sa stuck in delete state
CSCua15759	—	IOS crashed in function construct_phase2_hash
CSCua17283	—	Aggregate Policy-SVI not working with physical OIR of Aphrodit Line Card
CSCua17746	—	IKEv2 session fails with VSA and ISM VPN modules after CSCtn72884
CSCua28346	—	IKEV2 RSA- Crash in ikev2_ios_mib_tunnel_stop during rekey
CSCua31268	—	VRF-lite : ipv4 multicast traffic loss after "no address-family ipv6"
CSCua32379	—	ASR1k Hubs crashed at crypto_ss_set_ipsec_parameters
CSCua32821	—	Stanby console can be get even without "enable standby console"
CSCua33527	—	:%LFD-SW2-3-SMBADEVENT:TRACEBACK seen after 2nd & 3rd switch over
CSCua36739	—	call admission control increases with only one tunnel established
CSCua37873	—	LSM: MCAST traffic drops at th3 rx PE upon VSS SSO when VSL come back up
CSCua37898	—	MA2: Memory leak seen @ crypto_ss_enable_ipsec_profile on VSS
CSCua39107	—	iprib_first_hop not returning NHO route added by NHRP
CSCua43298	—	Port loopback mode may not be cleared in corner case
CSCua51991	—	Inconsistency for IPSec SA count between IKEv2 and IPSec PI database

Identifier	Technology	Description
CSCua56184	—	RP crashes during flexvpn longevity after multiple RP switchovers
CSCua61126	—	Diagnostic test fails with Wism2 on standalone
CSCua63614	—	6500: Input queue drops when Energywise is enabled
CSCua69657	—	Traceback seen when executing cli "sh clock detail"
CSCua84168	—	[SUP2T] NLB Multicast mode packets hit CPU then are routed.
CSCua84323	—	EthChnl-MP assert failure ahwidb_primary - Traceback
CSCua87594	—	cat6k:Spanning Tree interop between MST0 & RSTP takes 6 secs to converge
CSCua87737	—	Interface name in 'show ipv6 policy' is not complete
CSCua87743	—	Multiple crash observed on VSS setup after sso
CSCua90130	—	link down/up not logged even "logging event link-status default"
CSCua91959	—	monitor capture view/privilege setting causes MALLOC failures
CSCub01301	—	WS-X67XX 1G linecards: Changing the cos map reset the Tail Drop to WRED
CSCub01714	—	Qos -Agg-fwd Counter decrease under policy map after 15 min or so
CSCub05708	—	EnergyWise ACL feature is not OIR / SSO aware
CSCub05981	—	Interface down/down locally after WS-X6848-GE-TX boots
CSCub07673	—	ipsec session doesnt cm up for spa-ipsec-2g if ws-ipsec3 is also present
CSCub15825	—	SUP Crashes,if #no platform qos statistics-export delimiter is executed
CSCub20385	—	GETVPN SNMP: Rekey failure trap not sent on installation failure
CSCub22877	—	call-home VRF aware DNS behavior is not correct
CSCub22927	—	call-home need to change it new created tty privilege level to PRIV_MAX
CSCub24355	—	XE37: stale sm (s,g) states on vrf when stop the traffic.
CSCub33877	—	%RTMGR-3-TOPO_SYNC_ERR (Loadversion from latest texel to Yap CCO)
CSCub50852	—	Unable to use reserved vlan for firewall vlan-group
CSCub52879	—	CCP loopback test for Jian fails upon removal of service-vlan config
CSCub72971	—	inrerface resets counter shows 4294967295 after module OIR/switchover
CSCub81771	—	Revert support to allow multiple ace's in class-map
CSCub83606	—	"policy static sgt 7" has its effect even after it is unconfigured
CSCuc00098	—	Crash occurs with two Sup2Ts while standby Sup is initializing
CSCuc02668	—	Script cat6k_me_cfmosvlanbd_d8_y1731 fails for some 21 TCS
CSCuc11712	—	Fix build breakage of CSCuc05217
CSCuc26317	—	bugtrace() left in commit of CSCtz53188 to v151_1_sy_throttle
CSCej18051	AAA	Terminal Window PPP clients not able to login
CSCsb46724	AAA	AAA server group doesnt failover with mismatched keys for login
CSCsc49958	AAA	aaa authentication fallback to enable caches previously typed password
CSCsc78999	AAA	Address Error exception at TPLUS
CSCsg48725	AAA	TLB exception in tacacs_plus_get_conn
CSCsl18054	AAA	Incorrect user login can remove one-time credentials

Identifier	Technology	Description
CSCsq58176	AAA	No Calling-Station-Id in Access-Request during XAUTH
CSCsq88522	AAA	ha_sso: convergence time greater than expected for more than 2000 interf
CSCsr17680	AAA	test aaa group server request failing over
CSCsr25055	AAA	configuring same word in "enable secret" nd "en passw" doesnt give error
CSCsr76737	AAA	Commands displayed twice in config disapppears after using.
CSCsu04360	AAA	Acct-Time-Delay records and Tunnel-Link-Stop records are missing by LNS
CSCsu32327	AAA	aaa new-model should be deprecated
CSCsu46644	AAA	DROPACCTFAIL: Sys acct fails due to long ios ver length
CSCsu76800	AAA	Giga word attributes missing in Accounting request packets for prepaid
CSCsu82879	AAA	ISG ASR DM4:TracebackAAA-6-BADHDL: invalid hdl AAA ID 0, hdl 36020B6A,
CSCsu82893	AAA	Standby RP can not establish PPPoE session due to wrong Nas-port
CSCsv02117	AAA	session flapping cause %IDMGR-3-INVALID_ID: bad id in id_get (Out of IDs
CSCsv84557	AAA	Acct-Session-Id not getting created when unique-ident configured
CSCsv91587	AAA	ISG_PTA Session not coming up with aaa autho net def if-authenticated
CSCsw17553	AAA	Radius-server pac keyword is not nvgened when used with automated tester
CSCsw77313	AAA	failed authentication with login command changes the logged user
CSCsw80000	AAA	Radius Exec Callback denies all service-type values
CSCsx10449	AAA	aaa accounting delay-start commands allowed to exist at the same time
CSCsx31996	AAA	Booting RP after an RP s/o reset due to AAA HA failure
CSCsx97093	AAA	AAA Fails to parse RADIUS callback string ending in =
CSCsy39545	AAA	Tunnel-link-stop record is missing at LAC
CSCsy43147	AAA	crash found @ tplus_handle_sc_idle_timeout
CSCsz01313	AAA	PRE3 crash in aaa_idb_name_cleanup
CSCsz09373	AAA	POD Reply sent with physical intf ip when req rcvd with loopback intf ip
CSCsz21640	AAA	Crash with BusError when sending Accounting Stop
CSCsz27104	AAA	COA: session ID not decoded correctly causing COA nacks/push failures
CSCsz42529	AAA	RF Client AAA timeout : Standby keeps rebooting
CSCsz43356	AAA	CPUHOG and Traceback after multiple SSH logins
CSCsz61595	AAA	login on-failure does not behave consistently
CSCsz71782	AAA	ASR-RLS4: RSIM sends wrong format VSA 1 string crashes router
CSCta08360	AAA	LNS does not send SCCRP with false detection of duplicate SCCRQ.
CSCta16724	AAA	IOS release 12.4(24)T breaks partner SCP functionality
CSCta32501	AAA	Crafted RADIUS VSA attribute response causes device to crash
CSCta41064	AAA	console hangs with system accoutning and console authen with AAA Server
CSCta52869	AAA	3rd client is duplicated and overwrites 4th client in aaa pod server

