Release Notes for Cisco CSR 1000v Series, Cisco IOS XE 3S

Last Updated: 6/16/20

These release notes provide information about Cisco CSR 1000v Series Cloud Services Routers, for Cisco IOS XE 3S releases—through Cisco IOS XE 3.17S.

Cisco CSR 1000v Series Cloud Services Routers Overview

The Cisco CSR 1000v Cloud Services Router provides a cloud-based virtual router that is deployed on a virtual machine (VM) instance on x86 server hardware. The Cisco CSR 1000v router is a virtual platform that provides selected Cisco IOS XE security and switching features on a virtualization platform.

Cisco Systems, Inc.
www.cisco.com

When the Cisco CSR 1000v virtual IOS XE software is deployed on a VM, the Cisco IOS software functions just as if it were deployed on a traditional Cisco hardware platform. You can configure different features depending on the supported Cisco IOS XE software image. The Cisco CSR 1000v supports a subset of Cisco IOS XE software features and technologies.

The Cisco CSR 1000v provides secure connectivity from the enterprise premise (such as a branch office or data center) to the public or private cloud.

Cisco IOS XE 3S Releases and Cisco IOS Release Number Mapping

The Cisco CSR 1000 Series Cloud Services Routers releases correspond to the Cisco IOS XE releases. For example, Cisco IOS XE Release 3.13(0) is the software release for Cisco CSR 1000v Series Cloud Services Routers Release 3.13.0S.

Table 1 lists the mappings between the Cisco IOS XE 3S releases and their associated Cisco IOS releases.

Table 1 Cisco IOS XE 3S–to–Cisco IOS Release Number Mapping

Cisco IOS XE 3S Release	Cisco IOS Release
3.9(0)	15.3(2)S
3.10(0)	15.3(3)S
3.11(0)	15.4(1)S
3.12(0)	15.4(2)S
3.13(0)	15.4(3)S
3.14(0)	15.5(1)S
3.15(0)	15.5(2)S
3.16(0)	15.5(3)S
3.17(0)	15.6(1)S

Feature Navigator

You can use Cisco Feature Navigator to find information about feature, platform, and software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on cisco.com is not required.

System Requirements

The following sections describe the system requirements for the Cisco CSR 1000v Series Cloud Services Routers.

Hardware Requirements

Hardware Requirements (Cisco IOS XE 3.10S and Later)

For installation and hardware requirements, see the *Cisco CSR 1000v Series Cloud Services Router Software Configuration Guide*.

Hardware Requirements (Cisco IOS XE 3.8S and 3.9S)

The Cisco CSR 1000v router is a virtual machine, and can be supported on selected x86 hardware.

The following are the minimum requirements for the Cisco IOS XE 3.8S and 3.9S releases.

- The Cisco CSR 1000v router VM:
  - 4 virtual CPUs
  - 4 GB RAM
  - 8 GB Hard Drive
- PC running the VMware vSphere Client 5.0
- Server running VMware ESXi 5.0
  - CPU: Intel Nehalem or later is required.
  - Hardware Compatibility: Must be listed as supported on the VMware Hardware Compatibility List.

    The Cisco CSR 1000v is supported on all Cisco UCS servers. Table 2 lists the Cisco UCS and non-Cisco servers that have been tested for compatibility.

Table 2 Servers Tested with Cisco CSR 1000v Release 3.9(0)S

Vendor	Servers Tested for Compatibility
Cisco	• UCS B230 M2 • UCS C220 M3 • UCS C210 M2 • UCS C200 M2 • UCS B22 M3
HP	• HP ProLiant DL180G6
Dell	• Dell R720 with Xeon® E5-2660

Note Cisco UCS B230-M2, B440-M2, C260-M2, and C460-M2 servers with Intel Westmere-EX CPUs require UCS release 2.0(4) or later.

- Memory: 16GB DDR3 or higher
- Hard Drive: 100GB or higher
- Network Cards: 1 Gbps (3 or higher)
- The minimum clock rate supported is 1.9 Ghz

Note The Cisco CSR 1000v router supports a maximum of 10 vNICs (the maximum supported by ESXi 5.0)

Software Images and Licenses

Cisco Smart Licensing

Beginning with Cisco IOS XE Release 3.15S, the Cisco CSR 1000v supports activation using Cisco Smart Licensing. To use Cisco Smart Licensing, you must first configure the Call Home feature and obtain Cisco Smart Call Home Services. For more information, see the *Cisco CSR 1000v Cloud Services Router Software Configuration Guide*.

Cisco CSR 1000v Evaluation Licenses

Evaluation license availability depends on the software version:

- (Cisco IOS XE 3.12S and earlier) Evaluation licenses valid for 60 days are bundled with the software image. The evaluation license is for the Premium technology package.

  For instructions on activating the evaluation license, see the "Installing Evaluation Licenses for Cisco IOS XE 3.12S and Earlier" section of the *Cisco CSR 1000v Software Configuration Guide*.

- (Cisco IOS XE 3.13S and later) Evaluation licenses valid for 60 days are available at the Cisco Software Licensing (CSL) portal: http:/www.cisco.com/go/license

  The following evaluation licenses are available:

  - AX technology package license with 50 Mbps maximum throughput
  - APPX technology package license with 10 Gbps maximum throughput

  If you need an evaluation license for the Security technology package, or for an AX technology package with higher throughput, contact your Cisco service representative.

  For instructions on obtaining and installing evaluation licenses, see the "Installing Evaluation Licenses for Cisco IOS XE 3.13S and Later" section of the *Cisco CSR 1000v Software Configuration Guide*.

Cisco CSR 1000v Software Licenses

Cisco CSR 1000v software licenses are divided into feature set licenses. Supported feature licenses depend on the release.

Legacy License Types

Three legacy technology packages—**Standard**, **Advanced**, and **Premium**—were replaced in Cisco IOS XE Release 3.13 with the **IPBase**, **Security**, and **AX** technology packages.

The following feature sets are supported in Cisco IOS XE 3.12S and earlier:

- Standard Package: Basic Networking Routing (Routing, HSRP, NAT, ACL, VRF, GRE)
- Advanced Package: Standard package + Security features (IP Security VPN, Firewall, MPLS, Multicast, QoS)
- Premium Package: Standard package + Security features + Advanced Networking features (AppNav, AVC, OTV and LISP)

Current License Types

The following feature sets are supported beginning in Cisco IOS XE 3.12.1S:

- IPBase: Basic Networking Routing (Routing, HSRP, NAT, ACL, VRF, GRE)

  The IPBase package replaces the Standard package (legacy).
- Security: IPBase package + Security features (IP Security VPN, Firewall, MPLS, Multicast, QoS)

  The Security package replaces the Advanced package (legacy).
- AX: IPBase package + Security features + Advanced Networking features (AppNav, AVC, OTV and LISP)

  The AX package replaces the Premium package (legacy).

Note Cisco recommends using the IPBase, Security, or AX technology packages for compatibility with future releases. All technology packages support the same throughput maximums as the similar feature sets in earlier releases.

The following feature set is supported beginning with Cisco IOS XE 3.13S:

- APPX Package: IPBase package + Advanced Networking features - Security features (IP security features not supported)

Features Supported by License Packages

For more information about the Cisco IOS XE technologies supported in the feature set packages, see the overview chapter of the *Cisco CSR 1000v Cloud Services Router Software Configuration Guide.*

Throughput

The Cisco CSR 1000v router provides both perpetual licenses and term subscription licenses that support the feature set packages for the following maximum throughput levels:

- 10 Mbps
- 50 Mbps
- 100 Mbps
- 250 Mbps

- 500 Mbps
- 1 Gbps
- 2.5 Gbps
- 5 Gbps
- 10 Gbps

Throughput levels are supported for different feature set packages in each version. For more information about how the maximum throughput levels are regulated on the router, see the *Cisco CSR 1000v Cloud Services Router Software Configuration Guide.*

Memory Upgrade

Beginning with Cisco IOS XE 3.11S, a memory upgrade license is available to add memory to the Cisco CSR 1000v. This license is available only for selected technology packages.

Additional Information about Licenses and Activation

For more information about each software license, including part numbers, see the Cisco CSR 1000v Router Datasheet. For more information about the standard Cisco IOS XE software activation procedure, see the *Software Activation Configuration Guide, Cisco IOS XE Release 3S*.

Software Image Nomenclature for OVA Installation File

The Cisco CSR 1000v .ova installation file nomenclature provides information about a given release. The following are examples of filenames for .ova installation files:

- Standard release (note “std” in the filename)

  csr1000v-universalk9.03.15.00.S.155-2.S-std.ova
- Extended maintenance support release (note “ext” in the filename)

  csr1000v-universalk9.03.16.00.S.155-3.S-ext.ova

Table 3 lists the attributes and the release properties indicated.

Table 3 OVA Installation Filename Attributes

Filename Attribute	Properties
Example: universalk9	Indicates the installed image package.
03.16.00.S.155-3.S	Indicates that the software image is for the Cisco IOS XE 3.16.0S release image, mapped to 15.5(3) in the alternate release numbering system.
std or ext	Standard release or extended maintenance support release
C4	Indicates that the software image supports 4 CPUs on the VM.
M4G	Indicates that the software image requires 4 GB memory on the VM.

Table 3 OVA Installation Filename Attributes (continued)

Filename Attribute	Properties
N3	Indicates that the .ova image installs 3 vNICS. **Note** The Cisco CSR 1000v supports up to 10 vNICs in Cisco IOS XE 3.9S. The .ova installation process installs 3 vNICS. The remaining vNICS must be manually installed on the VM.
D8	Indicates that the software image requires an 8 GB hard disk.

Limitations and Restrictions in Cisco CSR 1000v Series Cloud Services Routers

Limitations and Restrictions in Cisco IOS XE 3.13S

- (Cisco IOS 3.13.0S) The Cisco CSR 1000v has a limit of 4096 IDBs (Interface Descriptor Blocks). This limits the total number of hardware and software IDB's at any one time to 4096.

Limitations and Restrictions in Cisco IOS XE 3.12S

This section lists limitations and restrictions on the Cisco CSR 1000v Series Cloud Services Router in Cisco IOS XE 3.12S.

- Microsoft Hyper-V has issues with tagged packets, so VLAN (dot1Q and QinQ) will not work on Microsoft Hyper-V.
- When the Cisco CSR 1000v is installed on Microsoft Hyper-V, the interface numbers can change after Microsoft Hyper-V fails over to a new server, or restarts after a live migration.
  - If the server is set to perform ungraceful failover, there is no workaround.
  - If the server is set to perform graceful failover or restart, enter the **clear platform software vnic-if nvtable** command before executing the failover or restart.

  This issue is not seen if the maximum number of interfaces is configured.
- On Citrix XenServer 6.1, the paravirtual drivers for the CSR 1000v will not work without a certain for the XenServer host. This is detrimental to performance. Use the following hot-fix to make sure that the VM loads with the proper paravirtual networking drivers:

  http://support.citrix.com/article/CTX137843

  Verify that the proper drivers are installed using the following command:
  show platform software vnic-if interface-mapping

The driver listed should be **vif** if the correct drivers are in use.

Limitations and Restrictions in Cisco IOS XE 3.10S

This section lists limitations and restrictions on the Cisco CSR 1000v Series Cloud Services Router in Cisco IOS XE 3.10S.

- Configuring Network Based Application Recognition (NBAR), or Application Visibility and Control (AVC) support on the Cisco CSR 1000v requires a minimum of 4GB DRAM on the VM, even when using the 1 vCPU configuration on the VM.
- On the Cisco CSR 1000v, all the NICs are logically named as the Gigabit Ethernet interface. The Cisco CSR 1000v does support the 10G IXGBE vNIC in passthrough mode; but that interface also is also logically named as a Gigabit Ethernet interface. Note that with emulated devices like VMXNET3/PV/VIRTIO from the hypervisor, the Cisco CSR 1000v is not aware of the underlying interfaces. The vSwitch may be connected to a 10 GB physical NIC or 1 GB physical NICs or multiple NICs (with NIC teaming on the hypervisor) as well.
- The following limitations have been observed on the Cisco CSR 1000v with the 1 vCPU configuration with 2.5 GB of RAM allocation on VMware ESXi:
  - If the memory Hot-Add option is enabled, and the Cisco CSR 1000v is powered on with 2.5GB initial memory, then the RAM allocation can only increase to a maximum of 3 GB. The system does not allow upgrading to more than 3GB of RAM allocation. The Virtual Machine Properties windows shows “Maximum Hot-Add Memory for this Power is 3 GB”.
  - If the Cisco CSR 1000v is powered on with 3GB initial RAM allocation, then the Hot-Add memory option doesn't work, and the option to select memory remains greyed out with the same message on the Properties windows, “Maximum Hot-Add Memory for this Power is 3 GB”.
  - If the Cisco CSR 1000v is powered up with 4GB initial RAM allocation, then the Hot-Add option works and you are able to add up to 64 GB of memory.

Limitations and Restrictions in Cisco IOS XE 3.9S

This section lists limitations and restrictions on the Cisco CSR 1000v Series Cloud Services Router.

- You may experience low virtual network I/O performance with an Intel 1 Gbps NIC using the igb driver. Cisco recommends that you use a 10 Gb NIC for higher throughput applications. For more information, see the VMware document at the following location and apply the settings:

  http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2018891
- The ESXi host power management policy should be set to High Performance. If this power management policy is not set, the Cisco CSR 1000v VM will crash due to the High Availability stuck thread detection not seeing the core running the data plane/ppe run for an extended period of time.

Features and Notes: Release 3.17S

For up-to-date information, see:

Cisco CSR 1000v Cloud Services Router Software Configuration Guide

Cisco CSR1000v DocWiki Home

Features

REST API: IP SLA Resource Expanded

Several new APIs have been added to the IP SLA resource of the REST API. See *Cisco IOS XE REST API Management Reference Guide* for details.

VMware Support

Added support for VMware ESXi 6.0.

Note Cisco IOS XE 3.16.1S and later also support VMware ESXi 6.0.

Red Hat Enterprise Linux Support

Added support for Red Hat Enterprise Linux 7.1.

Notes

Launching Cisco CSR1000v in Red Hat Enterprise Linux: Host Mode

Due to an issue specific to Red Hat Enterprise Linux, when launching the Cisco CSR1000v in a Red Hat Enterprise Linux environment using **virt-install**, set the host mode as follows:

- In Red Hat Enterprise Linux 6, use:

  ```
  --cpu host
  ```

- In Red Hat Enterprise Linux 7, use:

  ```
  --cpu host-model
  ```

For additional information about deployment in a KVM environment, see Installing the Cisco CSR 1000v in KVM Environments in in *Cisco CSR 1000v Cloud Services Router Software Configuration Guide*.

Default Console

When installing the Cisco CSR1000v software image, the default setting is to use is the **Virtual VGA console**. In some previous releases, the default setting was Automatic Console Detection. See Accessing the Cisco CSR 1000v Console in *Cisco CSR 1000v Cloud Services Router Software Configuration Guide.*

Features and Notes: Release 3.16S

For up-to-date information, see:

Cisco CSR 1000v Cloud Services Router Software Configuration Guide

Cisco CSR1000v DocWiki Home

Features

Support for CLNS

Beginning with Cisco IOS XE Releases 3.16S, the Cisco CSR 1000v supports Connectionless Network Service (CLNS). Requires the IPBase license package. For information, see the *Cisco CSR 1000v Cloud Services Router Software Configuration Guide*.

Supported I/O Modes

Beginning with Cisco IOS XE Releases 3.16S, the CSR supports several modes of communication between vNICs and the physical hardware:

- Para Virtual
- PCI Passthrough
- Single Root I/O Virtualization (SR-IOV)
- Cisco Virtual Machine Fabric Extender (VM-FEX)

For information, see the *Cisco CSR 1000v Cloud Services Router Software Configuration Guide*.

Features and Notes: Release 3.15S

For up-to-date feature information, see the *Cisco CSR 1000v Cloud Services Router Software Configuration Guide*.

New Features

Cisco Smart Licensing

Beginning with Cisco IOS XE Release 3.15S, the Cisco CSR 1000v supports activation using Cisco Smart Licensing. To use Cisco Smart Licensing, you must first configure the Call Home feature and obtain Cisco Smart Call Home Services. For more information, see the *Cisco CSR 1000v Cloud Services Router Software Configuration Guide*.

Notes

Access to REST API and PNSC via TLS

Beginning with Cisco IOS XE Releases 3.13.2, 3.14.1, and 3.15, REST API and Cisco Prime Network Services Controller (PNSC) support is limited to TLS.

Features and Notes: Release 3.14S

Notes: Cisco IOS XE 3.14.1S

Access to REST API and PNSC via TLS

Beginning with Cisco IOS XE Releases 3.13.2, 3.14.1, and 3.15, REST API and Cisco Prime Network Services Controller (PNSC) support is limited to TLS.

New Platform Features in Cisco IOS XE 3.14.0S

This section describes the new features supported on the Cisco CSR 1000v Series Cloud Services Router in Cisco IOS XE 3.14.0S that are specific to this platform. For more information, see the *Cisco CSR 1000v Cloud Services Router Software Configuration Guide*.

NAT, FW Box to Box Redundancy for Cisco CSR1000v Routers

For information, see:

- *IP Addressing: NAT Configuration Guide, Cisco IOS XE Release 3S*
- *Security Configuration Guide: Zone-Based Policy Firewall, Cisco IOS XE Release 3S*

Radio-aware Routing

Currently released under Controlled Availability terms.

New or Modified REST API Support

Beginning with Cisco IOS XE 3.14.0S, the Cisco IOS XE REST API supports:

- IPv6 addressing on an interface

Features and Notes: Release 3.13S

Notes: Cisco IOS XE 3.13.2S

Access to REST API and PNSC via TLS

- Beginning with Cisco IOS XE Releases 3.13.2, 3.14.1, and 3.15, REST API and Cisco Prime Network Services Controller (PNSC) support is limited to TLS.

New Platform Features in Cisco IOS XE 3.13.0S

This section describes the new features supported on the Cisco CSR 1000v Series Cloud Services Router in Cisco IOS XE 3.13.0S that are specific to this platform. For more information about these features, see the *Cisco CSR 1000v Cloud Services Router Software Configuration Guide*.

APPX License Package

Beginning with Cisco IOS XE 3.13.0S, the APPX license package provides support for the feature set supported in the Standard or IPBase license package, plus the feature set available in the AX package, but does not include support for security features (IPSec VPN, DMVPN, GETVPN, EZVPN, FlexVPN, SSLVPN).

Broadband Network Gateway Support

Beginning with Cisco IOS XE 3.13.0S, the Cisco CSR 1000v supports the Broadband Network Gateway feature set. This feature requires the L-CSR-BB-1K= feature add-on license. For more information, see the *Broadband Access Aggregation and DSL Configuration Guide, Cisco IOS XE Release 3S.*

Ethernet-based deployments only (PPPoE and IPoE) are supported. Note that the following features are not supported in this release:

- ATM-related features such as PPPoA, PPPoEoA
- PMIPv6
- GTP versions 1 and 2
- EoGRE

Intelligent Services Gateway Support

Beginning with Cisco IOS XE 3.13.0S, the Cisco CSR 1000v supports the Intelligent Services Gateway feature set. This feature requires the L-CSR-BB-1K= feature add-on license. Initial support will be for Wireless deployments in Hospitality environments. For more information, see the *Intelligent Services Gateway Configuration Guide, Cisco IOS XE Release 3S*.

Common OVF Tool (COT) Support

Beginning with Cisco IOS XE 3.13.0S, the Common OVF Tool (COT) is bundled with the Cisco CSR 1000v. The Common OVF Tool is an open-source tool for editing Open Virtualization Format (.ovf, .ova) virtual appliances such as the Cisco CSR 1000v. For more information, see the tool documentation at: https://github.com/glennmatthews/cot.

PfR Master Controller support for Cisco CSR 1000v

Beginning with Cisco IOS XE 3.13.0S, the Cisco CSR 1000v can perform as a Performance Router Master Controller. For more information, see the *Performance Routing Configuration Guide, Cisco IOS XE Release 3S*

Platform Hardware Throughput Monitor

Beginning with Cisco IOS XE 3.13.0S, the platform hardware throughput monitor can be used to monitor the platforms current throughput and receive a notification when the maximum allowable throughput level is close to being reached. The **set platform hardware throughput-monitor** command configures the percentage of throughput at which you are notified, and the interval for how often the router checks the throughput rate.

Shared Management Interface for REST API Support

Beginning with Cisco IOS XE 3.13.0S, the management virtual services container used for REST API support can share the same IP address as the router's management interface. In previous releases, a separate IP address had to allocated specifically for the virtual services container. In this release, this feature is supported for the virtual services container when used for REST API, but is not supported when the virtual services container is used for Cisco Prime Network Services Controller (PNSC) support.

Support for Single Root I/O Virtualization (SR-IOV) on VMware ESXi and Microsoft Hyper-V

Beginning with Cisco IOS XE 3.13.0S, the Cisco CSR 1000v supports Single Root I/O virtualization (SR-IOV) on VMware ESXi and Microsoft Hyper-V. No additional configuration is required on the Cisco CSR 1000v, but the host hardware must support the Intel VT-d or AMD IOMMU specification.

New or Modified REST API Support

Beginning with Cisco IOS XE 3.13.0S, the Cisco CSR 1000v supports new or modified REST APIs in the following functional areas:

- Save Configuration
- L2 Interfaces
- Bridge Domain
- VxLAN
- Multicast
- VRF
- VRF-Aware DNS
- OSPF
- BGP
- EIGRP
- VRF Routing Table
- NAT
- VPN site-to-site interface state
- LISP
- QoS
- HSRP

For more information, see the *Cisco IOS XE REST API Management Reference Guide*.

New Cisco IOS XE Software Features in Cisco IOS XE 3.13.0S

This section describes new features in Cisco IOS XE 3.13.0S that are supported on the Cisco CSR 1000v Series Cloud Services Router and on other platforms.

- PPPoE Client

  For detailed information, see the following documentation:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/bbdsl/configuration/xe-3s/bba-xe-3s-book/bba-pppoe-client-xe.html

- Appnav and EZconfig Enhancements

  For detailed information, see the following Cisco site:

  http://www.cisco.com/c/en/us/td/docs/routers/access/4400/appnav/csr-asr/apnavcsr.html

- Flexible NetFlow Export of TrustSec fields

  For detailed information, see the following Cisco site:

  https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cts/configuration/15-mt/sec-usr-cts-15-mt-book/cts-fnf.html

- Group Encrypted Transport VPN Key Server on CSR

  For detailed information, see the following Cisco site:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_getvpn/configuration/xe-3s/sec-get-vpn-xe-3s-book/sec-get-vpn.html

- LISP Multicast

  For detailed information, see the following Cisco site:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_lisp/configuration/xe-3s/irl-xe-3s-book/irl-lisp-multicast.html

- NBAR2 Integrated Protocol Pack 9.0.0

  For detailed information, see the following Cisco site:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/pp900/nbar-prot-pack600.html

Features and Notes: Release 3.12S

New Platform Features in Cisco IOS XE 3.12.1S

This section describes the new features supported on the Cisco CSR 1000v Series Cloud Services Router in Cisco IOS XE 3.12.1S. For more information about these features, see the *Cisco CSR 1000v Cloud Services Router Software Configuration Guide*.

New Technology Package Licenses

Beginning with Cisco IOS XE 3.12.1S, the following technology package licenses are supported:

- IPBase
- Security
- AX

For more information, see the "Cisco CSR 1000v Software Licenses" section on page 5.

Support for SSL VPN

Beginning with Cisco IOS XE 3.12.1S, the Cisco CSR 1000v supports SSL VPN. For more information, see the *SSL VPN Configuration Guide, Cisco IOS XE Release 3S.*

The Cisco IOS XE SSL VPN Support feature is only supported on the Cisco CSR 1000v in this release.

Support for Single Root I/O Virtualization (SR-IOV)

Beginning with Cisco IOS XE 3.12.1S, the Cisco CSR 1000v supports Single Root I/O virtualization (SR-IOV) to provide improved throughput for selected hypervisors. In this release, SR-IOV is supported for Citrix XenServer and KVM only. No additional configuration is required on the Cisco CSR 1000v, but the host hardware must support the Intel VT-d or AMD IOMMU specification.

New Platform Features in Cisco IOS XE 3.12.0S

This section describes the new features supported on the Cisco CSR 1000v Series Cloud Services Router in Cisco IOS XE 3.12S that are specific to this platform. For more information about these features, see the *Cisco CSR 1000v Cloud Services Router Software Configuration Guide*.

New Higher Throughput-Based Licenses

Beginning with Cisco IOS XE 3.12S, Cisco CSR 1000v licenses based on higher maximum supported throughput levels are available. You can purchase licenses to support maximum throughput levels of 2.5 Gbps and 5 Gbps. For more information, see the "Cisco CSR 1000v Software Licenses" section on page 5 and the *Cisco CSR 1000v Cloud Services Router Software Configuration Guide*.

Support for Microsoft Hyper-V Hypervisor

Beginning with Cisco IOS XE 3.12S, the Cisco CSR 1000v supports installation on the Microsoft Hyper-V hypervisor. The supported hypervisor version is Windows Server 2012 R2.

Support for VMware ESXi 5.5

Beginning with Cisco IOS XE 3.12S, the Cisco CSR 1000v supports installation on VMware ESXi 5.5.

Note VMware ESXi 5.5 update 3 is not supported at this time.

Support for KVM Using OpenStack

Beginning with Cisco IOS XE 3.12S, the Cisco CSR 1000v supports installation of a KVM instance on OpenStack.

Cisco CSR 1000v 8vCPU Configuration

Beginning with Cisco IOS XE 3.12S, the Cisco CSR 1000v offers a configuration option that uses 8 virtual CPUs (vCPUs) for VMware ESXi only.

Router Management Using Cisco Configuration Professional

Beginning with Cisco IOS XE Release 3.12S, the Cisco CSR 1000v supports managing the router using Cisco Configuration Professional. The minimum version required is Cisco Configuration Professional 2.8. For more information, see the Cisco Configuration Professional documentation.

New and Modified REST API Support

Beginning with Cisco IOS XE 3.12S, the Cisco CSR 1000v REST API supports the following APIs:

- VRF aware DHCP
  - DHCP excluded address
  - DHCP pool
  - DHCP bindings

- VRF aware Site-to-Site VPN
  - Tunnel
  - Keyring
  - Statistics
  - IKE Profile
- Site-to-Site VPN Tunnel Extension to support MTU
  - Tunnel
- Call Home
- Reload

For more information, see the *Cisco IOS XE REST API Management Reference Guide*.

New Cisco IOS XE Software Features in Cisco IOS XE 3.12.0S

This section describes new features in Cisco IOS XE 3.12S that are supported on the Cisco CSR 1000v Series Cloud Services Router and on other platforms.

- Object Groups for ACLs

  For detailed information, see the following Cisco document:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_zbf/configuration/xe-3s/sec-data-zbf-xe-book/sec-zbf-ogacl.html
- onePK Support

  For detailed information, see the following Cisco site:

  https://developer.cisco.com/web/onepk/home
- Packet Classification using Frame-Relay DLCI Number

  For detailed information, see the following Cisco document:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_classn/configuration/xe-3s/qos-classn-xe-3s-book/qos-classn-ntwk-trfc.html
- Support of AES-GCM as an IKEv2 cipher on IOS

  For detailed information, see the following Cisco document:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/xe-3s/sec-flex-vpn-xe-3s-book/sec-cfg-ikev2-flex.html
- TrustSec Interface & Subnet to SGT mapping

  For detailed information, see the following Cisco document:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cts/configuration/xe-3s/sec-usr-cts-xe-3s-book.html

Features and Notes: Release 3.11S

New Platform Features in Cisco IOS XE 3.11S

This section describes the new features supported on the Cisco CSR 1000v Series Cloud Services Router in Cisco IOS XE 3.11S that are specific to this platform. For more information about these features, see the *Cisco CSR 1000v Cloud Services Router Software Configuration Guide*.

Cisco CSR 1000v 2vCPU Configuration

Beginning with Cisco IOS XE 3.11S, the Cisco CSR 1000v offers a configuration option that uses 2 virtual CPUs (vCPUs).

Memory Upgrade License

Beginning with Cisco IOS XE 3.11S, the Cisco CSR 1000v provides a memory upgrade license to add up to 8 GB memory with route reflector support for the 500 Mbps maximum Premium package. For more information, see the "Cisco CSR 1000v Software Licenses" section on page 5.

Deployment of the Cisco CSR 1000v on an Amazon Machine Image (AMI)

Beginning with Cisco IOS XE 3.11S, the Cisco CSR 1000v supports deployment on an Amazon Machine Image (AMI). You can deploy a Bring Your Own License (BYOL) AMI using a license purchased from Cisco. For more information, see the *Cisco CSR 1000v Series Cloud Services Router Deployment Guide for Amazon Web Services*.

VxLAN Layer 2 and Layer 3 Gateway Support on the Cisco CSR 1000v

This release provides VxLAN (Virtual eXtensible Local Area Network) Layer 2 and Layer 3 support on the Cisco CSR 1000v. VxLAN is a technology that provides a Layer-2 overlay network, allowing for network isolation. The standard 802.1q VLAN implementation limits the number of tags to 4,096. However, cloud service providers may want to operate more than 4,096 virtual networks. VxLAN uses a 24-bit network ID, which allows for a much larger number of individual identified networks to be operated.

For more information, see the *Cisco CSR 1000v VxLAN Support* document.

New and Modified REST API Support

Beginning with Cisco IOS XE 3.11S, the Cisco IOS XE REST API (formerly called the Cisco CSR 1000v REST API) supports the following technologies:

- VRF
- EzVPN

The following REST APIs have been modified in this release:

- Global parameters
- ACL

For more information, see the *Cisco IOS XE REST API Management Reference Guide*.

Support for Remote Management by Cisco Prime Network Services Controller

Beginning with Cisco IOS XE 3.11S, the Cisco CSR 1000v supports remote management of the router using Cisco Prime Network Services Controller. For more information, see the *Cisco CSR 1000v Cloud Services Router Software Configuration Guide*. and the *Cisco Prime Network Services Controller* documentation.

New Cisco IOS XE Software Features in Cisco IOS XE 3.11S

This section describes new features in Cisco IOS XE 3.11S that are supported on the Cisco CSR 1000v Series Cloud Services Router and on other platforms.

New Cisco IOS XE Software Feature in Cisco IOS XE 3.11.1S

The following feature has been updated in the Cisco IOS XE 3.11.1 release.

- Dropping TCP Packets During Router Reboot Process in AppNav Controller Group Scenario

  For AppNav Controller Group (ACG) scenarios, a new CLI (**service-insertion acg-reload-delay**) provides a time delay before enabling WAN traffic for a router that has just rebooted. During the delay, the router drops all TCP packets passing through the WAN interface. This enables the router to synchronize flows before traffic is enabled, preventing unintended resetting of connections.

  For detailed information, see the following Cisco document:

  http://www.cisco.com/c/en/us/td/docs/routers/access/4400/appnav/csr-asr/apnavcsr.html

New Cisco IOS XE Software Features in Cisco IOS XE 3.11.0S

- Cisco Application Visibility and Control (AVC) Support in Cisco IOS XE 3.11S:

  For detailed information, see the following Cisco document:

  http://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/avc/ios_15-4_1T_ios_xe3_11/avc_user_guide_ios_15-4_1T_iosxe3_11.html

- Disjoint LISP RLOC Domains Support

  For detailed information, see the following Cisco document:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_lisp/configuration/xe-3s/irl-xe-3s-book/irl-lisp-support-for-disjoint-rloc-domains.html

- Enabling ALGs and AICs in Zone-Based Policy Firewalls

  For detailed information, see the following Cisco document:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_zbf/configuration/xe-3s/sec-data-zbf-xe-book/zbf-enable-alg-aic.html

- FNF: Prevent Export Storms

  For detailed information, see the following Cisco document:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fnetflow/configuration/xe-3s/fnf-xe-3s-book/fnf-xe-3s-book_chapter_010000.html

- IOS IKEv2 support for AutoReconnect feature of AnyConnect

  For detailed information, see the following Cisco document:

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

- IP Tunnel - GRE Key Entropy Support

  For detailed information, see the following Cisco document:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/configuration/xe-3s/ir-xe-3s-book/ir-tunls-gre-entropy-xe.html

- IPV4 ACL Chaining Support

  For detailed information, see the following Cisco document:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_acl/configuration/xe-3s/sec-data-acl-xe-3s-book/sec-ip4-acl-chng-sup.html

- ISIS - Remote LFA FRR

  For detailed information, see the following Cisco document:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_isis/configuration/15-s/irs-15-s-book/irs-rmte-lfa-frr.html

- LISP ESM Multihop Mobility

  For detailed information, see the following Cisco document:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_lisp/configuration/xe-3s/irl-xe-3s-book/irl-lisp-esm-multihop-mobility.html

- MPLS VPN over mGRE

  For detailed information, see the following Cisco document:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/configuration/xe-3s/ir-xe-3s-book/ir-mpls-vpnomgre-xe.html

- NBAR2 Integrated Protocol Pack 6.0.0

  For detailed information, see the following Cisco document:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/pp600/nbar-prot-pack600.html

- OSPF LFA IPFRR Phase 3

  For detailed information, see the following Cisco document:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/xe-3s/iro-xe-3s-book/iro-ipfrr-lfa.html

- Per Tunnel QoS for DMVPN

  For detailed information, see the following Cisco document:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/xe-3s/sec-conn-dmvpn-xe-3s-book/sec-conn-dmvpn-per-tunnel-qos.html

- TCP MSS Adjustment

  For detailed information, see the following Cisco document:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp/configuration/xe-3s/iap-xe-3s-book/iap-tcp.html

Features and Notes: Release 3.10S

New Platform Features in Cisco IOS XE 3.10S

This section describes the new features supported on the Cisco CSR 1000v Series Cloud Services Router in Cisco IOS XE 3.10S that are specific to this platform. For more information about these features, see the *Cisco CSR 1000v Cloud Services Router Software Configuration Guide*.

New Higher Throughput-Based Licenses

Beginning with Cisco IOS XE 3.10S, Cisco CSR 1000v licenses based on higher maximum supported throughput levels are available. You can purchase licenses to support a maximum throughput level of 100 Mbps, 250 Mbps, 500 Mbps, or 1 Gbps. The maximum throughput licenses for 10 Mbps and 50 Mbps introduced in Cisco IOS XE 3.9S are still supported; the throughput licenses for 25 Mbps are no longer supported. For more information, see the "Cisco CSR 1000v Software Licenses" section on page 5 and the *Cisco CSR 1000v Cloud Services Router Software Configuration Guide*.

Cisco CSR1000v Low Footprint (1vCPU, 2.5Gb memory)

Beginning with Cisco IOS XE 3.10S, the Cisco CSR 1000v offers a low footprint configuration option that requires only 1 virtual CPU (vCPU) and 2.5 Gb memory. This option is only supported on VMware ESXi.

Support for Citrix XenServer Hypervisor

Beginning with Cisco IOS XE 3.10S, the Cisco CSR 1000v supports installation on the Citrix XenServer hypervisor, version 6.02.

Support for Kernel Virtual Module (KVM)-Based Hypervisors

Beginning with Cisco IOS XE 3.10S, the Cisco CSR 1000v supports installation on the following KVM-based hypervisors:

- KVM hypervisors based on Red Hat Enterprise Linux 6.3 and QEMU 0.12
- Red Hat Enterprise Virtualization 3.1

Additional VMware ESXi 5.0 Features Supported in Cisco IOS XE 3.10S

Beginning with Cisco IOS XE 3.10S, the following VMware ESXi 5.0 features are supported on the Cisco CSR 1000v Cloud Services Router:

- Distributed Resources Scheduler
- Fault Tolerance

Support for VMware ESXi 5.1

Beginning with Cisco IOS XE 3.10S, the Cisco CSR 1000v supports VMware ESXi 5.1.

REST API Support for the Cisco CSR 1000v

Beginning with Cisco IOS XE 3.10S, the Cisco CSR 1000v provides support for RESTful APIs as an alternative to configuring the router using the Cisco IOS XE CLI. The REST API support is limited to the following technologies:

- Token-services
- Global
- Host-name, Domain-name, local-users, running-config, DNS servers, NTP
- Interface
- DHCP
- Routing (OSPF, BGP, EIGRP)
- ACL (IOS extended ACL)
- NAT
- ZBFW (Zone Based Firewall)
- IPSEC site-to-site VPN
- Licensing
- Monitoring
- Memory, CPU & Syslog

Note that IPV6 is not currently supported for the REST API. The Cisco CSR 1000v only supports the REST APIs over an HTTPS connection.

For more information, see the *Cisco IOS XE REST API Management Reference Guide*.

Additional Cisco IOS XE Technologies Supported in Cisco IOS XE 3.10S

The following Cisco IOS XE technologies are supported on the Cisco CSR 1000v Series Cloud Services Router beginning in Cisco IOS XE 3.10S:

- Overlay Transport Virtualization (OTV)
- Virtual Private LAN Service (VPLS)

New Cisco IOS XE Software Features in Cisco IOS XE 3.10S

This section describes new features in Cisco IOS XE 3.10S that are supported on the Cisco CSR 1000v Series Cloud Services Router and on other platforms.

- New Cisco IOS XE Software Feature in Cisco IOS XE 3.10.2S
- New Cisco IOS XE Software Features in Cisco IOS XE 3.10.0S

New Cisco IOS XE Software Feature in Cisco IOS XE 3.10.2S

The following feature has been updated in the Cisco IOS XE 3.10.2 release.

- Dropping TCP Packets During Router Reboot Process in AppNav Controller Group Scenario

  For AppNav Controller Group (ACG) scenarios, a new CLI (**service-insertion acg-reload-delay**) provides a time delay before enabling WAN traffic for a router that has just rebooted. During the delay, the router drops all TCP packets passing through the WAN interface. This enables the router to synchronize flows before traffic is enabled, preventing unintended resetting of connections.