Identifier	Technology	Description
CSCta79933	AAA	Different attributes sent to backup radius group
CSCta96363	AAA	"show tacacs" - Does Not Display Output for TACACS+ Private Servers
CSCtb14991	AAA	ASR SSO long failover time delay with no Radius Accounting Off
CSCtc39564	AAA	aaa accounting command is not recognized after reloading
CSCtc53436	AAA	IPv6 per user-static route missing on access server vrf routing table
CSCtc72940	AAA	ip vrf forwarding command not being executed under aaa
CSCtc83838	AAA	Memory leak from "aaa_req_alloc" on processing craft RADIUS packet.
CSCtc86075	AAA	Device reloads at print_acct_db
CSCtd00194	AAA	c1841 fails association with EAP authentication of non root bridge
CSCtd33642	AAA	RLS5: Flow Accounting fails with "delay start" configured
CSCtd43841	AAA	Framed-IPv6-Prefix attribute sent twice in Accounting Stop
CSCtd55353	AAA	show aaa memory detail causes Data Bus Error exception crash
CSCtd57788	AAA	Dynamic access list not removed when session goes down.
CSCte01126	AAA	ASR RP Crash due to l2tp_cc_get_l2x_internal process
CSCte48009	AAA	Nas-Port/NAS-Port-Id missing with PPPoEoA VCI larger than 32767
CSCte50206	AAA	Suppress null-username suppresses system accounting messages
CSCte52369	AAA	COA NACK error for first COA packet
CSCte83888	AAA	PoD Acct-Session-Id incorrectly converted to internal Session-Id
CSCte92659	AAA	Memory leak observed in AAA & SSS PM
CSCte98852	AAA	ASR1K: Duplicate session accounting-request message
CSCtf80580	AAA	ISG: radius-proxy client address config disappears after reload
CSCtf89408	AAA	ASR1K: RP Crash in memcpy, radius on RPSO with PPP connection establishm
CSCtf95308	AAA	ISG: Router crashes on adding unexpected values to radius profile
CSCtg44097	AAA	Connect-Info(77) attribute is sent twice in a Pre-Auth Access-Request
CSCtg58029	AAA	MF:%UTIL-STBY-3-TREE: Data structure error--attempt to remove an unthr
CSCtg91180	AAA	Junk Chars are thrown when Reply-Message attribute is present for user
CSCtg96280	AAA	To provide the support the cisco vsa for Framed IPV6 prefix.
CSCth18616	AAA	Fix issues in CSCtg14133 & CSCtg96280
CSCth23787	AAA	Router getting crash while unconfiguring "ipv6 mld join-group <add>
CSCth29393	AAA	ISG: Dowstream traffic stop being forward
CSCth38303	AAA	ISG: crash at radius_remove_pkt_id on non Cisco AZR reboot
CSCth40454	AAA	To resolve the build breakage for CSCth20315
CSCth64316	AAA	Unable to configure radius-server using snmp set
CSCth73173	AAA	PAC2 : ASR is crashing at 'be_radius_no_accounting_response_error'
CSCti01036	AAA	ASR1K crashes on Process Radius
CSCti37761	AAA	Device crashes with spurious access with AAA configured
CSCti59562	AAA	ISG DHCP acct stop does not clear IP initiated session

Identifier	Technology	Description
CSCtj37102	AAA	Authen TACACS server reused for exec author, but not command author
CSCtj48220	AAA	Router crash due to AAA
CSCtj56142	AAA	ISG considers dummy User-Name as session identifier
CSCtj63737	AAA	Crash at aaa_ha_print_all_stored_sp_name on executing sh aaa service-pro
CSCtj99431	AAA	Sessions coming up with shared key mis-match between ISG & Radius-Client
CSCtk00181	AAA	Password Aging with Crypto configuration fails
CSCtk36582	AAA	PWLAN: ACCT-ON/OFF clear all sessions within a client pool
CSCtl21684	AAA	username with access-class option does not pass local AAA authorization
CSCtl58005	AAA	IPv6 accounting delay; Accounting START sent before any NCP negotiated
CSCtl66117	AAA	Memory leak at the TPLUS process on a Standby SUP
CSCtn38037	AAA	"attribute acct-session-id overloaded" causing malformed radius packets
CSCtn67034	AAA	Username attribute is missing in the accounting records
CSCtn99665	AAA	Memory corruption in radius proxy on ISG
CSCto01943	AAA	Incorrect Acct-Authentic on PPP accounting start at ISG/LNS
CSCto49066	AAA	Radius proxy crashes with multiple accounting start/stop
CSCto71671	AAA	Radius source port extended does not always increase udp src port
CSCto82335	AAA	Outstanding Access Transaction left unprocessed after Radius comes alive
CSCto93880	AAA	IPv4 Enable authentication failed with tacacs
CSCtq21258	AAA	COA NACK'd when Radius pw larger then 32 bytes reduced to exactly 32 B
CSCtq36545	AAA	2960 %AAA-3-INVALIDPARM: invalid parameter was used when accessing AAA f
CSCtq75612	AAA	Cat2960S FlexStack configuration not synched despite config change
CSCtq99488	AAA	IP/IPv6 Session poisoned on Standby after CoA Account logon
CSCtr69926	AAA	Hot Stanby RP crash in convert_vsastring
CSCtr87070	AAA	TACACS Enable login with wrong source ip address
CSCts23882	AAA	ISG CoA: Invalid resp auth in CoA Account Profile Status Query Replies
CSCts84132	AAA	Kingpin: RP crash with Process = CDP Protocol
CSCtt04376	AAA	Username with access-class option fails AAA authorization with RADIUS
CSCtu34207	AAA	SessProvisioning fail in ISG-SCE interface after upgrade to 15.1
CSCtw57751	AAA	Tacacs enable authentication on IPv6
CSCtw60333	AAA	SS - HTTP Process getting hunged with Webauth using HTTPs request
CSCtw86212	AAA	ISG failing to support Radius Attribute filter configuration
CSCtw94598	AAA	Reported to RADIUS NAS Port type is changed from Ethernet to Async
CSCtx01026	AAA	Double password prompt for ssh authentication if cache is empty
CSCtx07303	AAA	Tacacs error messages "%TAC+: no address for get_server"
CSCtx31175	AAA	Framed-IP-Address added twice in accounting STOP record by ISGv4
CSCtx51420	AAA	RP crash just after boot on 15.2(02)S image nightly dated 14th jan
CSCtx63545	AAA	ISG crash with RP sessions when all radius servers are DEAD