  For detailed information, see the following Cisco document:

  http://www.cisco.com/c/en/us/td/docs/routers/access/4400/appnav/csr-asr/apnavcsr.html

New Cisco IOS XE Software Features in Cisco IOS XE 3.10.0S

- Cisco Application Visibility and Control (AVC) Support in Cisco IOS XE 3.10S:

  For detailed information, see the following Cisco document:

  http://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/avc/ios_xe3_10/avc_user_guide_iosxe3_10.html

- TrustSec SGT Handling: L2 SGT imposition and forwarding

  For detailed information, see the following Cisco document:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cts/configuration/xe-3s/sec-usr-cts-xe-3s-book/cts-sgt-handling-imp-fwd.html

- IOS-XE GTP TEID based ECMP

  For detailed information, see the following Cisco document:

  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipswitch_cef/configuration/xe-3s/asr1000/isw-cef-xe-3s-asr1000-book/isw-cef-load-balancing.html

Features and Notes: Release 3.9S

The following sections list the new features that are supported by the Cisco CSR 1000v Cloud Services Routers for Cisco IOS XE 3.9S.

New Platform Features in Cisco IOS XE 3.9S

This section describes the new features supported on the Cisco CSR 1000v Series Cloud Services Router in Cisco IOS XE 3.9S that are specific to this platform. For more information about these features, see the *Cisco CSR 1000v Cloud Services Router Software Configuration Guide*.

Throughput-Based Licenses

Beginning with Cisco IOS XE 3.9S, Cisco CSR 1000v licenses are based on the maximum supported throughput level. You can purchase licenses to support a maximum throughput level of 10 Mbps, 25 Mbps, or 50 Mbps. For more information, see Cisco CSR 1000v Software Licenses and the *Cisco CSR 1000v Cloud Services Router Software Configuration Guide*.

Additional Cisco IOS XE Technologies Supported in Cisco IOS XE 3.9S

The following Cisco IOS XE technologies are supported on the Cisco CSR 1000v Series Cloud Services Router beginning in Cisco IOS XE 3.9S:

- IP Multicast
- EoMPLS
- QoS
- Application Visibility Control (AVC)
- Network Based Application Recognition (NBAR)

Additional VMware ESXi 5.0 Features Supported in Cisco IOS XE 3.9S

The following VMware ESXi 5.0 features are supported on the Cisco CSR 1000v Cloud Services Router beginning in Cisco IOS XE 3.9S:

- Host-Level High Availability
- VM-Level High Availability
- vMotion
- Distributed vSwitch
- NIC Teaming
- NIC Load Balancing
- Mount or Pass Through of USB Storage

New and Changed CLI Commands

The following CLI commands specific to the Cisco CSR 1000v have been added in Cisco IOS XE 3.9S:

- **platform hardware throughput level**
- **show platform hardware throughput level**

The following CLI command specific to the Cisco CSR 1000v has been deprecated in Cisco IOS XE 3.9S:

- **license feature csr**

New Cisco IOS XE Software Features in Cisco IOS XE 3.9S

This section describes new features in Cisco IOS XE 3.9S that are supported on the Cisco CSR 1000v Series Cloud Services Router and on other platforms.

LISP Host Mobility Extended Subnet

For detailed information, see the following Cisco document:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_lisp/configuration/xe-3s/irl-xe-3s-book/irl-host-mob.html

LISP SHA-2 Support for Site Registration

For detailed information, see the following Cisco document:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_lisp/configuration/xe-3s/irl-xe-3s-book/irl-overview.html

Compute and export QoS metrics to FNF records

For detailed information, see the following Cisco document:

http://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/avc/ios_xe3_9/avc_soln_guide_iosxe3_9/avc_config.html

Enable NBAR URI extraction for HTTP transactions for persistent connections

For detailed information, see the following Cisco document:

http://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/avc/ios_xe3_9/avc_soln_guide_iosxe3_9/avc_config.html

Flexible NetFlow: MPLS Support

For detailed information, see the following Cisco document:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fnetflow/configuration/xe-3s/fnf-xe-3s-book/fnf-mpls-support.html

NAT - Paired Address Pooling Support

For detailed information, see the following Cisco document:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/xe-3s/iadnat-addr-pool.html

Export PfR MC-id and class-id to FNF record

For detailed information, see the following Cisco documents:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/avc/configuration/xe-3s/avc-xe-3s-book.html

http://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/avc/ios_xe3_9/avc_soln_guide_iosxe3_9/avc_config.html

Caveats

This section provides information about the caveats in Cisco CSR 1000v Series Cloud Services Routers Release 3S. Caveats describe unexpected behavior. Severity 1 caveats are the most serious caveats. Severity 2 caveats are less serious. Severity 3 caveats are moderate caveats. This section includes severity 1, severity 2, and selected severity 3 caveats.

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

http://www.cisco.com/c/en/US/support/tsd_products_field_notice_summary.html

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

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

Note If you have an account on Cisco.com, you can also use the Bug Search Tool (BST) to find select caveats of any severity. To reach the Bug Search Tool, log in to Cisco.com and go to https://tools.cisco.com/bugsearch/search. (If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)

For Best Bug Search Tool Results

For best results when using the Bug Search Tool:

- In the **Product** field, enter Cloud Services Router.
- In the **Releases** field, enter one or more Cisco IOS XE releases of interest. The search results include caveats related to any of the releases entered in this field.

The tool provides autofill while you type in these fields to assist in entering valid values.

Releases beginning with **3.x** have an equivalent release number beginning with **15.x**, as shown in the following table. Include the **15.x** equivalent to ensure that all relevant caveat results are displayed.

Table 4 Release Number Equivalents for Recent Releases

For...	...search using the following equivalent release numbers
3.14	3.14 and 15.5(1)
3.15	3.15 and 15.5(2)
3.16	3.16 and 15.5(3)

See the following sections.

- Caveats—Cisco IOS XE Release 3.17S
- Caveats—Cisco IOS XE Releases 3.14S to 3.16S
- Caveats—Cisco IOS XE Release 3.13S
- Caveats—Cisco IOS XE Release 3.12S

Caveats—Cisco IOS XE Release 3.17S

You can use the Bug Search Tool to view new and updated caveats: https://tools.cisco.com/bugsearch/search.

For Best Bug Search Tool Results

For best results when using the Bug Search Tool:

- In the **Product** field, enter Cloud Services Router.
- In the **Releases** field, enter one or more Cisco IOS XE releases of interest. The search results include caveats related to any of the releases entered in this field.

The tool provides autofill while you type in these fields to assist in entering valid values.

Releases beginning with **3.x** have an equivalent release number beginning with **15.x**, as shown in the following table. Include the **15.x** equivalent to ensure that all relevant caveat results are displayed.

Table 5 Release Number Equivalents for Recent Releases

For...	...search using the following equivalent release numbers
3.14	3.14 and 15.5(1)
3.15	3.15 and 15.5(2)
3.16	3.16 and 15.5(3)
3.17	3.17 and 15.6(1)

Resolved Caveats—Cisco IOS XE Release 3.17.4S

Table 6 Resolved Caveats—Cisco IOS XE 3.17.4S

Caveat	Description
CSCvd47757	Cisco CSR 1000v is not able to poll CISCO-IPSEC-FLOW-MONITOR-MIB

Resolved Caveats—Cisco IOS XE Release 3.17S

Table 7 Resolved Caveats—Cisco IOS XE 3.17S

Caveat	Description
CSCuw20432	CSR interfaces shows up DHCP/TFTP for Static IP configuration
CSCuv86049	ISR4331 and ISR4351 platforms crash during GRE performance testing
CSCuu98660	4331: MMA record timestamp mismatch btw PI/PD, TC missing after 48 hours
CSCuw71685	CSR1000v fails to pass traffic after upgrading ESXi to 5.5.0 patch 3a
CSCuv66659	CSR1000v: csr1kv stops Responding to ARP Requests
CSCuw27689	RESTAPI: VxLAN extension POST would be failed with response=500
CSCuv10190	CSR1k serial console is not working properly
CSCuw35757	CSR1000v incorrect API call to AWS

Open Caveats—Cisco IOS XE Release 3.17S

Table 8 Open Caveats—Cisco IOS XE 3.17S

Caveat	Description
CSCut95123	CSR1kv: Silent packet drop seen in aging test with low traffic rate
CSCuu24835	ULTRA 15.5 - SR-IOV (vfio) 9k packet forwarding broken
CSCuu81197	CSR Interfaces not coming up with certain VIC's on KVM using ENIC
CSCuw34077	ASR1k: FP crash due to poor handling of mem allocation failure in IFDB
CSCuw42095	CSR crashes before booting with 32 vCPU cores on ESXi
CSCun65825	ULTRA XE313: Packets Drop at BqsOor with traceback
CSCus85617	CSR configuration lost after power off/on
CSCut70456	CSR1k - qfp datapath utilization is wrong when ESXi drop prior to CSR Rx
CSCuu35014	CSR1000v Interface Responds to two different MAC Addr on KVM Enic VM-FEX
CSCuv42615	CSR1000v Interfaces occasionally enumerate incorrectly after reload
CSCuw17158	performance degradation on IPSec, NAT, FW, HQos with RHEL 7.1
CSCuw76571	CSR crashes when we scale MPLS LDP routes
CSCuw99060	Multiple Cisco Smart Licenses used after switching from CSL to SL

Caveats—Cisco IOS XE Releases 3.14S to 3.16S

- Open Caveats—Cisco IOS XE Release 3.16.7S
- Resolved Caveats—Cisco IOS XE Release 3.16.5S
- Open Caveats—Cisco IOS XE Release 3.16.5S
- Resolved Caveats—Cisco IOS XE Release 3.16.4aS
- Open Caveats—Cisco IOS XE Release 3.16.4aS
- Resolved Caveats—Cisco IOS XE Release 3.16.3S
- Open Caveats—Cisco IOS XE Release 3.16.3S
- Caveats—Cisco IOS XE Release 3.14 to 3.16.2S

Note To view details of the caveats for releases from 3.14 up to 3.16.2, use the Bug Search Tool as explained below in "Caveats—Cisco IOS XE Release 3.14 to 3.16.2S" section on page 35.

Resolved Caveats—Cisco IOS XE Release 3.16.9S

All resolved bugs for this release are available in the Cisco Bug Search Tool through the Resolved bug search. This search uses the following search criteria and filters:

Caveat ID Number	Description
CSCvm21219	Crash on Running "show vpdn tunnel summary" command.
CSCvm02572	Router crashes on SSH connection with "login on-failure log" enabled.
CSCvk65072	Crash due ZBF + NAT
CSCve89361	Crash in SISF while processing IPv6 packet
CSCvn78961	Subscribers cannot re-login due to CoA time-out (lite-sessions in routed mode)
CSCuw79412	%SYS-6-STACKLOW: Stack for process PPP SIP running low, 0/6000
CSCvm98100	External Interface on the PfR MC stuck in the shutdown state
CSCvm65397	Active RP crash at __be_datagram_done
CSCvi86082	ASR1001-x crash due to wrong packet size
CSCvk54416	Change the order of BYE and NOTIFY with 200 OK sipfrag body for successful REFER passthrough scenario

Resolved Caveats— Cisco IOS XE Release 3.16.9S

All resolved bugs for this release are available in the Cisco Bug Search Tool through the Resolved bug search. This search uses the following search criteria and filters:

Caveat ID Number	Description
CSCvm02572	Router crashes on SSH connection with "login on-failure log" enabled.
CSCve89361	Crash in SISF while processing IPv6 packet
CSCvn78961	Subscribers cannot re-login due to CoA time-out (lite-sessions in routed mode)
CSCuw79412	%SYS-6-STACKLOW: Stack for process PPP SIP running low, 0/6000
CSCvm65397	Active RP crash at __be_datagram_done
CSCvj92548	CSR1k-FlexVPN: Spoke to Spoke: Implicit NHRP entry due to expired resolution request handling.
CSCvk54416	Change the order of BYE and NOTIFY with 200 OK sipfrag body for successful REFER passthrough scenario

Resolved Caveats—Cisco IOS XE Release 3.16.8S

Table 9

Caveat	Description
CSCvh20090	License boot level and throughtput level can not be changed in AWS with volume set to over 8GB
CSCvh61384	16.6: vfr related drops are not observed in CSR platfrom

Open Caveats—Cisco IOS XE Release 3.16.8S

Table 10

Caveat	Description
CSCut70456	CSR1k - qfp datapath utilization is wrong when ESXi drop prior to CSR Rx
CSCuu81130	CSR1000v KVM SR-IOV IPv6 Unsuccessful Ping Traffic
CSCuw96928	CSR1000V: unexpected memupgrade log when boots

Resolved Caveats—Cisco IOS XE Release 3.16.7bS

Table 11

Caveat	Description
CSCvh61384	VRF-related drops are not observed in the Cisco CSR 1000v platform
CSCvi16916	Netflow not exporting with 03.16.7S release

Resolved Caveats—Cisco IOS XE Release 3.16.7S

Table 12

Caveat	Description
CSCve71400	Cisco CSR 1000v—GE interface output—Input queue "drops" counter miscalculation

Open Caveats—Cisco IOS XE Release 3.16.7S

Table 13

Caveat	Description
CSCut70456	Cisco CSR 1000v—qfp datapath utilization is incorrect when ESXi drops prior to Cisco CSR 1000v Rx
CSCuu81130	Cisco CSR 1000v—KVM SR-IOV IPv6 Unsuccessful Ping Traffic
CSCuw96928	Cisco CSR 1000v—unexpected mem upgrade log when boots
CSCvh19173	Throughput is licensed throughput when idcert renew failed and in EVAL mode
CSCvh20090	License boot level and throughput level cannot be changed in AWS with volume set at over 8 GB

Resolved Caveats—Cisco IOS XE Release 3.16.5S

Table 14

Caveat	Description
CSCut70456	CSR1000v qfp datapath utilization is wrong when ESXi drops prior to CSR Rx
CSCuu81130	CSR1000v KVM SR-IOV IPv6 Unsuccessful Ping Traffic
CSCuw96928	CSR1000v unexpected memupgrade log when CSR 1000v boots

Open Caveats—Cisco IOS XE Release 3.16.5S

Table 15

Caveat	Description
CSCva04110	AWS Gateway Redundancy not working because of delayed dns

Resolved Caveats—Cisco IOS XE Release 3.16.4aS

Table 16

Caveat	Description
CSCva11028	AWS: CSR 1000V becomes unreachable if rebooted with larger storage size
CSCva45347	PCIe pass-thru w/ ixgbe driver causes MaxTu drops due to TCP reassembly
CSCux14943	Cisco Cloud Services Router 1000V Command Injection Vulnerability
CSCuy58025	CSR1000V Hyper-V: Interface missing after reload with static mac-address
CSCuz11498	CSR %VXE_VNIC_IF-3-MSGINITERROR messages when API add delete new intf
CSCva27661	VASI subsystems are not packaged in ipbasek9 image for CSR1K platform
CSCuz52914	Openstack: CSR goes in grub mode if Hard Reset

Open Caveats—Cisco IOS XE Release 3.16.4aS

Table 17

Caveat	Description
CSCuz50549	CSR startup config sometimes disappear after reload.
CSCuz76369	AWS: CSR crashes, loses connectivity after detaching PMAP interface
CSCvb33668	AWS CSR 1000V: HA fails to resolve .com.cn domain for China region
CSCut70456	CSR1k - qfp datapath utilization is wrong when ESXi drop prior to CSR Rx

Table 17

Caveat	Description
CSCuu81130	CSR1000v KVM SR-IOV IPv6 Unsuccessful Ping Traffic
CSCuw96928	CSR1000V: unexpected memupgrade log when boots

Resolved Caveats—Cisco IOS XE Release 3.16.3S

Table 18

Caveat	Description
CSCuy43894	In Amazon Web Services, SSH to CSR fails if there is a space in the keyname
CSCuy30460	CSR AX_100M license produces an HSECK9 failure

Open Caveats—Cisco IOS XE Release 3.16.3S

Table 19

Caveat	Description
CSCux14943	Cisco Cloud Services Router 1000V Command Injection Vulnerability
CSCuz52914	Openstack: CSR goes into grub mode if Hard Reset

Caveats—Cisco IOS XE Release 3.14 to 3.16.2S

For Cisco IOS XE releases 3.14 to 3.16.2S, use the Bug Search Tool to view new and updated caveats: https://tools.cisco.com/bugsearch/search.

Caveats—Cisco IOS XE Release 3.13S

Resolved Caveats—Cisco IOS XE Release 3.13.9S

Table 20

Caveat	Description
CSCvh61384	VRF-related drops are not observed in the Cisco CSR 1000v platform

Open Caveats—Cisco IOS XE Release 3.13.8S

Table 21

Caveat	Description
CSCvf07343	Performance issues with CSR1kv using encrypted AMIs
CSCva11162	Config wipeout after add/delete an interface for ESX setup

Resolved Caveats—Cisco IOS XE Release 3.13.0S

- CSCuf51357

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

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

  Cisco has released free software updates that address these vulnerabilities.

  There are no workarounds to mitigate this vulnerability.

  This advisory is available at the following link:

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

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

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

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

  Conditions: See published Cisco Security Advisory

  Workaround: See published Cisco Security Advisory

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

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

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

- CSCum22661

  Symptom: When a Peer sends a certificate with no CDP, the IOS PKI client will try to retrieve the CRL through SCEP [GetCRL] directed to CA, based on enrollment url value, however in case of enrollment profile [with a valid enrollment url], it complains that the enrollment url is not present.

  Conditions: IOS PKI Client configured with an Enrollment profile, which has enrollment url and authentication url to communicate with the CA using SCEP.

  Workaround:

  a) configure the enrollment URL under the trustpoint directly instead of using it through enrollment profile

  or

  b) configure the CA to embed a CDP in the client certificates [an HTTP Server or SCEP URL]. Peer will need to be reenrolled afresh.

  SCEP URL looks like:

  crypto pki server IOS-CA

  cdp-url http://10.106.72.139/cgi-bin/pkiclient.exe?operation=GetCRL

  [Note: Before typing in ? next to pkiclient.exe in the URL above, type Ctrl+V]

- CSCum23619

  Symptom: No counter to show the ATM VC IFM call out and response

  Conditions: ATM VC IFM call

  Workaround: N/A

- CSCum29065

  Symptom: Group override does not take effect for interface-config strings. Actual ordering of interface config strings on cloned V-Access does not correspond to the expected order based on AAA settings in IKEv2 profile.

  Conditions: User & group authorization configured in IKEv2 profile.

  Workaround: Move all config-string attributes to a single authorization source (user or group).

- CSCum34515

  Symptom: QFP crash

  Conditions: SIP ALG traffic with FW and NAT

  Workaround: None.

- CSCum34624

  Symptom: IOSd crash when show platform condition after remove the corresponding interface

  Conditions: With "debug platform software cond-debug verbose" enabled, and after delete the interface show platform condition will trigger this crash.