Identifier	Technology	Description
CSCtx79286	AAA	RADIUS retansmit timer does not reflect actual timeout interval.
CSCtx80499	AAA	radius-server attribute 31 remote-id doesn't send remote-id in L2TPAVP22
CSCtx95339	AAA	ID leak while flapping walkby converted sessions in radius_parse_respons
CSCtx99544	AAA	Exception when no aaa accounting system default vrf VRF3
CSCty49762	AAA	EAP Framework and AAA AttrL Sub Uses All Process Memory
CSCty58241	AAA	Unexpected response increasing after change on radius host command
CSCtz18857	AAA	VRF-aware Radius test packet is not routable
CSCtz59615	AAA	Framed-IPv6-Route does not getput IPv6 route into IPv6 VRF routing table
CSCtz75380	AAA	ISG: creating invalid radius request packets during retransmission
CSCua94947	AAA	RP crashs when Framed-IPv6-Route downloaded from freeradius on MLPPP ses
CSCub17985	AAA	Memory leak with ppp event
CSCtj94631	Access	CEF switched locally generated traffic is not resettin dialer idle timer
CSCsz36400	Content	WCCP router may become confused with incompatible web-cache config
CSCtf28329	Content	wccp service group lookup takes place in VRF instead of global
CSCto64188	Content	ASR reload if mask assignment changes during "show ip wccp...detail" cmd
CSCec18644	Infrastructure	memory leak with wr mem command
CSCin89580	Infrastructure	Incorrect entry returned by SNMP query in CAT6k platform
CSCsq50191	Infrastructure	"do" -> "do-exec" MM 2, exec too at MM 3, with help and tab completion
CSCsz11746	Infrastructure	IOS Shell: Not skipping custom alias commands when prefixed with space
CSCta67945	Infrastructure	ifInOctets incorrect values when requested every second with other OIDs
CSCtb13469	Infrastructure	SYNCE:SIP400 crashed after we configure one input-source with MN SPA
CSCtc43231	Infrastructure	SNMP Informs Source Interface Command not working
CSCtc87480	Infrastructure	dir slavenvram and wr mem triggers slavenvram:/(Device or resource busy)
CSCte79777	Infrastructure	Syslog with filter: Process hog by Logger and crash
CSCte97113	Infrastructure	Standby crashes on config replace of parser view command
CSCtg17902	Infrastructure	Logger Process spiking the CPU utilization
CSCth01674	Infrastructure	*Dead* memory increasing in (coalesced)
CSCth83143	Infrastructure	IPv6 access list applied to SNMP community string does not work
CSCti10835	Infrastructure	Authorization failure, loopback interface creation, still creates it
CSCti18397	Infrastructure	Active RP crashed by stby due to missed keepalive
CSCti60077	Infrastructure	Memory leak in IP SNMP Process on cat6k
CSCti80535	Infrastructure	"Default interface range command" cause standby SUP reset
CSCti91384	Infrastructure	using logging persistent auto with boot image may partially erase config
CSCtj31116	Infrastructure	logging discriminator stops severity filtering
CSCtj92837	Infrastructure	Router throws the error messages NoSubTkn>, DblQuotTkn>, IOS.sh>,...
CSCtk18810	Infrastructure	Memory consumption - Virtual Exec process - get_block
CSCtk33038	Infrastructure	"exception crashinfo dump command" output missing from crashinfo file

Identifier	Technology	Description
CSCtk36938	Infrastructure	%SYS-SP-3-CPUHOG @preemption_forced_suspend
CSCtk68692	Infrastructure	kron-initiated write mem locks nvram indefinitely
CSCtl42934	Infrastructure	run sh mem debug leak chunk on stby RP will crash stby RP
CSCtl53576	Infrastructure	Router is getting Hang up at sh run
CSCtl97648	Infrastructure	Auto completion of cli's not working with xe33 throttle & t_base_1 image
CSCtl98778	Infrastructure	Memory leak at xos_mgd_timer_leaf_alloc
CSCtn17738	Infrastructure	Re-introduce "do write" in IOS 15.x
CSCtn50281	Infrastructure	SNMPv3 uses wrong mac for snmp engine ID
CSCtn56097	Infrastructure	mpls-lsp-monitor for pathecho fails
CSCtn78735	Infrastructure	"config replace" and "archive path" missing usbflash and flash on 1921
CSCtn87155	Infrastructure	Issue with bringup sessions and CoA with service template configuration
CSCto06848	Infrastructure	rttMonStatsCaptureTable loops infinitely after switchover on ASR
CSCto06915	Infrastructure	Sup720 remains in ROMMON after SP crash
CSCto70125	Infrastructure	High CPU due to IPSLA tcpConnect probess due to multiple start attempts
CSCtq16651	Infrastructure	IP SLA - udp-jitter probes do not work with VRF
CSCtq38731	Infrastructure	config mode exclusive not found in 15.0 ,only option is conf register
CSCtq55723	Infrastructure	IPSLA vrf: udp based operations and tcp-connect fail over a vrf
CSCtq56575	Infrastructure	rttMonEchoAdminTargetAddress does not replay with correct entry
CSCtq67750	Infrastructure	Customer hit CSCtn52350, is seeing before-after is on without turning on
CSCtq79382	Infrastructure	IP SLA Config Sync VRF
CSCtr45030	Infrastructure	Configuration mode is locked and standby resets
CSCtr55348	Infrastructure	Multiple issues if MIBs are polled and auto generated probes are present
CSCtr70655	Infrastructure	IOS.sh: Device crashes while editing an acl, then entering invalid text
CSCtr73288	Infrastructure	After a session timeout, standby console allows commands
CSCtr74573	Infrastructure	macro auto execute command not accepted by switch went sent by CNS CE
CSCtr74737	Infrastructure	"path flash" cmd fails in archive configuration in 1921 router
CSCtr89424	Infrastructure	twamp PI18: session table is not cleared after session is completed.
CSCts28977	Infrastructure	Role based CLI cmds not properly parsed by being at top of startup conf
CSCts67465	Infrastructure	MF:IPSLA VO: Reconfiguration of frequency value causes standby to reload
CSCtt21979	Infrastructure	Processor Pool Memory leak in IP SLA Responder with IPv6 Probes
CSCtt40507	Infrastructure	'no logging userinfo' no longer working
CSCtu09837	Infrastructure	XML-PI: BGP config partition is malformed
CSCtu16517	Infrastructure	IP SLA 3 show responder "Permanent Port" always Enabled
CSCtu30032	Infrastructure	user privlige issue when local authentication is configured
CSCtw46891	Infrastructure	IP SLA probes may not respond to SNMP jitter table
CSCtw55086	Infrastructure	"No Such Instance" for snmpwalk/get of rttMonJitterStatsTable
CSCtw59648	Infrastructure	BOOTLDR missing from show version

Identifier	Technology	Description
CSCtw71564	Infrastructure	MF: IPSLA-VO telpr. doesn't reports all packets (tx, rx) as test samples
CSCtw78343	Infrastructure	rttMonApplSupportedProtocols table missing on 151-4.M1
CSCtw88094	Infrastructure	MF:Standby reload due to line by line sync failure upon sch ipsla sessio
CSCtx05616	Infrastructure	cSUP2T - startup cfg is partially copied via rcp when compression is on
CSCtx19332	Infrastructure	cnma1b: Crash seen after "sh ethernet cfm maintenance-points remote"
CSCtx33213	Infrastructure	VTY idle exec-timeout during file copy
CSCtx74931	Infrastructure	SNMP get on some OIDs fails if zero in ipv4 addr
CSCtz44372	Infrastructure	GDB doesn't print full stack for process watchdog
CSCtz61205	Infrastructure	Issue with "show format disk0:spec.odm" on Cat6k - 15.0(1)IA273.286
CSCee38267	IPServices	NAT router may reload under heavy load of NAT traffic
CSCef16289	IPServices	Unconfiguring mapping and STATIC entries should be consistent
CSCeg27235	IPServices	DHCP: BOOTP sends RENEW request which causes problems
CSCsd17017	IPServices	New NAT entry in table when serial int flaps, seeing connectivity issues
CSCse99493	IPServices	Router crash with NAT overload and large number of NAT translations
CSCsx28813	IPServices	static translation with port doesn't work when applying NAT with route-m
CSCsz24818	IPServices	ASR:MCP_DEV- RP crash observed when trying to telnet using v6 address
CSCsz72591	IPServices	Router configured as a DHCP client crashes with crafted DHCP packet.
CSCth08845	IPServices	Bootcrash on ME3600x
CSCti71843	IPServices	Ping to NAT outside neighboring interface fails
CSCtj13146	IPServices	Stdby redundancy mode mismatch when switch from rpr mode to sso mode
CSCtl21294	IPServices	NAT: Port numbers are lost from running cfg if route-map option is used
CSCtq60703	IPServices	Device getting crashed while executing "do write network"
CSCtq84037	IPServices	ASR1006 does not update show redundancy history with my state informatio
CSCtq92940	IPServices	Active FTP transfers may become deadlocked -- CSCtl19967 replacement
CSCtr35456	IPServices	Router crash at datalist_next
CSCtr54218	IPServices	Sup7E showing incorrect uptime
CSCtr55973	IPServices	Spaces in bind authenticate string
CSCts00341	IPServices	CLI requiring DNS lookup cannot be configured when in SSO mode
CSCtw50141	IPServices	Incremental leaks at __be_ber_get_stringa pointing to LDAP Process
CSCtw61104	IPServices	DHCPv6 LQ:cmts crash with "Corrupted magic value in in-use chunk"
CSCtx40448	IPServices	MU: active SUP7e redundancy uptime wrong after SSO
CSCtx61491	IPServices	Static NAT Translations Fail When Destination Address is in 2 route maps
CSCtx95334	IPServices	TCAM entries are not correctly programmed for static nat w/ interface
CSCty98365	IPServices	mcp_dev crashes in rf mib code for b2b
CSCtz85702	IPServices	NAT TCP pptp-control timing-out use_count 1 - entry not removed
CSCua43193	IPServices	Dynamic NAT'g of TCP traffic fails when redudancy VIP is used for NAT
CSCua70136	IPServices	NAT VRF with PAT - PPTP translation failure with dynamic pool