  Workaround: N/A

- CSCum40043

  Symptom: Crypto sessions get stuck in UP-IDLE state in scale scenario on a Cisco CSR platform.

  Conditions: This symptom occurs on a Cisco CSR platform in Cisco IOS XE Release 3.11.

  Workaround: Bring the sessions up in very small increments, for example, 40 sessions at a time initially and keep monitoring. When the sessions stop coming up for 40 sessions at a time, switch to a smaller number like 20.

- CSCum43752

  Symptom: IOSD crash at ipv6_intf_mtu on flexvpn client

  Conditions: Flapping flexvpn client configured with ipv6 on tunnel interface.

  Workaround: None.

- CSCun04952

  Symptom: Traffic which needs to be send between appnav-controllers will get lost.

  Received inter-appnav-controller packets will get assigned to the shutdown tunnel interface.

  As a result, no flows will be synchronized between this appnav-controller and appnav-controllers in the same appnav-controller-group. Asymmetrically routed packet will also fail due to lack of flow and unable to query flow from other appnav-controller.

  Conditions: Having a shutdown tunnel interface configured with tunnel source equals to the local appnav-controller IP and tunnel destination equals to the IP of another appnav-controller in the appnav-controller-group (i.e. another ASR router).

  To detect this problem the following counter will go up for every dropped packet:

  show platform hardware qfp active statistics drop | i Disabled

  alternatively you can use a packet-trace feature on 3.10.2 and above to check for the dropped reply getting send to the shutdown tunnel interface.

  Workaround: Remove the shutdown tunnel from configuration or un-shutdown it.

  Further Problem Description: The received packet shares the same source and destination IP of an existing GRE tunnel before matching AppNav tunnel. And since the tunnel interface is disabled, the packet is dropped before reaching AppNav's handler.

- CSCun31021

  Symptom: A vulnerability in IKE module of Cisco IOS and Cisco IOS XE could allow an unauthenticated, remote attacker to affect already established Security Associations (SA). The vulnerability is due to a wrong handling of rogue IKE Main Mode packets. An attacker could exploit this vulnerability by sending a crafted Main Mode packet to an affected device. An exploit could allow the attacker to cause dropping of valid, established IKE Security Associations on an affected device.

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

  Workaround: 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 4.3/3.6:

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

CVE ID CVE-2014-2143 has been assigned to document this issue. Additional details about the vulnerability described here can be found at:
http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-2143

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

- CSCun32757

  Symptom: Debug platform condition matches traffic that is not included in the condition.

  Conditions: Use of packet tracer / conditional debugger.

  Workaround: Clear platform condition all and re enable.

- CSCun36235

  Symptom: Sometimes an error log is seen when tracing packets with 'debug platform packet-trace' or some of the data seems inconsistent.

  Conditions: Tracing multicast packets with packet-trace in IOS-XE 3.11.0 or IOS-XE3.12.0 using circular buffering:

  debug platform packet-trace <num-pkts> circular

  or using drop tracing:

  debug platform packet-trace drop [code <code-num>]

  Workaround: Avoid the commands above when using.

- CSCun68542

  Symptom: CSR1000v router running XE3.11 (15.4(1)S) working as Route Reflector. The route-reflector is advertising prefixes with incorrect subnet masks to ibgp peers and route-reflector clients. The incorrect prefixes are not present in the bgp table of the route-reflector itself, however they do get installed in the bgp table of the router receiving the update.

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

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

- CSCun83348

  Symptom: IPsec configured router sees unauthenticated router in INIT stage of ospfv3

  Conditions: Configure one router with ospfv3 auth and other router with no authentication

  Workaround: None.

- CSCuo72301

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

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

  Workaround: There is no workaround.

- CSCuo75582

  Symptom: Content sensitive help from CLI lists only three protocols instead of the full list. This is valid for securityk9 license when configuring class map:

  class-map type inspect

  match protocol ?

  Conditions: Tested on 4451-X , could be also happening on ASR1K

  Workaround: Use appx license instead of securityk9

- CSCuo75681

  Symptom: RP crash due to %SYS-2-CHUNKBADMAGIC in checkheaps in chunk MallocLite

  Conditions: Not known.

  Workaround: Not known.

- CSCuo77574

  Symptom: An error is seen while enabling "auto negotiation".

  Conditions: This symptom is observed when "auto negotiation" is configured on an interface.

  Workaround: There is no workaround.

- CSCuo79718

  Symptom:

  1) "crypto isakmp aggressive-mode disable" is in "show run all" by default.

     In spite of the disable command, IKE aggressive mode is enabled by default.

  2) The command remains in "show run all" output.

     "no crypto isakmp aggressive-mode disable" command cannot remove it from "show run all", and that change ("no" form) does not show up in "show run" output.

  The command works properly if it is configured explicitly.

  Conditions: Cisco IOS 15.1 or later

  Workaround:

  - See "show run" output to check if this feature is disabled or not.

  - To disable IKE aggressive mode, set "crypto isakmp aggressive-mode disable" explicitly.

- CSCuo82943

  Symptom: SADB Peer Chunk leak seen.

  Conditions: DmVPN Hub with 2000 simulated spokes in stress/scale scenario.

  Workaround: Unknown

- CSCuo96504

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

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

  Workaround: Remove and reconfigure the IKEv2 client configuration block.

- CSCuo86953

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

  Conditions: Open one session to the device and issue show logging. Let the output of the show logging command sit at the more prompt in the Trap logging session. While changing the logging host commands in a different session resume the output of the show logging command. There is a chance that both actions at the same time will make the device crash.

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

- CSCup07089

  Symptom: FlexVPN - IKEv2 authorization policy config gets deleted after reboot under some conditions.

  Conditions: If route set interface is configured for loopback interface

  Workaround: None.

- CSCup21524

  Symptom: A crash is observed:

```
\Exception to Fastpath Thread:
Frame pointer 0x7FEA1735D570, PC = 0x7FEB1F732559

-Traceback= 1#bb8f9a461a7850b52eefb2d5dc713d87  c:7FEB1F701000+31559
c:7FEB1F701000+32A09 :400000+442C515 :400000+4430C38 iosd_unix:7FEB1FED3000+1B0B6
:400000+6D46665 :400000+7AD419 :400000+2534AFB :400000+4422F8B :400000+70D1E1F
:400000+7117396 :400000+71154E6 :400000+6D6801F :400000+6D6787F :400000+4417B48
:400000+441AE07

IOS Thread backtrace:
UNIX-EXT-SIGNAL: User defined signal 2(12), Process = SSM connection manager
-Traceback= 1#bb8f9a461a7850b52eefb2d5dc713d87  pthread:7FEB1D279000+83BF

Auxiliary Thread backtrace:
-Traceback= 1#bb8f9a461a7850b52eefb2d5dc713d87  pthread:7FEB1D279000+A7C9
```

  Conditions:This issue occurred after a switchover from Active RP to Standby RP was done. The device had 1000 PPPoA sessions on the device. Call Admission Control (CAC) is also configured.

  Workaround:Remove the CAC configurations. For example, the following would have to be removed:

  call admission new-model

  call admission limit 1000

  call admission cpu-limit 80

- CSCup22022

  Symptom: ASR using ZBFW may not properly classify traffic when class-maps of type inspect reference an ACL that uses a service-type object-group.

  Conditions: A sample configuration that does not work:

  object-group service ICMP_OG

  icmp echo

  icmp echo-reply

  icmp traceroute

```
 icmp unreachable
 icmp time-exceeded
!
ip access-list extended ICMP_ACL
 permit object-group ICMP_OG any any
!
class-map type inspect match-all ICMP_CMAP
 match protocol icmp
 match access-group name ICMP_ACL
!
policy-map type inspect ICMP_PMAP
 class type inspect ICMP_CMAP
  inspect
 class class-default
!
zone-pair security INSIDE2OUTSIDE source INSIDE destination OUTSIDE
 service-policy type inspect ICMP_PMAP
```

Workaround: Applying the ACL to the interface, then reapplying it to the class-map sometimes resolves the issue. Once the issue is resolved, reloading the ASA will cause the original classification problem to reoccur.

- CSCup22590

  Symptom: Some Cisco Internetwork Operating System (IOS) releases may be affected by the following vulnerabilities:

  These products include a version of openssl that is affected by the vulnerabilities identified by the Common Vulnerability and Exposures (CVE) IDs:

  CVE-2014-0195 - DTLS invalid fragment vulnerability

  CVE-2014-0221 - DTLS recursion flaw

  CVE-2014-0224 - SSL/TLS MITM vulnerability

  This bug has been opened to address the potential impact on this product.

  Conditions: Devices running an affected version of Cisco IOS and utilizing an affected configuration.

  One of more of these vulnerabilities affect all versions of IOS prior to the versions listed in the Integrated In field of this defect.

  Workaround :None currently available.

  More Info: Known affected releases*

  12.2(58)SE2

  15.0(2)SE6

  15.1(1)SG

15.1(2)SG
15.4(3)M
15.4(2)T
15.4(1)T
15.3(3)M
15.3(2)T
15.3(1)T
15.2(4)M
15.2(3)T
15.2(2)T
15.2(1)T
15.1(4)M
15.1(3)T
15.1(2)T
15.1(1)T
15.4(3)S
15.4(2)S
15.4(1)S
15.3(3)S
15.3(2)S
15.1(7)S
15.1(6)S
15.1(5)S
15.1(3)S
15.1(4)S
15.1(2)S
15.1(1)S
15.1(2)SY
15.1(1)SY
15.2(1)E
15.2(2)E
15.2(3)E
15.0(1)EX
15.0(2)EX
15.1(1)XO
Known unaffected releases

12.2(55)SE9 and earlier

12.2(33)SRE10 and earlier

15.0(2)SG8 and earlier

12.2(33)SXJ7 and earlier

15.0(1)SY and earlier

*if just the base version is given then all the rebuilds and maintenance releases are impacted.

CVE-2014-0224:

All Cisco IOS services that provide a form of TLS or SSL encryption are affected by this vulnerability. This includes features such as the HTTPS Web Management interface.

CVE-2014-0195:

Cisco IOS devices that support SSLVPN (AnyConnect) and have the feature configured and enabled are affected by this vulnerability.

CVE-2014-0221:

Cisco IOS devices that support SSLVPN (AnyConnect) and have the feature configured and enabled are affected by this vulnerability.

PSIRT Evaluation:

The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 10/9.5:

https://intellishield.cisco.com/security/alertmanager/cvss?target=new&version=2.0&vector=AV:N/AC:L/Au:N/C:C/I:C/A:C/E:F/RL:U/RC:C

The Cisco PSIRT has assigned this score based on information obtained from multiple sources. This includes the CVSS score assigned by the third-party vendor when available. The CVSS score assigned may not reflect the actual impact on the Cisco Product.

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

http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

- CSCup30453

  Symptom: Large multicast packets are not reaching the receiver.

  Conditions:Using IPv6 VFR with multicast.

  Workaround:None .

- CSCup66672

  Symptom: AVC coarse grain configuration, while running the debug command show platform hardware qfp active feature nbar function sui_lut_remove_all_links the router crashed.

  Conditions: Since the command is debug should not happen on customers.

  Workaround: Not to use the debug command.

Open Caveats—Cisco IOS XE Release 3.13.0S

- CSCuo17906

  Symptom: The CLI show the overlap ip in its configuration but when using the GUI to admin down/up the interface, it will resulting "failed-to-apply".

  Conditions: When apply overlapping ip address between gigabitEthernet and tunnel interface

  Workaround: None.

- CSCuo41750

  Symptom: When Gig1 is configured on CSR and it is also used as the management ip, if we try to configure sub-interface Gig1.1, it gets configured as "native" by default(even without using the keyword "native"):-

  ```
  Router(config)#int gig1.1
  Router(config-subif)#encapsulation dot1Q 1
  Router(config-subif)#
  ```

  At this point, the telnet session is lost and so is the connectivity with PNSC. When logging in using Vsphere and checking the config, it shows gig1.1 is configured as the native sub-interface. As follows:

  ```
  interface GigabitEthernet1.1
  encapsulation dot1Q 1 native
  ```

  Conditions: Configure Gig1.1 when Gig1 is configured

  Workaround: None.

- CSCup58252

  Symptom: The default queue-limit programming might not be correct if changing the throughput level without rebooting the box.

  Conditions: The change of the license shaper value will not update the already programmed default queue-limit setting. It might cause performance or QoS drops condition misbehave.

  Workaround: No workaround except perform a router reload.

- CSCup16085

  Symptom: VLAN support is not present in SR-IOV.

  Conditions: CSR 1000v installation with SR-IOV.

  Workaround: There is no workaround.

- CSCup43283

  Symptom: CSR datapath processes are using regular memcpy to copy packet buffers in different stages, which seems to have impact on throughput performance.

  Conditions: Every packet forwarding involves buffer copies.

  Workaround: No workaround.

Caveats—Cisco IOS XE Release 3.12S

Resolved Caveats—Cisco IOS XE Release 3.12.1S

- CSCue27980

  Symptom: A CPP crash triggered by NBAR may occur on Cisco ASR 1000 Series routers, Cisco 4000 Series ISR routers, and Cisco CSR 1000v routers.

  Conditions: This symptom may occur under rare conditions of traffic mixture and rate when NBAR and NAT are both enabled.

  Workaround: There is no workaround.

- CSCuj23293

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

  Conditions: This symptom is observed while parsing to header, Gateway gets errors as below: Feb 26 12:07:28 EST: Parse Error: url_parseSipUrl: Received Bad Port Feb 26 12:07:28 EST: //2765/000000000000/SIP/Error/sippmh_cmp_tags: Parse Error in request header The correct response for the above should have been to send 400 Bad Request The request cannot be fulfilled due to bad syntax The memory associated with the above is not getting released is the side effect of the above.

  Workaround: There is no workaround. Further Problem Description: This issue was not seen on versions earlier than 15.3X

- CSCuj80245

  Symptom: No address prefix flow records get reported when packets get fragmented at Tunnel interface, which has enabled with AVC flow monitor.

  Conditions: May occur when packet are fragmented due the maximum packet length limit, called the Maximum Transmission Unit (MTU). When packet size is bigger than the interface MTU, the packet will be fragmented and will not be monitored by AVC.

  Workaround: Increase the size of the MTU to accommodate larger packets. For example, configure an MTU of 3000 bytes with the following CLI: Device(config)# interface Gig0/2/1 Device(config-if)# mtu 3000 Further Problem Description: The issue may occur when UDP traffic becomes fragmented over a DMVPN tunnel interface due to a default maximum packet size (MTU) of 1500 bytes.

- CSCul01335

  Symptom: FP may crash.

  Conditions: on changing pap limit from 30 to 60 ith traffic on

  Workaround: None

- CSCul29918

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

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

Conditions: A device configured for IPSec VTI and with path-mtu-discovery disabled.

Workaround: Issue is caused by ICMP unreachables. Blocking ICMP is a workaround.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4.3/4.1:

https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:N/A:P/E:F/RL:U/RC:C CVE ID CVE-2013-6694

has been assigned to document this issue.

Additional details about the vulnerability described here can be found at:

http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2013-6694

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

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

- CSCul69990

  Symptom: when flapping mpls mldp with scale v4 setup, the lspvif interface disappears in "show ip mfib" output, and packets are dropped.

  Conditions: mldp flapping.

  Workaround:

- CSCum04325

  Symptom: Duplicate entry seen in "sh lldp neighbor"

  Conditions: if the physical link is a member of a etherchannel bundle. lldp packets are processed on the bundle UIDB. Workaround: None.

  Further Problem Description: Solution: if the physical link is a member of a etherchannel bundle. lldp packets are processed on physical link UIDB instead of the bundle UIDB.

- CSCum29065

  Symptom: Group override does not take effect for interface-config strings. Actual ordering of interface config strings on cloned V-Access does not correspond to the expected order based on AAA settings in IKEv2 profile.

  Conditions: User & group authorization configured in IKEv2 profile.

  Workaround: Move all config-string attributes to a single authorization source (user or group).

- CSCum49437

  Symptom: ucode crash@ipv4_nat_cgn_mode_dp_rel_mem on changing nat mode.

  Conditions: In a scaled setup on changing nat mode

  Workaround: none

- CSCum53269

  Symptom: "no ip subnet" in l3-custom results in creating custom protocol.

  Conditions: Create L3 custom submode ip nbar custom t1est transport tcp id 1 "no ip subnet" cretaes custom protocol and exit submode.

  Workaround: None.

- CSCum68074

  Symptom: many packets are dropped for NatIn2out cause

  Conditions: PAT, interface overload.

  Workaround: PAT pool overload

- CSCum73167

  Symptom: LDAP ALG will encode the packet even there is no need to translate them, this will not impact function, but it is not necessary.

  Conditions: LDAP ALG will encode the packet even there is no need to translate them.

  Workaround: Will not impact function .

- CSCum85493

  Symptom: ping fails with tunnel protection applied.

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

  Workaround: Can switch to using IKEv2.

- CSCum86159

  Symptom: CPP crash.

  Conditions: Conditional debugging and packet tracing is enabled on join interface for OTV.

  Workaround: No workaround.

- CSCum95078

  Symptom: Large IPSEC packets get dropped when fragmentation is done after IPSEC encapsulation.

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

  Workaround: There is no workaround.

- CSCum95638

  Symptom: Multiple Tracebacks seen pertaining to uRPF component cannot allocate more memory No functional issues seen (i.e no session drops) .

  Conditions: TBs seen on Scaled Setup of 128K Authenticated Sessions + 256K Walkby sessions.

  Workaround: Lower the session scale during RP Switchover Tested 107K Authenticated Sessions + 223K Walkby Sessions with no issues.

- CSCum96156

  Symptom: IOS will fail to match the certificate map intermittently.

  Conditions: IOS PKI using certificate maps, to authorize the Peer certificates or override CDP. In this case: - if a certificate map is written on a PC, with upper case letters in them: Ex: crypto pki certificate map HR-Users 10 subject-name co ou = HR-Users - and this is a part of the configuration that is merged with the running config through IOS file-system [directly from flash or FTP/TFTP/HTTP etc], IOS retains the upper case letters. [contrary to certificate maps written through CLI, always converts everything to lower case letters] .

Workaround: A) - copy the certificate maps [that have upper case letters in them] to a notepad - remove the certificate maps [that have upper case letters in them] - paste the certificate maps, through IOS CLI - wherever these cert maps were being called, they will stay intact, and this change will take effect immediately or B) - The certificate map needs to enter IOS in a manner that IOS would insert it if you were to enter it in a CLI I.e. Make sure the external config generators generate the certificate map in such a way that everything is in lower case, and it has white spaces between DN OID, '=' and the value.

- CSCun04952

  Symptom: Traffic which needs to be send between appnav-controllers will get lost. Received inter-appnav-controller packets will get assigned to the shutdown tunnel interface. As a result, no flows will be synchronized between this appnav-controller and appnav-controllers in the same appnav-controller-group. Asymmetrically routed packet will also fail due to lack of flow and unable to query flow from other appnav-controller.

  Conditions: Having a shutdown tunnel interface configured with tunnel source equals to the local appnav-controller IP and tunnel destination equals to the IP of another appnav-controller in the appnav-controller-group (i.e. another ASR router). To detect this problem the following counter will go up for every dropped packet: show platform hardware qfp active statistics drop | i Disabled alternatively you can use a packet-trace feature on 3.10.2 and above to check for the dropped reply getting send to the shutdown tunnel interface.

  Workaround: Remove the shutdown tunnel from configuration or un-shutdown it.

  Further Problem Description: The received packet shares the same source and destination IP of an existing GRE tunnel before matching AppNav tunnel. And since the tunnel interface is disabled, the packet is dropped before reaching AppNav's handler.

- CSCun09973

  Symptom:

  A vulnerability in the Layer 2 Tunneling Protocol (L2TP) module of Cisco IOS XE on Cisco ASR 1000 Series Routers could allow an authenticated, remote attacker to cause a reload of the processing ESP card.

  The vulnerability occurs during the processing of a malformed L2TP packet. An attacker could exploit this vulnerability by sending malformed L2TP packets over an established L2TP session. An exploit could allow the attacker to cause a reload of the affected ESP card.

  Conditions: Device configured with "no vpdn ip udp ignore checksum'.'

  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-2014-2183

  has been assigned to document this issue.

  Additional details about the vulnerability described here can be found at:

  http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-2183

  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

- CSCun09753

  Symptom: Ping failed with input errors when HDLC interface MTU set/removed.

  Conditions: 1. set MTU (more than 2950) on HDLC interface , then remove MTU; 2. ping failed to peer HDLC interface.

  Workaround: N/A

- CSCun17558

  Symptom: COS markings not seen proper on the dot1q interface.

  Conditions: The issue will be seen if met all of following conditions: 1, MPLS packets with fragment happened in data plane on the dot1q interface.

  Workaround: No Workaround.

- CSCun20274

  Symptom: Standby RP source is not participating in clocking selection.

  Conditions: we must have the below specific netclk config on the ASR1k and need to perform RP-switchover. "network-clock select 1 BITS R0 <T1/E1> <Framing>" "network-clock select 2 BITS R1 <T1/E1> <Framing>"

  Workaround: Remove and re-apply the stby-network-clk Source with different framing Further Problem Description: This bug is specific to below combination. 1. You must configure NETCLK config on ASR RP-bits [Active and Standby RP bits] 2. Router must capable of hardware redundancy If the Customer is not using Netclk feature, you can ignore this ddts

- CSCun23109

  Symptom: Error message is seen in log: %IOSXE-3-PLATFORM: F0: cpp_cp: QFP:0.0 Thread:005 TS:00000006977394452567 %IPSEC-3-REPLAY_ERROR: IPSec SA receives anti-replay error, DP Handle 12, src_addr 192.1.2.0, dest_addr 192.1.1.0, SPI 0x250cc2eb

  Conditions: Traffic with over subscription shows the TBAR drops. Eventually all the traffic dropped.

  Workaround: Increase Anti-replay window size to 20sec.

- CSCun26706

  Symptom: onep_dpss_l2_raw_inject api returns ONEP_OK which is not support in IOS-XE platform.

  Conditions: only when application want to invoke onep_dpss_l2_raw_inject to inject l2 packet.

  Workaround: n/a

- CSCun26943

  Symptom: In an INTRA-box redundancy configuration, the STANDBY FP and ACTIVE FP may not be syncing dplane HA records robustly. The easiest way for the customer to recognize if this *might* be happening is by examining the output of the show platform hardware qfp active system intra and the show platform hardware qfp standby system intra CLIs. If the output shows the counters " rx dropped" and/or "retx" continuously incrementing, then this problem may have been encountered.

  Conditions: DUAL FP systems with stateful HA features such as NAT configured.

  Workaround: NONE s

- CSCun31021

  Symptom: A vulnerability in IKE module of Cisco IOS and Cisco IOS XE could allow an unauthenticated, remote attacker to affect already established Security Associations (SA). The vulnerability is due to a wrong handling of rogue IKE Main Mode packets. An attacker could exploit this vulnerability by sending a crafted Main Mode packet to an affected device. An exploit could allow the attacker to cause dropping of valid, established IKE Security Associations on an affected device.

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

  Workaround: 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 4.3/3.6:

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

  CVE ID CVE-2014-2143 has been assigned to document this issue. Additional details about the vulnerability described here can be found at:
  http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-2143

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

- CSCun35149

  Symptom: enable performance monitor on local switching interface.

  Conditions: Two interfaces are connected as local switching

  Workaround: None

- CSCun36235

  Symptom: Sometimes an error log is seen when tracing packets with 'debug platform packet-trace' or some of the data seems inconsistent.

  Conditions: Tracing multicast packets with packet-trace in IOS-XE 3.11.0 or IOS-XE3.12.0 using circular buffering: debug platform packet-trace <num-pkts> circular or using drop tracing: debug platform packet-trace drop [code <code-num>]

  Workaround: Avoid the commands above when using

- CSCun39642

  Symptom: MLP bundle flow control is not functional.

  Conditions: Generate ICMP ECHREQ from the router to outside host over an MLP causes the bundle queuing process with a consequences of WRED malfunction and member links queue growth beyond the set queue-limits.

  Workaround: None.

- CSCun39803

  Symptom: Intermittent connectivity loss between hosts at different OTV sites. Pinging from one host to the other more than 8 times restores connectivity for about 8-10 minutes. Packet captures show ARP request broadcasts from a host at one site not being received by the host at the other site for about 7-8s, and then suddenly starting to work. This problem has a tendency to get worse over time, with more and more hosts being affected over the course of a week or two until connectivity between sites is essentially gone.

Conditions: ASR1K running 15.4 or 15.3 code, possibly earlier code, with OTV configured.

Workaround: None on the ASR thus far. Statically configuring ARP entries on the hosts will work.

- CSCun40957

  Symptom: ISR4400-X Ucode Crash on 15.3(3)S, 15.4(1)S, 15.4(2)S CSR1000v Ucode Crash on 15.4(2)S.

  Conditions: When sending a large packet over a small MTU that results in more than 8 fragments, the ucode will crash.

  Workaround: Ensure your largest MTU is not more than 8x your smallest MTU.

- CSCun41526

  Symptom: On ETR all the datapath packets are punted to RP unexpectedly due to lisp LSB checking.

  Conditions: LISP network, send traffic from ITR to ETR, easy to see without lisp instance scale.

  Workaround: none

- CSCun48994

  Symptom: The CP process crashes while collapsing a hierarchy layer node that had once exceeded 4000 entries. The collapse occurs when the number entries falls below 4000.

  Conditions: This problem occurs while collapsing a node that had once exceeded 400 entries. The problem is specific to MLPPP, MFR and GEC aggregate because these features require notification when a schedule ID changes. The schedule ID changes when a scheduling node is reconstructed. The issue hit when the operation involves both the flushing and SID notification.

  Workaround: None.

- CSCun55310

  Symptom: An ATM-port might show input-errors of type overrun. Conditions: They get counted so, because they hit an on-demand AutoVC, where the nature of the packets (for example ILMI or BPDU) should not raise the VC.

  Workaround: The concerning VC could be configured as permanent or the packets should be prevented on neighbor device as it is seen as unwanted or unexpected traffic.

  Further Problem Description: Counting the packets as errors is correct, but counting them as overruns is misleading.

- CSCun57531

  Symptom: Ucode Crash on CSR1000v.

  Conditions: An initialization race condition may cause the CSR1000v to not align some memory correctly, which will result in a ucode crash.

  Workaround: Reboot the CSR1000v.

- CSCun58672

  Symptom: VTCP not send tcp segments according adjustment mss

  Conditions: tcp sync with mss 1460 from interface B, and Interface A sent out sync with mss 1390 tcp segments (tcp payload 1390) come from interface A observed tcpsegments with tcp payload 1460 sent out via interface B.

  Workaround: None.

- CSCun59253

  Symptom: DMVPN spoke (ISR) gets stuck in NHRP state after config-unconfig-reconfing with TP.

  Conditions: DMVPN with TP.

  Workaround: Reboot the router.

- CSCun74441

  Symptom: When there is TBAR related drops, it is reported as IPFormatErr in Global Statistics.

  Conditions: GetVPN config, with TBAR drops.

  Workaround: None

- CSCun76382

  Symptom: Possible router crash due to deadlock in CPP processor caused by LUT NBAR code.

  Conditions: Crash may occur only if stile_sys_lookup_table_set_aging is used in a loaded protocol pack.

  Workaround: None.

- CSCun78318

  Symptom: ACLs applied to the mgmte do not work on the new active RP after a RP switch over.

  Conditions: After a RP switch over as the old standby RP becomes the new active RP.

  Workaround: Remove then reapply the ACLs to the mgmte on the new active RP.

- CSCun84368

  Symptom: Netflow cache entry is not created for IPV6 flows and entries for IPv4 entries is not accurate . For IPv4 entries the BGP next hop is not updated and set to 0.0.0.0.

  Conditions: Upon Execution of RP switchover.

  Workaround: After RP switch-over, remove BGP configuration from Core router ("P") , and configure it back. updaon BGP update on PE router, the BGP - NH will appear in FNF records.

- CSCun89491

  Symptom: Memory leak in crypto process .

  Conditions:10K scale SA setup and flap testing.

  Workaround: None.

- CSCun85761

  Symptom: L2 frame check failure when payload length increase with ldap alg.

  Conditions: Steps: ====== translate sipAddress into longer address length.

  Workaround: n/a

- CSCun91199

  Symptom: NAT ALG not translating in case of multiple sip address in SDP.

  Conditions: sip invite message containing oline and cline with different addresses and both need translation dynamic nat with acl configured.

  Workaround: Simplify the ACL associated with NAT mapping configuration.

- CSCun89036

  Symptom: Traceback when IPV6 traffic is transiting through ATM sub-interface.

  Conditions: Configuration of "atm route-bridged ipv6" configured at ATM sub-interface level.

  Workaround: none

- CSCun92245

  Symptom: A Cisco router or switch may experiences a memory leak due to "Crypto IKMP" process. This may occur if multiple DHCP servers are configured under crypto config. Eg: crypto isakmp client configuration group NAME dHCP X.X.X.X X.X.X.X dhcp X.X.X.X X.X.X.X

  Conditions: Multiple Dhcp servers configured under crypto.

  Workaround: Only use a single Dhcp server. Due to an error in code, only the memory structures associated with data from the last Dhcp server in the list are properly freed after a lookup takes place. Data from other servers in the list is retained indefinitely with each lookup.

- CSCun97294

  Symptom: core dump won't be generated after kernel crash in x86_64 platforms.

  Conditions: kernel crash.

  Workaround: None.

- CSCun99766

  Symptom: A router crashes while making changes to an AppNav policy map or a class map.

  Conditions: This symptom occurs under the following conditions: - Multiple AppNav controllers are used. - Sessions are created and can be seen using **show service-insertion statistics sessions**. - AppNav policy map and class map is modified when live traffic is redirected by AppNav. - Policy map or class map change results in a mismatch between AppNav controllers.

  Workaround: When using AppNav Controller Group with multiple ACs, avoid changing the policy map or class map when there are active sessions present (use **show service-insertion statistics sessions**.

  Further Problem Description: A crash occurs after a policy map or class map change results in changes to the existing session and subsequently a new connection matching this session is synced to the other ACs which are not aware of the new policy map or class map.

- CSCuo02270

  Symptom: Issues with source VLAN numbers while using with ERSPAN.

  Conditions: VLAN greater than 1005 were not displayed in the running config. There is no service impact.

  Workaround: NA.

- CSCuo02558

  Symptom: Crash in cpp_cp_svr when executing 'show platform packet-trace packet all'.

  Conditions: Crash can only occur when executing 'show platform packet-trace packet all'.

  Workaround: Display a single packet at a time using 'show platform packet-trace packet <num>' instead of using 'all'.

  Further Problem Description: Problem is very difficult to reproduce as probability of hitting the issue is less than 0.1%.

- CSCuo02894

  Symptom: Packet-trace statistics sometimes appear to report out-of-sync counts.

  Conditions: Using packet-trace in IOS-XE3.11.

  Workaround: None.

- CSCuo16280

  Symptom: Router might crash at the traceback as mentioned in description of ddts

  Conditions: This crash can be simulated only with wrong config as it is being done in this case. Wrong config part1: Spoke has an active crypto map based session terminating on DVTI headend. Spoke now tries to bring up dmvpn tunnel (with same 6 tuple info) with same headend. So when shut/noshut is issued for dmvpn tunnel, spoke initiates CHILD_IPSEC_SA request instead of new session request. So when headend gets this child_sa_request proposal, ike forwards the proposal to IPSEC for proposal validation. Ipsec must have rejected the proposal with "no_proposal_chosen/ts_unacceptable" reason (because protocol is 47 for dmvpn and is different from dvti based session which is ?ip?) instead of rejecting it with "invalid KE" reason. Because IKE got unexpected INVALID_KE error from IPSEC (which it should have never got), there is a condition failing in IKE code resulting in crash!! Wrong config part2: Overlapping ikev2 profiles on headend. Which causes dmvpn tunnel also fall on "dvti" based ike profile, resulting in IPSEC proposal validation failure.

  Workaround: Correct the configuration

- CSCuo19730

  Symptom: Cisco IOS XE includes a version of OpenSSL that is affected by the vulnerability identified by the Common Vulnerability and Exposures (CVE) ID CVE-2014-0160.

  This bug has been opened to address the potential impact on this product.

  Conditions: Cisco IOS XE devices running release 3.11.0S, 3.11.1S or 3.12.0S and with the WebUI interface over HTTPs enabled. No other versions of Cisco IOS XE are affected.

  Devices with the WebUI interface enabled and using HTTPs as transport protocol will include the following configuration:

  ```
  transport-map type persistent webui http-webui
   secure-server
  ip http secure-server
  transport type persistent webui input http-webui
  ```

  Devices running IOS XE release 3.11.0S, 3.11.1S or 3.12.0S but WITHOUT the WebUI interface enabled, or with the WebUI interface enabled but NOT using HTTPs as transport protocol are NOT AFFECTED by this vulnerability.

  Devices running IOS XE release 3.11.0S, 3.11.1S or 3.12.0S and with the HTTPs server enabled (by including in their configuration the line "ip http secure-server") are NOT affected. Both the HTTPs server and the WebUI interface need to be enabled for a device to be vulnerable.

  The WebUI configuration guide is available at

  http://www.cisco.com/c/en/us/td/docs/routers/asr1000/configuration/guide/chassis/asrswcfg/webui.html

  Workaround: Not currently available.

  Further Problem Description: Additional details about this vulnerability can be found at http://cve.mitre.org/cve/cve.html

  Software version and Fixes

The first column is the Cisco IOS XE Software Release. The second column is the First Fixed Release.

3.9.xS Not vulnerable

3.10.xS Not vulnerable

3.11.xS Vulnerable

3.12.xS Vulnerable

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4.3/4.3:

https://intellishield.cisco.com/security/alertmanager/cvss?target=new&version=2.0&vector=AV:N/AC:M/Au:N/C:P/I:N/A:N/E:H/RL:U/RC:C

The Cisco PSIRT has assigned this score based on information obtained from multiple sources. This includes the CVSS score assigned by the third-party vendor when available. The CVSS score assigned may not reflect the actual impact on the Cisco Product. CVE-2014-0160 has been assigned to document this issue.

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

http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

- CSCuo20090

  Symptom: The saved ACLs applied to the mgmte from startup-config may not work after system reload.

  Conditions: After system reload.

  Workaround: Remove then reapply the ACLs to the mgmt after system reload.

- CSCuo23251

  Symptom: ucode crash@alg_fw_l7_inspect .

  Conditions: with alg traffic and fw config .

  Workaround: none

- CSCuo02619

  Symptom: IOSD memory leak in CRYPTO_malloc .

  Conditions: flapping flexvpn sessions from Anyconnect or Windows 7 IKEV2 clients.

  Workaround: None

- CSCuo31109

  Symptom: when platform receive a pre inject flow message, current behavior is create this flow in CFT, when a matching packet coming, platform will go to classification feature, if it matches the classification, packet will be punted, if missed, simply do nothing .

  Conditions: call api onep_dpss_pre_flow_add_with_complete_tuple in a callback.

  Workaround: N/A

  Further Problem Description: expected behavior is create this flow in CFT, set action to bypass, when a matching packet coming, bypass the flow. current behavior is create this flow in CFT, when a matching packet coming, platform will go to classification feature, if it matches the classification, packet will be punted, if missed, simply do nothing

- CSCuo40596

  Symptom: when ping xtr to pxtr, the pxtr response message is LSB disabled,the packet was seen on punt path.

  Conditions: None.

  Workaround: It's random, Sometimes will be hit, sometimes is not.

- CSCuo41760

  Symptom: Kernel messages seen on router.

  Conditions: After a router reload and when initiating Vlans through power cli.

  Workaround: None.

- CSCuo42772

  Symptom: can't configure erspan session destination port.

  Conditions: can not configure the erspan destination port when the port index exceed the 9215.

  Workaround: Reload system.

- CSCuo55508

  Symptom: A cpp-ucode crash is encountered.

  Conditions: Using packet-trace to trace packets in a feature environment where packets are replicated using egress conditions. debug platform packet-trace enable debug platform packet-trace packet 16 fia-trace debug platform condition egress debug platform condition start.

  Workaround: Do not use fia-trace.

- CSCuo55610

  Symptom: Incomplete kernel core file with filename ending in .TEMP_IN_PROGRESS.

  Conditions: Active RP kernel core dump in dual RP2 systems.

  Workaround: None

- CSCuo61943

  Symptom: Incorrect classification of NBAR.

  Conditions: Problem should not occur since all protocol packs released to IOS XE version 15.4(02)S will make sure not to introduce this issue.

  Workaround: Not required since released protocol packs will not introduce this issue.

- CSCuo72301

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

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

  Workaround: unknown

- CSCuo74467

  Symptom: GETVPN traffic dropped.

  Conditions: When enabled anti-replay with default time-based 5 seconds.

  Workaround: Increase the anti-replay time interval to 10 seconds .

- CSCuo76455

  Symptom: CSR AMI generate with SRIOV and launched as C3 type cannot be reached after bootup

  Conditions: SRIOV CSR AMI only.

  Workaround: None.

- CSCuo83946

  Symptom: With Cisco IOS-XE 15.4(2)S, when adv/prem 2.5G, 5G or 10G license is installed, no more than 150 IPSec tunnels could be established.

  Conditions: Normal conditions.

  Workaround: No workaround available.