Identifier	Technology	Description
CSCub18395	IPServices	PAT not working when shut/no shut nat+hrsp config interface
CSCtc42278	ISDN	%DATACORRUPTION-1-DATAINCONSISTENCY - ISDN incoming call
CSCtk95992	LegacyProtocols	DLSw fails to set up circuit using UDP with peer-on-demand
CSCsq41969	Management	Incorrect cikePeerLocalAddr & cikePeerRemoteAddr in cikeTunnelStop trap
CSCtd54694	Management	Switch crashes on Show cdp neighbor detail in some conditions
CSCte58825	Management	IOSD crash on SNMPWalk at get_ipsec_policy_map
CSCtg29298	Management	cipsCryptomapSetIfTable shows only first crypto map applied to interface
CSCti36310	Management	ASR memory leak when IKE attribute are pulled by snmp
CSCtr11469	Management	Crah seen @ cns_connect_socket_exception
CSCts54684	Management	Memory leak on IPSec background pc 'ipscmTT_addTunnel'
CSCtw59338	Management	MTRACE and crash following on switch using CDP
CSCtx01604	Management	Pointer truncation found in cns_ea_call_function()
CSCtx73612	Management	ASR crash while performing SNMP of IPsec stats.
CSCtj62999	MPLS	Session not coming up when PBR is configured on the VT
CSCtl02677	MPLS	CsC MPLS VPNs can not forward VRF traffic when using c7600
CSCtq36772	MPLS	rd value missing in sh run XML formatting
CSCtw66832	MPLS	Verbatim TE: Flood of "Path Error from Myself" when conn next-addr fails
CSCty71843	MPLS	Traceback @ lfd_sm_start/lfd_sm_handle_event_state_stopped during bootup
CSCua40273	MPLS	ASR1K:Crash at _be_mplsvpnmib_get_vrf_interface_info
CSCsy96166	Multicast	"ip service reflection" command removed from interface on reload
CSCth60923	Multicast	sg-expiry-timer not working on all routers
CSCtj61150	Multicast	MFIB: PIM-BIDIR: A flag lost on interfaces when RP mapping changes
CSCtj95782	Multicast	Multicast Tunnel Interface (MTI) getting assigned to vrf default
CSCtk59748	Multicast	Traffic loss seen for MVRFs after SSO Switchover
CSCtk76140	Multicast	Routing Protocols should not run over Multicast tunnel interfaces
CSCtl90570	Multicast	Pim neighborship is shown only one PE and not on both
CSCtn73737	Multicast	All SSM groups are pruned when configuring ip multicast boundary command
CSCtq14253	Multicast	ipv6 vrf-lite multicast joins/register not forwarded to RP
CSCtq46337	Multicast	Unavailable ipv6 ACL prevent configuring ipv4 ACL
CSCts06324	Multicast	PIM prunes not sent in PIM DM
CSCts41032	Multicast	%SYS-2-NOBLOCK: suspend with blocking disabled tracebacks.
CSCts97856	Multicast	Traffic loss during PIM assert due to 0/0 metric being sent
CSCtt17762	Multicast	mtrace output missing path information
CSCtu28623	Multicast	PIM does not trigger Prune to old RPF neighbor
CSCtw76855	Multicast	MRIB RPC timeout too low,need to increase this timeout to a higher value
CSCtx55357	Multicast	multicast boundary doesn't block Auto RP on ASR1k
CSCtz22062	Multicast	Intermittent duplicates and packet drops in an extranet scenario

Identifier	Technology	Description
CSCtz54535	Multicast	mroute sometime get "Outgoing int:null" when OTV ED gets back to AED
CSCua45122	Multicast	ipmulticast event trace consumes huge memory on 3k
CSCub09124	Multicast	MVPN MDT failure due to multicat boundary on non-current RPF interface.
CSCsi49953	QoS	sip1- tx cpu crashes @ blt_pak_holdq_peek with RCK070410
CSCsl70963	QoS	Priority and class default pkts drop-H/W MLP+fragment+llq on SIP400
CSCsl28726	Routing	Crash when PBR unconfigured
CSCsm53205	Routing	Flash updates in RIP are not filtered by output distribute-lists
CSCsq83006	Routing	Port-channel down makes EIGRP SIA
CSCsx64858	Routing	.PRE2 crashed in fib_fib_display_sw_or_plat_output_chain() when sh ip ce
CSCsz44301	Routing	DMVPN PH3: Adjacency issues doesn't bring mgre tunnel and nhrp
CSCta32721	Routing	show running partition router ospf/isis/bgp display eigrp config
CSCta69213	Routing	Bus error crash at rn_match part II
CSCtb87856	Routing	Hub Crash seen in performance testing
CSCtc23465	Routing	DMVPN tunnel config causes router to crash
CSCtc34209	Routing	NHRP Error Indication Packet Incorrect
CSCte37338	Routing	Error messages are thrown when creating virtual link.
CSCte50911	Routing	Rvd BGP AFI/SAFI for IPV6 is displayed as "Address family ?: received"
CSCte57710	Routing	Process replies to ping to I/F downed unlike cef handling.
CSCte66460	Routing	different behavior between static ipv4 and ipv6 routes
CSCte69608	Routing	ipv6 route can not be added to RIB after dot1q encap is delete and add
CSCte82226	Routing	SYS-SP-2-NOBLOCK error while changing the MTU on Port-channel
CSCtf04169	Routing	IPv6 should provide an API to send RS to solicit RA
CSCtf12730	Routing	iBGP route get redistributed into IGP in case of VRF lite
CSCtf19115	Routing	IBGP next hop self on RRs for IPv4/IPv6
CSCtf51640	Routing	corrupt debug ip packet detail # output
CSCtg07308	Routing	no ip nhrp map mult dyn doesnot clear dynamic entries on multicast table
CSCth33748	Routing	Traffic Forwarded via IP helper-address not dropped with egress acl
CSCth90147	Routing	IPv6 Ready Fail: Solicited RA not suppressed
CSCti16621	Routing	BGP Graceful Restart triggered when receiving a BGP NOTIFICATION
CSCti69990	Routing	Router getting crash at ipv6_nd_set_state
CSCti98347	Routing	NHRP Shortcut does not appear to update upon failure
CSCtj29754	Routing	IPv6 static routes cannot be installed in the routing table
CSCtj32137	Routing	RP Crash at fib_fib_src_remove_all_repopulating_sources
CSCtj38519	Routing	Pacing time increases proportionally with the number of peers on dmvpn
CSCtj55920	Routing	Incorrect TCP MSS with PMTUD disabled
CSCtj85792	Routing	IP CEF Switching statistics feature output mis-leading / confusing
CSCtj99048	Routing	NSF: type-5 lsa remains even after type-7 becomes unroutable v3 and v2