- CSCup22487

  Symptom: Some Cisco IOS-XE releases include a version of openssl that is affected by the vulnerabilities identified by the Common Vulnerability and Exposures (CVE) IDs:

  CVE-2010-5298 - SSL_MODE_RELEASE_BUFFERS session injection or denial of service

  CVE-2014-0076 - Fix for the attack described in the paper "Recovering OpenSSL ECDSA Nonces Using the FLUSH+RELOAD Cache Side-channel Attack"

  CVE-2014-0198 - SSL_MODE_RELEASE_BUFFERS NULL pointer dereference

  CVE-2014-0224 - SSL/TLS MITM vulnerability

  This bug has been opened to address the potential impact on this product.

  Conditions: Devices running an affected version of IOS-XE and the 'webui' has been configured to use HTTPS.

  This vulnerability affects IOS-XE 3.11.0S, 3.11.1S, 3.12.0S, and 3.13.0S.

  Workaround: Not Available.

  Further Problem Description:

  Devices with the WebUI interface enabled and using HTTPs as transport protocol will include the following configuration:

  ```
  transport-map type persistent webui http-webui
   secure-server
  ip http secure-server
  transport type persistent webui input http-webui
  ```

  Devices running IOS XE release 3.11.0S, 3.11.1S or 3.12.0S but WITHOUT the WebUI interface enabled, or with the WebUI interface enabled but NOT using HTTPs as transport protocol are NOT AFFECTED by this vulnerability.

  Devices running IOS XE release 3.11.0S, 3.11.1S or 3.12.0S and with the HTTPs server enabled (by including in their configuration the line "ip http secure-server") are NOT affected. Both the HTTPs server and the WebUI interface need to be enabled for a device to be vulnerable.

  The WebUI configuration guide is available at

  http://www.cisco.com/c/en/us/td/docs/routers/asr1000/configuration/guide/chassis/asrswcfg/webui.html

  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 7.8/7.5:

  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: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

- CSCup22590

  Symptom: Some Cisco Internetwork Operating System (IOS) releases may be affected by the following vulnerabilities:

  These products include a version of openssl that is affected by the vulnerabilities identified by the Common Vulnerability and Exposures (CVE) IDs:

  CVE-2014-0195 - DTLS invalid fragment vulnerability

  CVE-2014-0221 - DTLS recursion flaw

  CVE-2014-0224 - SSL/TLS MITM vulnerability

  This bug has been opened to address the potential impact on this product.

  Conditions: Devices running an affected version of Cisco IOS and utilizing an affected configuration.

  Workaround: None currently available.

  Further Problem Description: CVE-2014-0224:

  All Cisco IOS services that provide a form of TLS or SSL encryption are affected by this vulnerability. This includes features such as the HTTPS Web Management interface.

  CVE-2014-0195:

  Cisco IOS devices that support SSLVPN (AnyConnect) and have the feature configured and enabled are affected by this vulnerability.

  CVE-2014-0198:

  Cisco IOS devices that support SSLVPN (AnyConnect) and have the feature configured and enabled are affected by this vulnerability.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 10/9.5:

  https://intellishield.cisco.com/security/alertmanager/cvss?target=new&version=2.0&vector=AV:N/AC:L/Au:N/C:C/I:C/A:C/E:F/RL:U/RC:C

  The Cisco PSIRT has assigned this score based on information obtained from multiple sources. This includes the CVSS score assigned by the third-party vendor when available. The CVSS score assigned may not reflect the actual impact on the Cisco Product.

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

  http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

Open Caveats—Cisco IOS XE Release 3.12.1S

- CSCum47653

  Symptom: Configuring VRF aware VXLAN results in traffic drop.

  Conditions: Applying the VRF related configuration on the VTEP for VXLAN traffic results in traffic drop.

Workaround: Remove and re-apply the configuration

- CSCum66856

  Symptom: CSR1000:DMVPN stuck in harp with “crypto ikev2 cts “ cli.

  Conditions: Seen with crypto ikev2 cts cli

  Workaround: none

- CSCum69661

  Symptom: Some configuration such as hostname missing after replacing startup config with a different file followed by reload.

  Conditions: Here are conditions under which this issue seen. 1) Erase startup config 2) copy config file from boot-flash or FTP to startup config 3) reload.

  Workaround: Workaround is to re configure the missing config.

- CSCun64410

  Symptom: The Error message

  ```
  "*Mar 11 00:58:05.160: VXE-CSL-DBG:CSR image type = 3GETOBJ 1 = standard,2 =
  csr1000v_ami_byol, 3 = , GRP = csr1000v CONFIG BOOT CONFIG = ZN$ CONFIG BOOT GROUP DID
  NOT MATCH % group 'csr1000v' is not valid "
  ```

  occurs on configuring the license boot level.

  Conditions: The issue is seen only on Cisco CSR 1000v BYOL AMI images, on configuring the license boot level.

  Workaround: User can configure another boot level, without clearing the existing license boot level.

- CSCuo36773

  Symptom: Tracebacks seen on CSR.

  Conditions: None .

  Workaround: None

Resolved Caveats—Cisco IOS XE Release 3.12.0S

- CSCue33225

  Symptom: The **sh plat hard qfp act dat infr sw-hqf** output is truncated.

  Conditions: When 5 Gi interfaces are defined, the output is truncated

  Workaround: Use less than 5 Gi interfaces.

- CSCue75176

  Symptom: IDFW is not working for sgt replaced because of policy static sgt <sgt-num> command.

  Conditions: Configure policy static sgt <sgt-num> command on ingress interface and in FW do match for same sgt number given in this CLI.

  Workaround: None.

- CSCug13606

  Symptom: Gigabit Ethernet interface counters show a value near 2 to the 64th.

  Conditions: Occurs on a Cisco CSR1000v router using VMXNET3 driver after an Etherchannel interface is configured.

  Workaround: Performing “clear counters” will reset the counter to zero.

- CSCuh76624

  Symptom: The **show platform software object-manager f0 statistics** command shows pending-objects that do not clear after making configuration changes (or potentially on system boot).

  Conditions: Can occur on the CSR1000v or ISR4400X platforms with large scale configurations.

  Workaround: No workaround.

- CSCuh84775

  Symptom: An error message will be shown on the screen after adding a new interface on AMI. And the performance will be bad since the MTU is only 1500.

  Conditions: Add a new interface on the fly.

  Workaround: Reload.

- CSCui82955

  Symptom: Observing more packet latency under oversubscribing throughput license on CSR1000v.

  Conditions: Oversubscribing throughput license limit.

  Workaround: No workaround .

- CSCuj09641

  Symptom: There is no rapid-pvst spanning-tree mode in CSR1000v

  Conditions: Rapid-PVST option not observed in case of CSR1000v.

  Workaround: None.

- CSCuj28057

  Symptom: Crash alert group is not subscribed in Cisco TAC profile.

  Conditions: Call-home default configuration.

  Workaround: Create user profile to subscribe crash alert group.

- CSCuj42597

  Symptom: The following firewall policy is attached to the firewall zone-pair to allow http transactions:

```
class-map type inspect match-all http-servers
match protocol http
!
policy-map type inspect fw-policy
  class type inspect http-servers
     inspect
  class class-default
    drop log
```

  The policy would cause lots of TCP out-of-order segment drops for HTTP flows, especially with long HTTP transactions which require multiple segments to complete the transaction (such as downloading large file from HTTP server); the TCP out-of-order segment drops cause lots of retransmissions, lowering the throughput and at times even causing the request to fail:

```
csr01#sh platform hardware qfp active feature firewall drop
-----------------------------------------------------------------------------
Drop Reason                                                          Packets
-----------------------------------------------------------------------------
TCP out-of-order segment                                                6500
Stray Segment                                                              9
```

Replacing the class-map with the following using ACL to match HTTP port does not stop the TCP out-of-order segment drops for HTTP flows:

```
ip access-list extended http-port
   permit tcp any any eq www
!
 class-map type inspect match-all http-servers
    match access-group name http-port
```

Conditions: Filtering HTTP flows.

Workaround: Replace the 'match protocol http' statement with a ACL match statement, and a 'match protocol tcp' statement in the class-map like below:

```
ip access-list extended http-port
   permit tcp any any eq www
!
class-map type inspect match-all http-servers
  match access-group name http-port
  match protocol tcp
```

- CSCuj47897

  Symptom: The inspect class-map is a nested class-map, with one 'match class-map ...' statement already configured. IOSd crash when the 'no match class-map ...' command is entered (e.g., typo error):

  ```
  csr(config)#class-map type inspect parent
  csr(config-cmap)#match class-map child
  csr(config-cmap)#no match class-map non-exist
  ```

  The crash only happens for inspect class-map, performing the same operation with regular class-map does not cause IOSd crash.

  Conditions: Removing non-exist 'match class-map ...' statement from nested inspect class-map.

  Workaround: Make sure no typo when removing 'match class-map ...' statement from nested inspect class-map; or remove the nested class-map and reconfigure with the correct statements.

- CSCuj56977

  Symptom: There is no cap of IPsec tunnel numbers on CSR1000v.

  Conditions: This symptom is observed all the time.

  Workaround: There is no workaround.

- CSCuj89039

  Symptom: REST API is not working on AWS CSR. Conditions: in any condition

  Workarounds: No workaround.

- CSCul21158

  Symptom: ESP crashes for IOS-XE based platforms.

  Conditions: Crash may occur when executing the CLI command: show platform hardware qfp active infrastructure exmem map

  Workaround: None.

  Further Problem Description: Command has been executed in field and internally without issue but the defect has been identified internally and a fix being provided as a preventive measure.

- CSCum04973

  Symptom: CSR1K may experience drops.

Conditions: Communication between hosts through CSR on the same ESXi host - LRO and TSO enabled.

Workaround: Disable LRO and TSO:

1) On the host ESXi we disable LRO and TSO using this procedure:

Log in to the ESXi host or vCenter Server by using the vSphere Client.

Navigate to the host in the inventory tree, and on the Configuration tab click Advanced Settings under Software.

Select Net and scroll down until you reach parameters starting with VMXNET.

Set the following LRO parameters from 1 to 0:

```
netSwLROSL
Net.Vmxnet3SwLRO
Net.Vmxnet3HwLRO
Net.Vmxnet2SwLRO
Net.Vmxnet2HwLRO
Net.UseHwTSO
```

Reboot the ESXi/ESX host to apply the changes.

2) On the end hosts disable LRO and TSO : ethtool -K eth0 tso off ethtool -K eth0 lro off to check if they are disabled: ethtool -k eth0 | grep offload

Further Problem Description: References:

http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2055140

http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=1027511

- CSCum40043

  Symptom: Crypto sessions get stuck in UP-IDLE state in scale scenario on CSR platform.

  Conditions: CSR with XE3.11.

  Workaround: Bring the sessions up in very small increments e.g. of 40 sessions at a time initially and keep monitoring. When the sessions stop coming up for 40 sessions at a time, switch to smaller number e.g. 20.

Open Caveats—Cisco IOS XE Release 3.12.0S

- CSCul97435

  Symptom: Hyper-V Vswitch GUI only allows creation of one VLAN. In addition after the vSwitch GUI is used to create a VLAN it is not possible to send traffic from CSR1000v to a peer using subinterfaces. - Hyper-V vSwitch blocks traffic from mac-addresses that it did not assign. This causes protocols that assign there own mac-addresses to fail. (ex: HSRP, CLNS, EtherChannel).

  Conditions: Problems are observed on CSR1000v running on Hyper-V hypervisor.

  Workaround: No known workarounds.

- CSCum66856

  Symptom: CSR1000: DMVPN stuck in nhrp with “crypto ikev2 cts “ cli

  Conditions: Seen with crypto ikev2 cts cli

  Workaround: None

- CSCum69661

  Symptom: Some configuration such as hostname is missing after replacing startup config with a different file followed by reload.

  Conditions: Here are the conditions under which this issue is seen.

  1) Erase startup config

  2) copy config file from bootflash or tftp to startup config

  3) reload.

  Workaround: Workaround is to reconfigure the missing configuration.

- CSCum89383

  Symptom: When flapping NVI/Loopback interfaces of CSR acting as VxLAN gateway

  Conditions: Happens only with the scaled VxLAN configuration (500 VNI with 1:1 mcast group)

  Workaround: None

- CSCum95132

  Symptom: Kernel crashes occur while executing RFC2544 traffic tests.

  Conditions: Longevity testing starting with packet size of 78 bytes to 1483 bytes utilizing incremental step size of 64 bytes. Typically, the crash occurs after 3-4 iterations of this pattern (1 million packets sent per each packet size).

  Workaround: CPU Affinity (pinning) to KVM process and VHOST process, and utilizing the latest 3.12 images (2/12 and later) thus far has shown this issue to stop.

Caveats—Cisco IOS XE Release 3.11S

Resolved Caveats—Cisco IOS XE Release 3.11.2S

- CSCtq21722

  Symptom: Cisco switch may reload when configured for SNMP.

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

  Workaround: Remove the SNMP host configurations for SNMP informs. eg: no snmp-server host x.x.x.x informs version 2c <removed>

- CSCtz45833

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

  Conditions: Router is acting as a mid point for MPLS-TE tunnels and is doing ERO expansion. In the case the ERO expansion fails (due to IGP race conditions, or inter-AS scenario) and backup tunnels are in use (for MPLS-TE FRR feature) the router may crash.

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

- CSCuc21859

  Symptom: Memory leak is seen at ssf_owner_get_feature_sb.

  Conditions: This symptom occurs when the discriminator configuration is with logging, as given in the below examples: logging discriminator <NAME> logging host x.x.x.x discriminator DEBUG logging discriminator SysLog mnemonics drops NAME.

  Workaround: Remove the discriminator configuration from the logging configuration.

- CSCue23898

  Symptom: A Cisco router running Cisco IOS Release 15.3(1)T may crash with a bus error immediately after issuing the 'write memory' command. Example: 14:44:33 CST Thu Feb 14 2013: TLB (load or instruction fetch) exception, CPU signal 10, PC = 0x228B2C70 \.

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

  Workaround: There is no workaround.

- CSCuh06074

  Symptom: Unnecessary Retransmissions going on in HA mode.

  Conditions: When LDP NSR is enabled on any or all test units.

  Workaround: No workarounds.

  More Info: Occurring mainly due to unusual and indeterminate time taken by IPC to communicate packet info to standby and bring back ack to active

- CSCui52587

  Symptom: When they "no interface Vlan XX", ntp broadcast config in the last vlan will disappear.

```
-------------------------------------------------

router(config-router)#
router(config-router)#do sh run int vlan 905
Building configuration...

Current configuration : 326 bytes
!
interface Vlan905
 ip address X.X.X.X 255.255.255.0
 ip access-group XX out
 no ip redirects
 no ip proxy-arp
 ip pim dr-priority 90
 ip pim query-interval 10
 ip pim sparse-mode
 standby 105 ip X.X.X.X
 standby 105 timers 5 15
 standby 105 priority 150
 standby 105 preempt
 delay 150
 ntp broadcast
end
```

```
router(config-router)#
router(config-router)#no interface Vlan141
router(config)#
router(config)#
router(config)#do sh run int vlan 904
Building configuration...

Current configuration : 324 bytes
!
interface Vlan904
 ip address X.X.X.X 255.255.255.0  ip access-group XX out  no ip redirects  no ip
proxy-arp  ip pim dr-priority 90  ip pim query-interval 10  ip pim sparse-mode
standby 22 ip X.X.X.X  standby 22 timers 5 15  standby 22 priority 150  standby 22
preempt  delay 150  ntp broadcast end

router(config)#
router(config)#
router(config)#do sh run int vlan 905
Building configuration...

Current configuration : 311 bytes
!
interface Vlan905
 ip address X.X.X.X 255.255.255.0
 ip access-group XX out
 no ip redirects
 no ip proxy-arp
 ip pim dr-priority 90
 ip pim query-interval 10
 ip pim sparse-mode
 standby 105 ip X.X.X.X
 standby 105 timers 5 15
 standby 105 priority 150
 standby 105 preempt
 delay 150
end>>>>>>>>>>>>>>>>>> ntp broadcast disappeared
----------------------------------------
```

Conditions: The symptom was confirmed in 15.1(1)SY and 15.1(1)SY1

Workaround: Reconfigure ntp broadcast for the last vlan.

- CSCui73249

  Symptom: NHRP local (no socket) entry gets converted to a socket entry causing matching traffic to be null route.

  Conditions: DMVPN phase 3 network.

  Workaround: Configure 'ip nhrp server-only' or remove 'ip nhrp shortcut' on the hub router.

- CSCuj13596

  Symptom: Issuing a command crypto key move rsa aaa non-exportable" throws an error, Failed to move keypair aaa to device.

  Conditions: Before issuing the above command, generate the rsa keys with label 'aaa'.

  Workaround: None.

- CSCuj66318

  Symptom: After applying an NTP access-group to deny inbound NTP queries, a device still responds to NTP queries as if the ACL was not configured. It will affect IOS-XE too.

  Conditions: An NTP access-group must be configured to deny inbound NTP queries.

```
================ access-list 99 deny any ! ntp access-group query-only 99 ============
```

In the example shown, even though all inbound NTP queries should be denied, we will still process them as if the access-group was not configured

Workaround: Use NTP authentication instead of NTP access-groups to restrict NTP hosts.

More Info: After applying an NTP ACL access-group serve-only to permit inbound NTP client request - the correct ntp client association is established only in case that NTP authentication is applied.

- CSCuj88820

  Symptom: Router acting as a PKI client continues auto-enrollment to its CA even after the CA certificate has expired.

  Conditions: Client router is configured with 'auto-enroll' under its trustpoint.

  Workaround: Remove 'auto-enroll' from the trustpoint on the PKI client router, or, Delete the trustpoint in question on the PKI client router.

  Further Problem Description: Consider a scenario where a PKI client has failed to auto renew its identity certificate i.e. it failed to re-enroll with its CA for some reason. The client router is expected to retry until one of the conditions below is reached: 1. "enrollment retry count" which is configured under the trustpoint is reached or, 2. CA certificate expires. However, it is seen the client router will continuously attempt to auto renew its identity certificate even after the CA certificate has expired.

- CSCul01067

  Symptom: Memory leak occurs in process and I/O memory.

  Conditions: This symptom is observed when NTPv6 is configured, for example; "ntp server ipv6 2001::1"

  Workaround: Remove the NTPv6 configuration.

- CSCul18872

  Symptom: An LDP session to a Juniper peer flaps when RP switchover occurs with mpls ldp nsr configured on a Cisco router running IOS.

  Conditions: This symptom is observed when an mpls LDP session is established with a Juniper peer and RP switchover occurs with mpls ldp nsr configured.

  Workaround: In order to workaround the traffic loss which occurs when the session flaps, configure mpls ldp graceful-restart in addition to nsr.

- CSCul90667

  Symptom: Error message and traceback are printed to console. Conditions: IGP times out while Standby RP is becoming NSR Active.

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

- CSCum19875

  Symptom: PW status change messages, XCONNECT-5-PW_STATUS, are not all captured in log when PW status change logging is enabled.

  Conditions: XCONNECT-5-PW_STATUS messages were rate-limited to 8 messages per 8 msec. For example, if 10 PWs changed state together via interface down then 8 messages would be logged and the remaining would be lost.

  Workaround: No workaround.

- CSCum48928

  Symptom: XML Bootstrap configuration for the CSR1000v containing the configuration commands "service internal" and "license accept end user agreement force" is not successfully applied, as the "license ..." command is always issued before the "service internal" command, regardless of which command comes first in the XML file.

  Conditions: Only happens on CSR1000v and only happens when the bootstrap configuration commands are provided in XML (ovf-env.xml) format.

  Workaround: Provide plain-text bootstrap configuration file (iosxe_config.txt) instead.

  Further Problem Description: Cisco Virtual Appliance Configuration (CVAC) subsystem in IOSd attempts to fix up the order of XML configuration commands by moving all "license" commands to the head of the list. However, "license accept end user agreement force" is only a valid command after "service internal" has been configured, so this re-ordering causes the command to be rejected.

- CSCun45272

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

  Conditions: A reoptimization of a tunnel that has failed with path protection enabled.

  Workaround: There is no workaround.

- CSCun49450

  Symptom: CSR1000v may lose the configuration when performing a password recovery.

  Conditions: Configuration is ignored by changing the configuration register to 0x40, and the system is booted in an effort to recover from a lost password.

  Workaround: Restore the configuration from a backup copy.

- CSCun63294

  Symptom: TCP connections into/out of applications running in virtual service containers can stall and never revive. This can be seen by trying to scp a large file into a container, and also for any TCP connection (e.g. Thrift) out from the container.

  Conditions: Any large file transfer over TCP or long lived TCP connection with reasonable traffic bandwidth/total.

  Workaround: None known. More Info: Transferring of small files, or short lived TCP connections do not seem to be affected. Non-TCP protocols (e.g. UDP) do not seem to be affected.

- CSCun73782

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

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

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

Workaround: 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 4.3/3.6:

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

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

Additional details about the vulnerability described here can be found at:

http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-3262

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

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

- CSCuo19730

  Symptom: Cisco IOS XE includes a version of OpenSSL that is affected by the vulnerability identified by the Common Vulnerability and Exposures (CVE) ID CVE-2014-0160.

  This bug has been opened to address the potential impact on this product.

  Conditions: Cisco IOS XE devices running release 3.11.0S, 3.11.1S or 3.12.0S and with the WebUI interface over HTTPs enabled. No other versions of Cisco IOS XE are affected.

  Devices with the WebUI interface enabled and using HTTPs as transport protocol will include the following configuration:

```
transport-map type persistent webui http-webui
 secure-server
ip http secure-server
transport type persistent webui input http-webui
```

  Devices running IOS XE release 3.11.0S, 3.11.1S or 3.12.0S but WITHOUT the WebUI interface enabled, or with the WebUI interface enabled but NOT using HTTPs as transport protocol are NOT AFFECTED by this vulnerability.

  Devices running IOS XE release 3.11.0S, 3.11.1S or 3.12.0S and with the HTTPs server enabled (by including in their configuration the line "ip http secure-server") are NOT affected. Both the HTTPs server and the WebUI interface need to be enabled for a device to be vulnerable.

  The WebUI configuration guide is available at

  http://www.cisco.com/c/en/us/td/docs/routers/asr1000/configuration/guide/chassis/asrswcfg/webui.html

  Workaround: Not currently available.

  Further Problem Description: Additional details about this vulnerability can be found at http://cve.mitre.org/cve/cve.html

  Software version and Fixes

  The first column is the Cisco IOS XE Software Release. The second column is the First Fixed Release.

  3.9.xS Not vulnerable

  3.10.xS Not vulnerable

  3.11.xS Vulnerable

  3.12.xS Vulnerable

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4.3/4.3:

https://intellishield.cisco.com/security/alertmanager/cvss?target=new&version=2.0&vector=AV:N/AC:M/Au:N/C:P/I:N/A:N/E:H/RL:U/RC:C

The Cisco PSIRT has assigned this score based on information obtained from multiple sources. This includes the CVSS score assigned by the third-party vendor when available. The CVSS score assigned may not reflect the actual impact on the Cisco Product. CVE-2014-0160 has been assigned to document this issue.

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

http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

Resolved Caveats—Cisco IOS XE Release 3.11.1S

- CSCuh84775

  Symptom: An error message will be shown on the screen after adding a new interface on AMI. And the performance will be bad since the MTU is only 1500.

  Conditions: Add a new interface on the fly.

  Workaround: Reload.

- CSCuj75560

  Symptom: Cannot recover from a CSR 1000v failed-to-apply state after the policy is deleted or moved to a different profile.

  Conditions: This problem occurs when trying to instantiate or assign a CSR 1000v with a wrong configuration. A failed-to-apply state appears. If you delete or move to a different policy without fixing the configuration, the failed-to-apply state remains.

  Workaround: Do one of the following:

  - If instantiating a CSR 1000v, redeploy the CSR 1000v with the correct configuration.
  - If assigning a CSR 1000v, fix the configuration, then uninstall and install the Prime NSC CPA process in the CSR device.

- CSCul00007

  Symptom: Files cannot be downloaded via the management interface via FTP/HTTP/SCP. This can include firmware files, configuration files, or license files.

  Conditions: This symptom occurs on using the management interface on a Cisco ASR 1000 or ISR 4450-X router.

  Workaround: There are two workarounds for this issue.

  (1) Use an interface other than the management interface to download the file or use a protocol that does not use TCP as the session transport such as TFTP.

  (2) Set the IP_ADDRESS rommon variable to the IP address of the management interface.

- CSCul02627

  Symptom: UEA: Log files are not generated with PTP configurations

  Conditions: Configure RSP2 as the slave and RSP1 as the master

Go to shell using “request platform software system shell”

cd /tmp/rp/trace

ls -ltr

Notice that the log files related to PTP aren't present

Workaround: Reload of RSP2

- CSCul28053

  Symptom: ASR1k [or any IOS-XE based Cisco Router, like CSR1kv] sends Radius Accounting Stop message even when the IPSec VPN session is up. For example in XE 3.9 stop request is sent after about 1600 seconds, and in XE 3.9.2 it is sent after about 5800 seconds.

  Conditions: ASR1k [or any IOS-XE based Cisco Router, like CSR1kv] acting as IPSec [IKEv1] Server. Also It is configured to perform VPN client authentication and accounting with the Radius Server.

  Workaround: None

- CSCul53598

  Symptom: POST /api/v1/auth/token-services return HTTP response code 201 instead of 200

  Conditions: When creating a token.

  Workaround: None.

- CSCul66853

  Symptom: Routing policy is not configured correctly if using routing profile swapping.

  Conditions: If the routing policy has the same rules between the swapped profiles.

  Workaround: No workaround.

- CSCul82306

  Symptom: PUT on /api/vi1/interface/<intf> with an empty string "" does not clear or unset the description.

  Conditions:

  Workaround: To clear or unset the description, omit the description attribute in the JSON input for the PUT request.

- CSCum04973

  Symptom: CSR 1000v may experience drops.

  Conditions: Communication between hosts through CSR on the same ESXi host - LRO and TSO enabled.

  Workaround: Disable LRO and TSO:

  1) On the host ESXi we disable LRO and TSO using this procedure:

     Log in to the ESXi host or vCenter Server by using the vSphere Client.

     Navigate to the host in the inventory tree, and on the Configuration tab click Advanced Settings under Software.

     Select Net and scroll down until you reach parameters starting with VMXNET.

     Set the following LRO parameters from 1 to 0:

     ```
     netSwLROSL
     Net.Vmxnet3SwLRO
     Net.Vmxnet3HwLRO
     ```

```
Net.Vmxnet2SwLRO
Net.Vmxnet2HwLRO
Net.UseHwTSO
```

Reboot the ESXi/ESX host to apply the changes.

2) On the end hosts disable LRO and TSO : ethtool -K eth0 tso off ethtool -K eth0 lro off to check if they are disabled: ethtool -k eth0 | grep offload

Further Problem Description: References:

http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2055140

http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=1027511

Open Caveats—Cisco IOS XE Release 3.11.1S

- CSCuj20980

  Symptom:CSR1000v reloads when using VxLAN.

  Conditions: An interface configured with VxLAN is flapped. Greater than 2k VNIs are used.

  Workaround: Note that it is recommend to use less than 2k VNIs. However, this may not completely mitigate the issue

- CSCum40043

  Symptom: Crypto sessions get stuck in UP-IDLE state in scale scenario on CSR platform.

  Conditions: CSR with XE3.11.

  Workaround: Bring the sessions up in very small increments e.g. of 40 sessions at a time initially and keep monitoring. When the sessions stop coming up for 40 sessions at a time, switch to smaller number e.g. 20.

- CSCuh56746

  Symptom: Crash observed when creating a zone for zone based firewalls

  Conditions: Seen when using standard or evaluation licenses.

  Workaround: Apply the appropriate premium or advance license to configure zone based firewalls.

Resolved Caveats—Cisco IOS XE Release 3.11.0S

- CSCug99517

  Symptom: the CSR will continuing try to boot IOS and not complete. It will generate a kernel crash.

  Conditions: When enabling VMware FT on CSR VM and power up.

  Workaround: Don't enable VMware FT.

- CSCuh11994

  Symptom: cpp_svr crash noticed executing the command **show platform hardware cpp active infrastructure punt policer handle 1000 cpp**

  Conditions: Noticed without any feature configurations

  Workaround: None

- CSCuh18239

  Symptom: The CSR may crash when sweeping between 2 CSR's with larger 9KB MTU while inducing link reset.

  Conditions: When sending large MTU traffic, and creating link reset.

  Workaround: Avoid causing link reset repeatedly.

- CSCuh19651

  Symptom: cpp_cp_svr process on a CSR1000v router crashes.

  Conditions: Crash occurs when nbar is configured on a virtual machine with less than 4GB of memory.

  Workaround: When configuring nbar use at least 4GB of memory on the Virtual Machine.

- CSCuh36562

  Symptom: The CSR running on ESXi will dump trace back continuously when config the 10th VMXNET3 interface.

  Conditions: When configure the 10th VMXNET3 interface.

  Workaround: None

- CSCuh76624

  Symptom: The **show platform software object-manager f0 statistics** command shows pending-objects that do not clear after making configuration changes (or potentially on system boot).

  Conditions: Can occur on the CSR1000v or ISR4400X platforms with large scale configurations.

  Workaround: No workaround

- CSCui05390

  Symptom: The hierarchical QoS policy like the following is attached to an interface:

```
class-map match-any control-protocols
match access-group name control-protocols
match dscp cs6
class-map match-all netflow-export
match access-group name netflow-export
!
policy-map child-qos
class control-protocols
bandwidth percent 10
class netflow-export
bandwidth percent 5
set dscp cs6
class class-default
bandwidth percent 85
policy-map parent-qos
class class-default
shape average 50000000
service-policy child-qos
!
interface GigabitEthernet3
ip address 11.1.2.1 255.255.255.0
service-policy output parent-qos
```

  No traceback seen when the QoS policy is attached to the interface. However after saving configuration, then reboot the CSR, most of the times, the following traceback and error message is seen when the CSR boot up:

```
*Jul 11 22:20:58.678: %CPPOSLIB-3-ERROR_NOTIFY: F0: cpp_cp: cpp_cp encountered an
error -Traceback= 1#f1dd138d618ceb5371e769279bde85a8 errmsg:7F2B10679000+121D
cpp_common_os:7F2B13694000+DA05 cpp_common_os:7F2B13694000+D904
cpp_common_os:7F2B13694000+19BDE cpp_bqs_mgr_lib:7F2B241E8000+1CDE6
cpp_bqs_mgr_lib:7F2B241E8000+123C9 cpp_qos_ea_lib:7F2B254FD000+108B5
cpp_qos_smc_lib:7F2B25781000+2016 cpp_common_os:7F2B13694000+11F9E
cpp_common_os:7F2B13694000+119DA cpp_common_os:7F2B13694000+1181B evlib:7F2B1266D00
*Jul 11 22:20:58.701: %FMFP-3-OBJ_DWNLD_TO_CPP_FAILED: F0: fman_fp_image: qos hqf:
class=0.0, dpidx=6, qid=0x0:0x40000001 (p:0x40000001), dir=both directions download to
CPP failed
```

Conditions: Attaching hierarchical QoS policy to interface, save config, and reboot the CSR.

Workaround: None.

- CSCui36288

  Symptom: CRS kernel crash when adding or removing vNIC to the CSR VM from vSphere.

  Conditions: Virtual interfaces deleted dynamically via vSphere may eventually cause corruption of data resulting in a crash of the Linux kernel

  Workaround: Do not remove virtual interfaces dynamically (while router is running). Instead, take the router out of service, delete the virtual interface, and re-start the router.

- CSCuj50874

  Symptom: CSR licensing not taking any effect

  Conditions: On a CSR router with 10Mbps license, we are able to send 54Mbps of traffic without any drops

  Workaround: none

- CSCuj78853

  Symptom: Crash when doing config replace with active traffic

  Conditions: With OTV active flow, when we do config replace, we observe the crash.

  Workaround: None

Open Caveats—Cisco IOS XE Release 3.11.0S

- CSCui49262

  Symptom: No characters are displayed when typed.

  Conditions: When booting up CSR with csr.cnfg.

  Workaround: Reboot the CSR.

- CSCuj45318

  Symptom: The CSR Management container hosting the REST API and Cisco Prime Network Services Controller functionalities sometimes cannot successfully pick up its IP address from the system configuration. This will result in two symptoms:

  - REST API URLs will not be reachable.
  - Cisco PNSC will report the Cisco CSR1000v as unreachable.

  Conditions: During periods of high memory usage, particular during boot up after license level change.

  Workaround: Reboot the Cisco CSR 1000v.

Caveats—Cisco IOS XE Release 3.10S

Resolved Caveats—Cisco IOS XE Release 3.10.3S

- CSCto07376

  Symptom: The device reload when we grant certificates. crypto pki server <> grant all.

  Conditions: Configured for crypto.

  Workaround: None.

- CSCua73834

  Symptom: IOS CA issues incorrect rollover identity certificates to its clients; the rollover certificates issued will have an expiry date corresponding to the end-date of the currently active (and soon to expire) CA certificate. Thus, the rollover identity certificate will not be valid after the CA rollover takes place.

  Conditions: The issue is seen only if the clients have sent the rollover certificate request via an IOS RA certificate server.

  Workaround: None.

- CSCuh47047

  Symptom: An IOS router may fail IKE Main Mode negotiation if the peer device sends both the seconds and kilobytes Life Type with their respective Life Duration attributes.

  Conditions: This condition can occur when an IOS router is the responder for an IKE session, and the peer proposes both seconds and kilobytes Life Duration in its SA proposal.

  Workaround: The workaround is to remove one of the Life Type attributes from the peer device configuration.

- CSCui59927

  Symptom: Memory Leak observed on the device due to IPSEC causing the free memory to deplete to an extent where box becomes unreachable.

  Conditions: IPSEC scaling being high.

  Workaround: Reduce Scaling of IPSEC sessions.

- CSCui39989

  Symptom: PKI fails to validate (sub, peer) cert chain received from IKE.

  Conditions: - PKI hierarchy: root -> sub -> peer - root and sub locally trusted - IKE profile configured with "ca trust-point sub" only - chain-validation from sub to root

- CSCuj40010

  Symptom: When the primary peer becomes unreachable, the FlexVPN client establishes a tunnel with the backup peer as expected. However, if the primary peer becomes reachable again, the client attempts to build a new tunnel even though it has an existing active tunnel with the backup peer.

  Conditions: The Flex client is configured with multiple peers and peer reactivate is not enabled.

Workaround: None.

- CSCuj74574

  Symptom: Router acting as a PKI client fails to delete its expired identity and CA certificates after it has rolled over. So, the output of "show crypto pki certificate" shows that the router has two sets of certificates: One set of identity and CA certificates that is current and valid. Another set of identity and CA certificates that is old and expired. Both sets of certificates are bound to the same trustpoint.

  Conditions: The issue is seen primarily when the client router has enrolled to an IOS CA via and IOS RA router.

  Workaround: None. The old set of certificates get deleted eventually upon the next certificate renewal process initiated by the client router.

  Further Problem Description: An example of what is observed:

```
Router#sh crypto pki cert
Time source is NTP, 16:18:12.777 UTC Tue Oct 8 2013
!--- Note the current time above.

Certificate
  Status: Available
  Certificate Serial Number (hex): 0B
  Certificate Usage: General Purpose
  Issuer:
    cn=Root-CA
    ou=TAC
    o=Cisco
    c=IN
  Subject:
    Name: DMVPN-HUB1-NEW.cvo.IN.Cisco.Cisco
    Serial Number: XYZ1234567A
    serialNumber=XYZ1234567A+hostname=DMVPN-HUB1-NEW.cvo.IN.Cisco.Cisco
  Validity Date:
    start date: 16:17:31 UTC Oct 8 2013
    end   date: 16:37:31 UTC Oct 8 2013
  Associated Trustpoints: cvo-pki

CA Certificate (Rollover)
  Status: Available
  Certificate Serial Number (hex): 09
  Certificate Usage: Signature
  Issuer:
    cn=Root-CA
    ou=TAC
    o=Cisco
    c=IN
  Subject:
    Name: Root-CA
    cn=Root-CA
    ou=TAC
    o=Cisco
    c=IN
  Validity Date:
    start date: 16:17:31 UTC Oct 8 2013
    end   date: 16:57:31 UTC Oct 8 2013
  Associated Trustpoints: cvo-pki

Certificate
  Certificate Serial Number (hex): 08
  <snip>
  Subject:
```

```
    Name: DMVPN-HUB1-NEW.cvo.IN.Cisco.Cisco
  Validity Date:
    start date: 15:57:05 UTC Oct 8 2013
    end   date: 16:17:31 UTC Oct 8 2013
  Associated Trustpoints: cvo-pki
!--- This is the old/expired ID cert.

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 05
  <snip>
  Subject:
    Name: Root-CA
    :
  Validity Date:
    start date: 15:37:31 UTC Oct 8 2013
    end   date: 16:17:31 UTC Oct 8 2013
  Associated Trustpoints: cvo-pki
!--- This is the old/expired CA cert.
```

- CSCuj88820

  Symptom: Router acting as a PKI client continues auto-enrollment to its CA even after the CA certificate has expired.

  Conditions: Client router is configured with 'auto-enroll' under its trustpoint.

  Workaround: Remove 'auto-enroll' from the trustpoint on the PKI client router, or, Delete the trustpoint in question on the PKI client router.

  Further Problem Description: Consider a scenario where a PKI client has failed to auto renew its identity certificate i.e. it failed to re-enroll with its CA for some reason. The client router is expected to retry until one of the conditions below is reached:

  1. "enrollment retry count" which is configured under the trustpoint is reached or,

  2. CA certificate expires. However, it is seen the client router will continuously attempt to auto renew its identity certificate even after the CA certificate has expired.

- CSCuj96893

  Symptom: Cisco router hangs and it stopped passing the traffic. Customer needs to reload the router to make it work until it hangs next time. It hangs sometimes once in month.

  Conditions: This issue is seen with more than one router.

  Workaround: There is no workaround.