Identifier	Technology	Description
CSCtk67846	Routing	Show commands on ASR1000 are truncating long interface names
CSCtk95879	Routing	OSPF crash in print_ip_address_name
CSCtk97921	Routing	EIGRP: Router fails to send lower bandwidth value to stub router
CSCtk98559	Routing	Inconsistent show bgp ipv6 output
CSCtl03222	Routing	MP-BGP address family mdt tunnel takes 40 sec to come up
CSCtl23348	Routing	ospfv3 crashed in corner unconfig case
CSCtl24029	Routing	Partial Route Calculation Trigger overwrite ispf trigger
CSCtl48297	Routing	command "no router bgp" causes RP active crash on asr1006
CSCtl74193	Routing	Multicast RPF fails for routes matched on the default route
CSCtl76209	Routing	bgp dampening unconfiguration leads to peer reload in cat4k
CSCtl82255	Routing	Table version not matches main table version in ibgp
CSCtl90341	Routing	Crash was observed at spoke while verifying NHS Recovery
CSCtn04716	Routing	Stby reload forever after switchover for 'area range' cmd under AF
CSCtn13208	Routing	7606-S show mac-accounting input byte decrease
CSCtn26750	Routing	Config Sync: Line-by-Line sync verifying failure with ipsec spi change
CSCtn28089	Routing	Static route is not seen in RIP DB after I/F removal with static present
CSCtn36227	Routing	Alignment correction at ipv6_checksum with IPv6 ping sweep
CSCtn38722	Routing	BGP NHT - show ip bgp internal not showing correct information
CSCtn41793	Routing	ISG: Downstream traffic not flowing after OIR/SSO
CSCtn42588	Routing	SPF fails to run after fast neighbor flaps
CSCtn42601	Routing	OSPF: Trace-back @ __be_ospf_redistribute after route-map manipulation
CSCtn58005	Routing	IPv6 ISIS doesn't filter local L1 routes when redistributed into L2
CSCtn63216	Routing	ASR - NHRP registrations shouldn't do a routing table lookup
CSCtn78914	Routing	Missing route-map name in redistribute in IPV6 eigrp after reload ASR.
CSCtn83348	Routing	Unexpected sequence number displayed on ipv6 access-list
CSCtn92994	Routing	IP aliases may result in different routes on T-train and XE
CSCto05416	Routing	Encoding for BGP Link Bandwidth Community needs change from 0x0006
CSCto15667	Routing	Static rouote is not removed if aggregate-address is configured in BGP
CSCto17490	Routing	IPv6 traffic class being set to 128 when should be set to 0
CSCto55606	Routing	eigrp saf-neighbhorship is not stable with two loopbacks
CSCto60216	Routing	OSPFv3 related TB&Crash after "issu runversion"
CSCto73963	Routing	Routes over MPLS TE FA tunnel not in RIB (2nd part of CSCto46716)
CSCto85731	Routing	Crash seen @nhrp_cache_info
CSCto88581	Routing	Standby crash in nsr interface message checkpoint handler
CSCto98212	Routing	Router crashed when RIPng process is removed on interface twice
CSCtq27712	Routing	Missing Summary route originated by the router in the local table
CSCtq43285	Routing	Routing churn BGP-EIGRP in VRF-Lite

Identifier	Technology	Description
CSCtq56948	Routing	Inherit default route flag on the IPL and the RR sourced pref
CSCtq57742	Routing	Router crashes for corrupted chunk memory when BGP neighbor is shutdown
CSCtq71011	Routing	BGP_DP: Crash seen at bgp_compute_bestpath
CSCtq71368	Routing	Standby reloads continuously when loopback ip is changed and switchedove
CSCtq78386	Routing	ipv6 address family not getting removed with summary-prefix
CSCtq95384	Routing	BGP still holding memory even after removal in scale NSR scenario
CSCtq98469	Routing	route-map set ipv6 set next-hop does not apply change to prefix
CSCtq99664	Routing	Traffic not flowing for set VRF under ipv6 route-map
CSCtr12019	Routing	NHS registration not attempted on P2P GRE
CSCtr14728	Routing	OSPF-NSR:summarized type 5 LSA getting MAXAGE after RP SO
CSCtr19922	Routing	Potential crash executing 'show adj internal dependents'
CSCtr25386	Routing	BFDv6 static route association fails after re-enabling interfaces
CSCtr29098	Routing	BGP filter-list denying everything in 12.2(33)SRE2
CSCtr43437	Routing	DMVPN HUB not seeing eigrp hello's from spokes after failover
CSCtr47642	Routing	BGP_DP: Bestpath selection takes too long in certain condition
CSCtr53941	Routing	BGP_DN: Incorrect dynamic neighbor counter value
CSCtr57804	Routing	ASR deletes ipv6 prefix no-advertise command from subinterfaces
CSCtr69416	Routing	conected routes get redistributed without ospf process enabled.
CSCtr69492	Routing	Show interface loop 0 unnumbered , shows wrong "number of IP add polled"
CSCtr70641	Routing	EIGRP doesn't learn routes in mixed eigrp tlv versions running setup
CSCtr78977	Routing	DMVPN Phase 2: Need to clear NHRP Temporaries when used NHS is down
CSCtr86436	Routing	Router doesn't respond to ICMP echo-req from vrf to global loopback
CSCtr86666	Routing	EIGRP flap waiting for INIT ACK, out of order seq
CSCtr89882	Routing	NGMWR:Platform errors are seen in load balance sceanrio
CSCts23708	Routing	Flex NHRP does not not install route for remote spoke tunnel address
CSCts25780	Routing	ip vrf import map issue
CSCts39240	Routing	BGP_DP: advertise command not available under template peer-policy
CSCts50099	Routing	'show ipv6 traffic' only counts IPv6 process-switched traffic
CSCts55371	Routing	LSAs are not flooded to the peers.
CSCts57162	Routing	OSPFv2: missing routes after OSPF-4-CONFLICTING_LSAID
CSCts68630	Routing	IPV6 ACLs doesn't match the traffic as configured
CSCts84357	Routing	IS-IS Needs to use a single BFD client Handle
CSCts97925	Routing	IPv6 pings fail within the same VRF through global next hop
CSCtt02313	Routing	PfR: Uncontrol TC due to Exit Mismatch
CSCtt02645	Routing	opSYS-3-CPUHOG when clearing nhrp on DMVPN hub
CSCtt07525	Routing	Flex: Crash on remote spoke when clearing NHRP locally.
CSCtt17301	Routing	PE sends invalid BGP label for VPNv4 prefix

Identifier	Technology	Description
CSCtt17785	Routing	ASR doesn't exchange routes with ASA, reports ASA as version 0.0/0.0
CSCtt20427	Routing	PE with additional-path install does not send VPNv4 updates
CSCtt35936	Routing	RLS3.4 EIGRP route updates are not sent to DMVPN spokes
CSCtt43933	Routing	ASR1K : Conflict on Expanded named vs. Numeric extcommunity-list
CSCtt45789	Routing	%UTIL-3-TREE: Data structure error--attempt to reference an uninitialize
CSCtt95505	Routing	Router crashes on ipv6 routing protocol config
CSCtt98511	Routing	Interface i/p rate and o/p rate not consistent for IPv6 traffic (3925)
CSCtu08647	Routing	RR functionality still present, when peer moved from ibgp to ebgp
CSCtu10243	Routing	bgp fast-external-fallover not work immediately
CSCtu11013	Routing	TBs and crash upon receipt of EIGRP SAF services from Pagent
CSCtu18201	Routing	[RLS12} Observe router crash after the router bootup Mcp_31st
CSCtu19450	Routing	IOSD crash @ SNMP - ipv6_compare_address_lex
CSCtu22167	Routing	RP crash due to mistral error interrupt on LC OIR
CSCtu28696	Routing	ASR1k RP exception @ rip_process_mgd_timers on clear ip route*
CSCtu28990	Routing	RLS10.2:RP crash observed @SYS-6-STACKLOW: Stack for process XDR mcast
CSCtu41137	Routing	IOSD Core@fib_table_find_exact_match while unconfig tunnel int
CSCtu72236	Routing	Dynamic BGP failure with MD5 configured
CSCtw58685	Routing	NAT doesn't send gratuitous arp for translated address in C3900
CSCtw59780	Routing	dynamic neighbors are not cleaned up after peer flap
CSCtw62514	Routing	OSPFv3: default hello/dead interval incorrect for P2MP
CSCtw65210	Routing	Shut/no shut redistribute static using interface might cause BGP Next-ho
CSCtw72975	Routing	ISIS inter-/intra-process route ownership corrupts RIB/L1/L2 DB
CSCtw79182	Routing	PE-CE OSPFv2: DN-bit ignoed for External LSA
CSCtw86712	Routing	ASR1K : RP Crashes@oce_base_explore_chain
CSCtx04709	Routing	Active routes remain in topology but does not go SIA after route lost
CSCtx23014	Routing	HSRP hellos cannot be sourced from certain IPs for specific vlan
CSCtx29557	Routing	standby crash @ fib_fib_src_interface_sb_init
CSCtx44508	Routing	enabling iBGP NSR delays sync after switchover
CSCtx45373	Routing	"%VRF specified does not match this router" message seen during reload
CSCtx47213	Routing	session with iBGP local-as flaps due to bad attrb. NOTIF on rcv RR route
CSCtx52095	Routing	I/O Leak for Middle Buffer at nhrp_getbuffer
CSCtx56389	Routing	ASR1k: IP ARP req filtered ..it's our address even if vrf is used.
CSCtx66046	Routing	OSPF NSR: Stby crashes @ __be_db_free_check
CSCtx67474	Routing	updt sent with empty nlri when msg consist of 2byte ASpath & 4byte AGGR
CSCty01913	Routing	sh ip int Output Feature should be empty LI
CSCty02403	Routing	EIGRP topo entry with bogus nexthop created when SoO and TAG are present
CSCty04423	Routing	Discrepancy between SNMP-reported & Actual BGP Neighbor State

Identifier	Technology	Description
CSCty05150	Routing	OSPF default summary route withdrawn after SSO switchover on ABR
CSCty08070	Routing	OSPFv3: Traceback@process_events_waiting_p
CSCty11254	Routing	BGP-PIC:Table version not bumped causing stale repair path in RIB table
CSCty22787	Routing	ISIS multi-topology transition mode does not correctly init MTID 0
CSCty37445	Routing	Split Horizon Automatically turned off with distribute-list route-map
CSCty61269	Routing	RT extended community not carried as part of C-multicast routing
CSCty64255	Routing	Issue with Prefix limit in BGP L3VPN Route leaking Feature
CSCty68348	Routing	ospf state not synced to stdby after shut/no shut of ospf proc on active
CSCty84356	Routing	ospfv3 area range commands cause standby to reboot due to sync
CSCty90223	Routing	Crash seen at nhrp_nhs_recovery_co_destroy during setup and config
CSCty91465	Routing	Enabling CEF causing pings between VRF and global routing table to break
CSCty96052	Routing	Extreme corner case: Crash during BGP scanner process run
CSCtz03779	Routing	ASR903:Stdby crash @ fib_vrf_mgr_lookup_vrf on ISSU from 3.6 -> 3.5
CSCtz05394	Routing	LDP-IGP Synchronization not enabled after OSPF protocol shutdown
CSCtz14634	Routing	Negative BW values on the opaque-lsa - 20 GIG link
CSCtz14713	Routing	OSPF - BFD Race Condition when router-id is changed
CSCtz25825	Routing	Null0 route is remaining in multiple VRF even if remove aggregate-addres
CSCtz26683	Routing	RPF chk not supported on tunnel but getting configured.
CSCtz31972	Routing	Rcvd in Used as bestpath does not count up in show ip bgp neighbor.
CSCtz44989	Routing	Redistribution between two different EIGRPv6 VRF using BGP doesnt work
CSCtz48338	Routing	BGP Scanner crashing on ActiveRP and StandbyRP on VRF deletion
CSCtz56671	Routing	Watchdog Crash when Removing ACL Statement
CSCtz58710	Routing	IPRT-3-INVALID_NEXTHOP for process OSPF Router
CSCtz71084	Routing	BGP PIC EDGE prefix leak after removal of prefix
CSCtz76650	Routing	IPv6 nhrp phase 2 doesn't work with EIGRP or OSPF as routing protocol
CSCtz80329	Routing	DMVPN: NHRP cache is converted to host address within different subnet
CSCtz98347	Routing	Repair path is not available for metric more than 1024 with ISIS LFA
CSCua06598	Routing	Router crash when polling inetCidrRouteEntry ipv6 MIB
CSCua16758	Routing	Counters fluctuating on BGP Nei. shutdown causing skewed metrics
CSCua19425	Routing	ASR Watchdog Timeout: BGP Router during BFD message servicing
CSCua24689	Routing	2547oDMVPN : fragment sent without label with vfr
CSCua27852	Routing	traffic loss is seen in pure BGP NSR environment
CSCua38237	Routing	ISIS PSNP packets are sent with empty MD5 hash
CSCua38597	Routing	bgp remove-private -AS does not remove private asn with continue clause
CSCua40790	Routing	Incremental leaks at IPToOctetString on polling MIBs on the router
CSCua47570	Routing	Observing rp crash @ ospfv3_show_event_data_rib
CSCua91104	Routing	ISISV6BFD: Traceback seen 'Process = ISIS Adj'

Identifier	Technology	Description
CSCub10951	Routing	BGP-DP: Missing updates for inter-cluster BE
CSCub53660	Routing	IS-IS does not remove alternate paths when best path changes level
CSCub54872	Routing	fib missing connected interface for interface receive prefix
CSCsd72758	Security	Scheduler Thrashing in the SSH Process
CSCsm23548	Security	MF:standby crashed during pasting configuration on the active console.
CSCsw30535	Security	Crash on certificate re-enrollment using SCEP
CSCsx65975	Security	ISSU(rls2.3->rls3.0) corrupted memory and mcp_fastpath crashes with ssh
CSCsx68728	Security	BSTUN Async-generic broadcast frames replicated to remote TCP peers
CSCsy33068	Security	CVO SDP webpage size problem
CSCsy34256	Security	Tracebacks are observed at SSL_shutdown
CSCsz81724	Security	PKI storage commands removed when usb device not connected at boot time
CSCsz84055	Security	System crashed unexpected while open ssh2 session
CSCsz93306	Security	SCEP server always replies with md5/des
CSCta73534	Security	IOS scp server deletes file when EOF not received but doesn't send error
CSCta98976	Security	IOS CS crashes when migrating to rollover CA cert
CSCtb11454	Security	Configuration not auto-saved when rolling over (new CA validity start)
CSCtb26396	Security	SSL socket_connect failed occurs under load requiring GW reload
CSCtb95267	Security	Saving config w/o USB present erases reference to certificates on USB
CSCtc49391	Security	Router fails to enroll with CA server
CSCtc88738	Security	SSH Blank PW Change Method Doesn't Work when using psswd authentication
CSCtd34056	Security	Cisco ASR 1002 - "crypto pki crl ca size" to be saved in the config
CSCtd54301	Security	Router got struck @ syntax-conf-ssh-pubkey-data
CSCtd72194	Security	Memory leaks seen in Crypto PKI RECV process
CSCtd73923	Security	PKI_Token-Unable to remove rsa keys from the token
CSCtd89026	Security	SecureCRT 4.09 fails to connect, post CSCin90961
CSCtd90960	Security	Reverse SSH to aux line fails during multiple authentication retries
CSCtd92020	Security	Authenticating Trustpoint fails when vrf configured
CSCte61528	Security	Router getting crashed at crypto_ca_trust_point_command
CSCte64621	Security	VSA stops passing traffic after IPSEC rekey
CSCte68288	Security	PKI: Spurious memory access @ name_lookup_viewname
CSCte79081	Security	after "crypto pki import", do enroll CA, the router will stuck in enroll
CSCte91782	Security	Unable to unconfigure crypto pki server < >
CSCtf25293	Security	Authorization is not working properly in pubkey feature
CSCtf65159	Security	spurious memory access @ tti_delete_from_url_profile_list
CSCtf69128	Security	The CRL Cache Size Test after reload Fails
CSCtg22080	Security	memory leak @ crypto_ca_cert_hexmode_quit_function

Identifier	Technology	Description
CSCtg23653	Security	Offline LDAP server can cause PKI delays
CSCtg28806	Security	Router crash at PKI enroll
CSCtg38344	Security	Router does not load any config after ip ssh pubkey-chain on a reload
CSCtg51619	Security	OCSP revocation check does not use source interface loopback
CSCtg55650	Security	Offline server test needs to check source interface
CSCtg57831	Security	HA CA servers: serial number mismatch on active and standby
CSCtg67747	Security	VSA drops dlsw traffic after E1 flap [crypto_engine_ps_vec(): no subbloc
CSCtg73401	Security	router crashed using command: sh cry pki cert verbose
CSCth37092	Security	Active router crashes during sync while implementing PKI-HA feature
CSCth55579	Security	Router reloads at clean_out_RA_certs after enrolling with CA server
CSCth56306	Security	IOS PKI:SUBCA Cert - incorrect start date
CSCth66192	Security	SCP to unreachable host cause ASR crash
CSCti03199	Security	config-sync failure due to deleted idb associated with crypto pki trustp
CSCti22544	Security	CRL retrieval fails: LDAP with dirName or URI without host
CSCti26202	Security	ModExp Hardware support (DH Scale/performance improvement)
CSCti34795	Security	PKI: RA mode SCEP requests will not time out or cannot be canceled
CSCti58272	Security	PKI Server grant auto trustpoint feature does not support PKIAAA
CSCti74453	Security	Server key lost & pki server fails to come up on Standby after failover
CSCti80904	Security	Steelers boxes reloads at sec_send_command while bootup
CSCti86043	Security	Configuration Change to PKI Certificate Crashes The Router
CSCtj81938	Security	l3vpn profile configurations are getting lost after SSO
CSCtj84001	Security	%SYS-2-MALLOCFAIL:malloc_named_dynamic_chunk Memory allocation failed.
CSCtk18607	Security	Router crash at ssh_pubkey_command_nvgen and ssh_pubkey_nvgen
CSCtk62247	Security	Ikev2 session fails with rsa-sign when hierarchical ca servers used
CSCtk62950	Security	crash when suspending ssh session
CSCtl92013	Security	SDP returns 'Failed to verify the signature'
CSCtn17867	Security	IOS HA CA: %Failed to revoke certificate error reported on standby
CSCtn22691	Security	CRL timer is not updated on the standby CA after intial expiration
CSCtn40571	Security	IOS Sub-CA may install multiple rollover certs
CSCtn71224	Security	IOS CA Server may fail to auto-grant Sub-CA certificate requests
CSCtn85411	Security	Encrypt pre-shared key cause existing pre-share key stop to work
CSCtn90611	Security	unicast/multicast pak getting dropped with VAM2+ and counter anti-replay
CSCto11238	Security	OSPF cannot be enabled on Tunnel interface
CSCto11371	Security	Crash encountered while validating OCSP responder certificate
CSCto55026	Security	PKI fails if DNS lookup is required
CSCto59568	Security	AAA+SSH Memory leak during SCP copy
CSCto62631	Security	12.2(58)SE crashes on second SSH session when banner is enabled

Identifier	Technology	Description
CSCtq21131	Security	VSA: NAT-Demux outside_rport is displayed as Unassigned state
CSCtq21785	Security	Crash Due To Performing A CRL Check On An Invalid Certificate
CSCtq29642	Security	VRF Command Disappears From Trustpoint Configuration Upon Reload
CSCtq30686	Security	RA crashes on granting request that was earlier stuck in granted state
CSCtq33102	Security	Cisco router crashes in an SDP enviroment with CVO
CSCtq36976	Security	VSA breaks BFD when crypto map on same interface
CSCtq53502	Security	IPv6 rd won't come up after a reload unless a workaround is exectuted
CSCtq76032	Security	Unable to grant all pending requests on RA
CSCtr06926	Security	CA Server goes to Disable State ones Trustpoint authenticated
CSCtr07339	Security	Enrollment via SCEP fails when v6 address is configured
CSCtr20273	Security	ECDSA CSR doesn't use appropriate security
CSCtr40792	Security	Tunnel hwidb reused before free on standby
CSCtr62854	Security	IOS SubCA server missing "Key Cert Sign" key usage and "CRL Signature"
CSCts05026	Security	Router crashes at "(conf-ssh-pubkey)#no server"
CSCts27333	Security	MTU inconsistent in the standby VSS sup, traffic punted in some cases
CSCts31860	Security	Deprecated : "ip scp source-interface" Hidden command
CSCts45908	Security	corrupt cert file crash XE router
CSCts65564	Security	DMVPN hub router crash when crl caching is disabled
CSCts82058	Security	Creation of Overlay interface leading (tunn) to continuous router crash
CSCts82990	Security	OCSP URL DNS resolution not vrf-aware
CSCtt05212	Security	SCP not working with AES
CSCtt11210	Security	PKI - IKE cert-req contains issuer-name instead of subject-name of SubCA
CSCtt14527	Security	Crypto timers are not re-evaluated after NTP synchronizes
CSCtt18020	Security	crash cleaning up ssh session
CSCtt46762	Security	"clear line vty" doesn't clear SSH v1 session when interface is shutdown
CSCtt70585	Security	IPSec IPV6 Tunnel is not forwarding traffic
CSCtw52819	Security	OQD:Packet Drops seen on mGRE tunnel.
CSCtw55424	Security	SSH support for vrf with ipv6 addr/hostname
CSCtw56439	Security	IPSEC: "IP MTU" CLI disappears after the router is reloaded
CSCtx14467	Security	device crashes if kron used to copy over config via scp
CSCtx60792	Security	IOS PKI fails to receive CA rollover shadow certificate
CSCtx87185	Security	008 Output missing for show crypto pki certificates
CSCty04359	Security	Manually created WExp certificate - after upgrade Wexp went to offline
CSCty32463	Security	Kingpin & 1RU Unable to sync in SSO mode w/ 'crypto pki' configuration.
CSCty51453	Security	OCSP Bad requests - incorrect length or truncated payload
CSCtz00581	Security	IOS PKI HA: manual granting does not work when active router powered off
CSCua01008	Security	Chunk leak in Crypto IKMP - 124-24.T5

Identifier	Technology	Description
CSCua43930	Security	"Checksum value parsed from GRE Header is incorrect "
CSCua71038	Security	Crash while checking OCSP certificate status and CRL chaching
CSCub35403	Security	CRL is not retrieved when attemping to use more than one possible signer
CSCte91471	WAN	NTP v4 takes several hours to sync when multiple servers are configured
CSCtf88705	WAN	NTP sync fail after change of interface ip.
CSCth66604	WAN	Modify Action routines of few cli's for ISSU compatibility
CSCti42915	WAN	Interoperability test for NTPv4 and NTPv3 using authentication
CSCti46834	WAN	NTP sync problem with satellite link
CSCti82141	WAN	ntp pps-discipline CLI gets removed after reload when inverted included
CSCtj69886	WAN	NTP multicast mode not working over MVPN
CSCtk10401	WAN	Local log archive shows 'ntp authentication-key 1 md5 pwd' in clear text
CSCtk74660	WAN	CRIS issue. NTP: time updates > panic threshold should be ignored
CSCto29467	WAN	Issues found during Unit Test after getting latest NTP v4 open source
CSCto55708	WAN	Build Error @ /ip-core-apps/ntp/ntpcore/src/refim/ntp_loopfilter. c:350
CSCto71384	WAN	892J Source address is incorrect after source interface is down
CSCtt04371	WAN	Need to change the default setting in NTPv4 for faster sync
CSCtu40183	WAN	NTP status Unsynchronized for Cluster member switches
CSCtw45592	WAN	CLI "NTP Server <dns name>" - does not get synced to standby
CSCty22840	WAN	Router crashes due to CPU Watchdog on NTP Process
CSCty46031	WAN	NTPv4 ntp response for ipv6 is sending the response in port 123

Troubleshooting

These sections describes troubleshooting guidelines for the Catalyst 6500 series switch configuration:

System Troubleshooting

This section contains troubleshooting guidelines for system-level problems:

- When the system is booting and running power-on diagnostics, do not reset the switch.
- After you initiate a switchover from the active supervisor engine to the redundant supervisor engine, or when you insert a redundant supervisor engine in an operating switch, always wait until the supervisor engines have synchronized and all modules are online before you remove or insert modules or supervisor engines or perform another switchover.

- If you have an interface whose speed is set to **auto** connected to another interface whose speed is set to a fixed value, configure the interface whose speed is set to a fixed value for half duplex. Alternately, you can configure both interfaces to a fixed-value speed and full duplex.
- If you apply both ACL and FnF with sampler on the SVI interface, the operational state of the Feature Manager gets reduced which causes the traffic to get software switched. In this state, if incoming traffic rate is high, CPU utilization will also go high. Therefore, apply ACL and FnF without sampler on the SVI interface. Otherwise, apply ACL and FnF with sampler on the physical interface.

Module Troubleshooting

This section contains troubleshooting guidelines for module problems:

- When you hot insert a module into a chassis, be sure to use the ejector levers on the front of the module to seat the backplane pins properly. Inserting a module without using the ejector levers might cause the supervisor engine to display incorrect messages about the module. For module installation instructions, refer to the *Catalyst 6500 Series Module Installation Guide*.
- Whenever you connect an interface that has duplex set to autonegotiate to an end station or another networking device, make sure that the other device is configured for autonegotiation as well. If the other device is not set to autonegotiate, the autonegotiating port will remain in half-duplex mode, which can cause a duplex mismatch resulting in packet loss, late collisions, and line errors on the link.

VLAN Troubleshooting

Although DTP is a point-to-point protocol, some internetworking devices might forward DTP frames. To avoid connectivity problems that might be caused by a switch acting on these forwarded DTP frames, do the following:

- For interfaces connected to devices that do not support DTP, in which trunking is not currently being used, configure interfaces with the **switchport mode access** command, which puts the interface into access mode and sends no DTP frames.
- When manually enabling trunking on a link to devices that do not support DTP, use the **switchport nonegotiate** and **switchport mode trunk** commands, which puts the interface into trunking mode without sending DTP frames.

Spanning Tree Troubleshooting

The Spanning Tree Protocol (STP) blocks certain ports to prevent physical loops in a redundant topology. On a blocked port, switches receive spanning tree bridge protocol data units (BPDUs) periodically from neighboring switches. You can configure the frequency with which BPDUs are received by entering the **spanning-tree vlan** *vlan_ID* **hello-time** command (the default frequency is set to 2 seconds). If a switch does not receive a BPDU in the time period defined by the **spanning-tree vlan** *vlan_ID* **max-age** command (20 seconds by default), the blocked port transitions to the listening state, the learning state, and to the forwarding state. As it transitions, the switch waits for the time period specified by the **spanning-tree vlan** *vlan_ID* **forward-time** command (15 seconds by default) in each of these intermediate states. If a blocked spanning tree interface does not receive BPDUs from its neighbor within 50 seconds, it moves into the forwarding state.

Note We do not recommend using the UplinkFast feature on switches with more than 20 active VLANs. The convergence time might be unacceptably long with more than 20 active VLANs.

To debug STP problems, follow these guidelines:

- The **show vlan virtual-port** command displays the number of virtual interfaces.
- These maximum numbers of virtual interfaces are supported:

	MST	RPVST+	PVST+
Per-switch limits:	100,000 total	12,000 total	15,000 total

Note Cisco IOS software displays a message if you exceed the maximum number of virtual interfaces.

- After a switchover from the active to the redundant supervisor engine, the ports on the redundant supervisor engine take longer to come up than other ports.
- Record all spanning tree-blocked ports in each switch in your network. For each of the spanning tree-blocked ports, record the output of the **show interface** command. Check to see if the port has registered many alignment, FCS, or any other type of line errors. If these errors are incrementing continuously, the port might drop input BPDUs. If the input queue counter is incrementing continuously, the port is losing input packets because of a lack of receive buffers. This problem can also cause the port to drop incoming BPDUs.
- On a blocked spanning tree port, check the duplex configuration to ensure that the port duplex is set to the same type as the port of its neighboring device.
- On trunks, make sure that the trunk configuration is set properly on both sides of the link.
- On trunks, if the neighboring device supports it, set duplex to full on both sides of the link to prevent any collisions under heavy traffic conditions.

Additional Troubleshooting Information

For additional troubleshooting information, refer to the publications at this URL:

http://www.cisco.com/c/en/us/support/switches/catalyst-6500-series-switches/tsd-products-support-troubleshoot-and-alerts.html

System Software Upgrade Instructions

See this publication:

http://www.cisco.com/c/en/us/support/docs/switches/catalyst-6500-series-switches/28724-161.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 THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

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

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.

This document is to be used in conjunction with the *Catalyst 6500 Series Cisco IOS Software Configuration Guide* publication.