- CSCul05056

  Symptom: A Cisco router may crash when configuring NBAR or any other feature which enables NBAR internally. In the crash log file, the crash will be shown as a STACKLOW condition. Examples of this are:

  ```
  %SYS-6-STACKLOW: Stack for process Config Probe running low, 0/12000 %SYS-6-STACKLOW:
  Stack for process SSH Process running low, 0/12000 %SYS-6-STACKLOW: Stack for process
  InitializeNbarAPI running low, 0/12000
  ```

  Conditions: This crash is triggered by enabling NBAR directly or indirectly through another feature. Two such examples are configuring NAT on an interface or configuring NBAR on an interface. For example:

  ```
  (config)#interface gigabitethernet0/1
  (config-if)#ip nbar protocol-discovery
  (config)#interface gigabitethernet0/1
  (config-if)#ip nat inside
  ```

The router may not crash depending on how the configuration is done. For example configuring the feature over the console will not cause a crash. Configuring the feature over SSH, through FTP, Smart Install, etc though will cause the crash.

Workaround: A possible workaround may be to configure the feature over the console or through telnet.

- CSCul13619

  Symptom: When incoming ESP packet has as final destination a local interface on the GM itself (including loopback), the packet is recirculated after decryption causing it to be dropped. If the decrypted packet is only a transit one, for example, it is for a host on a connected LAN, all works as expected.

  Conditions: This issue occurs due to GETvpn, ipv6 and use of ingress ipv6 access lists.

  Workaround: There is no workaround.

- CSCul40500

  Symptom: MD5 is used to sign the PKCS10 embedded in SCEP encrypted message whatever hashing algorithm is configured under the relevant trustpoint or whatever the best hashing algorithm reported by the SCEP GetCACaps message is.

  Conditions: Using SCEP for router enrollment.

  Workaround: None.

- CSCul93523

  Symptom: CPP 0 failure Stuck Thread(s) detected.

  Conditions: Setting up about 2.2kps traffic with both nat/non-nat packets.

  Workaround: none

- CSCum04973

  Symptom: CSR1K may experience drops.

  Conditions: - communication between hosts through CSR on the same ESXi host - LRO and TSO enabled.

  Workaround: disable LRO and TSO: 1) On the host ESXi we disable LRO and TSO using this procedure: Log in to the ESXi host or vCenter Server by using the vSphere Client. Navigate to the host in the inventory tree, and on the Configuration tab click Advanced Settings under Software. Select Net and scroll down until you reach parameters starting with Vmxnet. Set the following LRO parameters from 1 to 0: Net.VmxnetSwLROSL Net.Vmxnet3SwLRO Net.Vmxnet3HwLRO Net.Vmxnet2SwLRO Net.Vmxnet2HwLRO Net.UseHwTSO Reboot the ESXi/ESX host to apply the changes. 2) On the end hosts disable LRO and TSO : ethtool -K eth0 tso off ethtool -K eth0 lro off to check if they are disabled: ethtool -k eth0 | grep offload

  Further Problem Description: References:
  http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2055140

  http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=1027511

- CSCum08864

  Symptom: When there is policy changed (either KS or GM) in Pre-PAL, ASR1K used to re-register. The reason is that in TCAM we can't insert or move SA. ACL merge was done in ACE driver, re-registration was triggered from there. Post-PAL, ACL merge intelligence is moved to Control plane, so ACL is changed, it does the change flow priority. The SA is inserted with second priority, ASR1K is not able to handle that.

  Conditions: ACL change on the KS or the GM.

  Workaround: There are 4 Workaround :

  1. Manually clear GetVPN registration on ASR1K using "clear crypto gdoi".

  2. If permit ACL is appended to KS ACL or ACL is removed from bottom of KS ACL, then there is not flow priority change, and issue is not observed there. Limitation with this workaround is Group config on KS has only one SA. Also if Deny ACL is added there are few packet drops are observed.

  3. EEM script which monitors Rekey Syslog and clears the registration. This is same as workaround 1, but automatically done. disadvantage of this workaround is that Rekey syslog is same during normal rekey and policy change rekey, so with normal rekey also re-registration will happen. Sample EEM script : event manager applet GM_RE_REG event syslog occurs 1 pattern ".*GM_RECV_REKEY.*" action 10 syslog priority warnings msg "EEM trigger workaround for CSCum08864" action 20 cli command "enable" action 30 cli command "clear cry gdoi" pattern "Are you sure you want to proceed" action 40 cli command "yes".

  4. The ACL swapped on KS with new ACL and Rekey is done. The ASR1K GM will re-register, there is small packet drop during re-registration.

- CSCum29065

  Symptom: Group override does not take effect for interface-config strings. Actual ordering of interface config strings on cloned V-Access does not correspond to the expected order based on AAA settings in IKEv2 profile.

  Conditions: User & group authorization configured in IKEv2 profile.

  Workaround: Move all config-string attributes to a single authorization source (user or group).

- CSCum32910

  Symptom: Chunk manager is consuming memory with the allocated memory incrementing on SADB Peering Ch.

  Conditions: Leak when crypto is configured.

  Workaround: none

- CSCum61595

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

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

  Conditions: This symptom does not occur under specific conditions.

  Workaround: There is no workaround.

- CSCum71485

  Symptom: Increasing number of TEK generated every 30 secs.

  Conditions: 1. Change the Group Identity on the Secondary KS causing encryption failure, Change the Group Identity on the Primary KS. All the GMs are deleted from the KSs.

2. Restore the Secondary Key Server. Wait for it to come up as Primary for the Group : GETVPN-GROUP-1

3. Restore the Primary Key Server with Group : GETVPN-GROUP-1

4. This is creating a new TEK policy every 30 sec from the newly elected Primary Key Server KS2. The sequence number for rekey remains 1.

5. KS1 is restored to be the primary role. 6. After the existing TEKS from the KS2 are expired it behaves normally.

Workaround: None.

- CSCum73167

  Symptom: LDAP ALG will encode the packet even there is no need to translate them, this will not impact function, but it is not necessary.

  Conditions: LDAP ALG will encode the packet even there is no need to translate them.

  Workaround: Will not impact function

- CSCum93484

  Symptom: Cisco 7301 router running EzVPN leaks memory when Crypto IKMP calls AAA API's which allocates memory for AAA attribute list.

  Conditions: This symptom is observed in device running EzVPN, when it tries to allocate memory for AAA attribute list.

  Workaround: Reload the router.

- CSCum94408

  Symptom: Intermittently, if a root's CRL to validate Sub does not get downloaded [Internal or External failures], and the CRL by Sub gets downloaded, the following message will be seen:

  ```
  [Debug crypto isakmp and Debug crypto pki m/t/v/c] ISAKMP (35845): adding peer's
  pubkey to cache ISAKMP:(35845): processing SIG payload. message ID = 0
  %CRYPTO-3-IKMP_QUERY_KEY: Querying key pair failed.
  ```

  Conditions: This symptom occurs in Cisco IOS configured with the IKEv1, Authentication mode RSA-SIG [Certificates]. PKI Infrastructure is as follows: Root -> Sub -> ID - Root and Sub Trustpoint have "revocation-check crl none". - Sub has "chain-validation continue Root".

  Workaround: Disable Revocation-check and Chain-validation under Sub Trustpoint.

- CSCum96156

  Symptom: IOS will fail to match the certificate map intermittently.

  Conditions: IOS PKI using certificate maps, to authorize the Peer certificates or override CDP. In this case: - if a certificate map is written on a PC, with upper case letters in them: Ex: crypto pki certificate map HR-Users 10 subject-name co ou = HR-Users - and this is a part of the configuration that is merged with the running config through IOS file-system [directly from flash or FTP/TFTP/HTTP etc], IOS retains the upper case letters. [contrary to certificate maps written through CLI, always converts everything to lower case letters]

  Workaround:

  A) - copy the certificate maps [that have upper case letters in them] to a notepad - remove the certificate maps [that have upper case letters in them] - paste the certificate maps, through IOS CLI - wherever these cert maps were being called, they will stay intact, and this change will take effect immediately or

B) - The certificate map needs to enter IOS in a manner that IOS would insert it if you were to enter it in a CLI I.e. Make sure the external config generators generate the certificate map in such a way that everything is in lower case, and it has white spaces between DN OID, '=' and the value.

- CSCun09640

  Symptom:

  The following errors are seen when adding a child policy to a parent policy while configuring hierarchical QoS.

```
 %CPPOSLIB-3-ERROR_NOTIFY: F0: cpp_cp:  cpp_cp encountered an error
 %CPPOSLIB-3-ERROR_NOTIFY: F0: fman_fp_image:  fman-fp encountered an error
%PMAN-3-PROCHOLDDOWN: F0: pman.sh:  The process cpp_ha_top_level_server has been
helddown (rc 69)
%PMAN-3-PROCHOLDDOWN: F0: pman.sh: The process cpp_cp_svr has been helddown (rc 134)
```

  This can result in a ESP (F Fabric) reload, causing a traffic outage

```
*Feb 13 07:39:05.829: %IOSXE_OIR-6-ONLINECARD: Card (fp) online in slot F0
```

  Conditions:

  1. An interface with a service-policy applied.

  2. Replacing the child policy on the parent hierarchical policy applied to the interface.

  Workaround:Remove the policy from the interface before making the changes to the child/parent policy then reapply the policy to the parent.

  OR

  If you issue the no command to remove the child policy from the parent and then query for pending configuration objects using the "show platform software object-manager fp active statistics" command to make sure there are no pending objects, then issue the service-policy to add the new child policy to the parent, you will not see the ESP crash.

  Further Problem Description:

  When replacing the child policy configured on a parent policy applied to an interface, the ESP may crash.

```
conf t
policy-map parent
class class-default
no service-policy child_A
service-policy child_B
end
```

  Using a file, that replace a child policy, copied from the hard-disk of the router to the running configuration will almost always cause the ESP to crash. If file is copied from tftp, it is less likely. If using CLI to replace the child policy, crash has not been experienced, but can not be completely ruled out. The issue is heavily based on timing and how fast the "no service-policy child_A" and "service-policy child_b" are processed together.

- CSCun26137

  Symptom: ISR G2 router may crash while configure VTI/GRE tunnels.

  Conditions: Configuring VTI/GRE tunnels.

  Workaround: Shut down tunnel before making tunnel configuration changes

- CSCun31021

  Symptom: A vulnerability in IKE module of Cisco IOS and Cisco IOS XE could allow an unauthenticated, remote attacker to affect already established Security Associations (SA). The vulnerability is due to a wrong handling of rogue IKE Main Mode packets. An attacker could exploit this vulnerability by sending a crafted Main Mode packet to an affected device. An exploit could allow the attacker to cause dropping of valid, established IKE Security Associations on an affected device.

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

  Workaround: 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 4.3/3.6:

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

  CVE ID CVE-2014-2143 has been assigned to document this issue. Additional details about the vulnerability described here can be found at:

  http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-2143

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

- CSCun99766

  Symptom: Router crashed while making changes to AppNav policy-map and/or class-map.

  Conditions: Multiple AppNav controllers are used. Sessions had been created and can be seen using "show service-insertion statistics sessions". AppNav policy-map and class-map is modified when live traffic are being redirected by AppNav. Policy-map / class-map change resulted in mismatch between AppNav Controllers.

  Workaround: When using AppNav Controller Group with multiple ACs, avoid changing policy-map / class-map when there are active sessions present (use "show service-insertion statistics sessions").

  Further Problem Description: When policy-map, class-map change results in changes to existing session. When a new connection matching this session is sync'd to the other ACs which are not aware of the policy-map / class-map, it results in crash.

- CSCuo02558

  Symptom: Crash in cpp_cp_svr when executing 'show platform packet-trace packet all'.

  Conditions: Crash can only occur when executing 'show platform packet-trace packet all'.

  Workaround: Display a single packet at a time using 'show platform packet-trace packet <num>' instead of using 'all'.

  Further Problem Description: Problem is very difficult to reproduce as probability of hitting the issue is less than 0.1%.

Resolved Caveats—Cisco IOS XE Release 3.10.2S

- CSCug63839

  Symptom: The Cisco 7301 router running c7301-advipservicesk9-mz.152-4.M3 experiences a memory leak in the Crypto IKMP process particularly on the crypto_ikmp_config_send_ack_addr function.

Conditions: This symptom occurs when running the Cisco 7301 router and connecting EasyVPN through it.

Workaround: Reload the router over a period of time.

- CSCuh35993

  Symptom: create an RRI route for deny ACL lines in the crypto map

  Conditions: 15.x code and L2L ipsec tunnel

  Workaround: None

- CSCui06926

  Symptom: Initiator sends identity certificate based on “ca trustpoint” under the isakmp-profile. However, the responder does not do this. Instead it gets the identity certificate from the *first* trustpoint (out of the list of trustpoints) based on peer's cert_req payload in MM3.

  Conditions: This symptom is observed under the following conditions: 1. IKEv1 with RSA-SIg Authentication, where each Peer has two certificates issued by the same CA. 2. Each Peer has isakmp profiles defined that match on certificate-map and have “ca trustpoint” statements with self-identity as fqdn.

  Workaround: There is no workaround. At this point, responder does not have control over selecting the right certificate.

- CSCui84532

  Symptom: RP is again fragmenting it.

  Conditions: Giant pkts are sent from SPA after LAF.

  Workaround: No work around.

- CSCui85371

  Symptom: Ikev2 session is NOT coming UP

  Conditions: Ikev2 session is NOT coming UP Loopback to loopback ping is not going through.

  Workaround: NO

- CSCuj02503

  Symptom:'Internal_service' license state shows as 'Active, Not In Use' even after its expiry. The system Linux Shell cannot be accessed upon expiry of the 'Internal_service' 1 Day license which is expected. However if an new 1 Day license is installed again, the license state comes up as 'Active, In Use' but Linux Shell cannot be accessed.

  Conditions:Install 1 Day 'Internal_service' license. Let the license expire then install another 1 Day 'Internal_service' license.

  Workaround: Configure and unconfigure the 'platform shell' configuration command to recover the license to proper working state.

  ```
  Router#config terminal
  Router(config)#platform shell
  Router(config)#no platform shell
  Router(config)#platform shell
  ```

  Now the System Linux Shell would be accessible.

- CSCuj02519

  Symptom: Chunk memory leak in Crypto Proxy

  Conditions: This is only seen with IPSEC HA configured

Workaround: None at this time.

- CSCuj31165

  Symptom: crpcipSecGlobalActiveTunnels is incrementing endlessly.

  Conditions: crpcipSecGlobalActiveTunnels OID does not decrements when the current active tunnel is removed.

  Workaround: no work around.

- CSCuj71234

  Symptom: Tracebacks with the following signature "%QFPOOR-4-LOWRSRC_PERCENT" are seen on the console with negative percentage complaining of resource depletion.

  Conditions: These tracebacks are usually seen on a clean-up operation performed on a router i.e manual removal of all configurations. But it's not limited to only this operation and could be seen with router configuration as well.

  Workaround: None.

  Further Problem Description: Error messages with “-ve” percentage values of resource depletion are incorrectly being printed on the console. It's safe to ignore them as the router is not under any duress. Moreover these traces don't cause any operational impact. It should be noted however that if such tracebacks are reported with “+ve” percentage values of resource depletion, then it's an altogether different issue. In such a case, the system may be under duress and inspection of the router configurations and it's operational state is required.

- CSCuj84219

  Symptom: Error messages shown on KS after SW upgrade to 15.2(4)M. Whenever a GM with multiple GDOI groups registers, an error message is logged on the respective KS: Oct 4 11:31:28.477 CEST: %CRYPTO-6-IKMP_NO_ID_CERT_FQDN_MATCH: ID of ce-de-xxxxx.wan.domain.net (type 2) and certificate fqdn with ce-de-xxxxx

  Conditions: Multiple GDOI groups with different GETVPN local-addresses configured on GM. GM/KS are ISR G2 routers running on 15.2(4)M code.

  Workaround: Configure “crypto isakmp identity dn”, i.e. set the ISAKMP identity to the distinguished name (DN) of the router certificate.
  http://www.cisco.com/c/en/US/docs/ios/security/command/reference/sec_c4.html#wp1060149

- CSCul20010

  Symptom: The user will see the system shaping to too low a rate when a tunnel moves to a faster interface, and shaping to too high a rate when a tunnel moves to a slower interface.

  Conditions: Upon a dynamic move of a tunnel to a link with a different speed and the QoS configuration option “shape average percent” has been applied, then rates are not automatically re-calculated.

  Workaround: The workaround to this issue is to avoid “shape average percent” when possible. If not possible, then after a tunnel moves occurs modify the shaping percent by plus or minus 1 percent, and then restore to original value because this forces recalculation of the shaping rate.

- CSCul02627

  Symptom: UEA: Log files are not generated with PTP configurations

  Conditions: Configure RSP2 as the slave and RSP1 as the master Go to shell using “request platform software system shell” cd /tmp/rp/trace ls -ltr Notice that the log files related to PTP aren't present.

  Workaround: Reload of RSP2

- CSCul04434

  Symptom: Given a GETVPN GM that is configured with an ipv6 crypto map, if that crypto map is applied to two interfaces (one common identity, e.g. loopback) and if certain configuration operations are performed, the GM will loose connectivity to the ipv6 group. If the GM has dual-stack interfaces with both an ipv4 and an ipv6 crypto map. The IPv4 GETVPN functionality will not be affected while triggering the event documented in this defect.

  Conditions: Performing configuration operations that follow the patterns described below : 0. IPv6 Crypto Map applied to two interface (E0/0 and E2/0, lets call them Primary and Secondary) At this stage all works well IPv6 traffic is encrypted between two test GMs.

  1. Shut down Secondary interface (E2/0) Result, no change in functionality GM can still exchange encrypted IPv6 traffic with peers.

  2. Remove the ipv6 crypto map from the Primary interface (E0/0, while E2/0 is in admin shutdown state). Result, IPv6 traffic is sent out in clear text

  3. Re-apply crypto map to the Primary interface (i.e. E0/0) Result, no change, packets are still being sent out in clear text, even though GDOI sees the E0/0 interface as associated with the cry map and group.

  4. Remove the crypto map from the Secondary interface which is still in shutdown state Result : No change in the behavior

  5. Remove and re-apply the crypto map on the Primary interface Result : GM re-registers

  Workaround: Remove the ipv6 crypto map from the Secondary Interface before shutting it down.

- CSCul15647

  Symptom: Classification by ACL in QoS is broken when using it with IPSec tunnel.

  Conditions: -use ACL for classification in policy-map and apply a QoS to physical interface -qos pre-classify is configured under IPSec tunnel

  Workaround: apply a QoS to IPSec tunnel

- CSCul39211

  Symptom: With an IOS router set as an EZVPN client, with either interactive (CLI) or HTTP-Intercept authentication enabled, if the user does not enter in proper credentials within 10 seconds, the router will resend AM3 to the EzVPN server. This causes a retransmission storm to trigger and quickly tear down the tunnel, which causes the authentication to fail.

  Conditions: IOS router acting as EzVPN client

  Workaround: 1) Have users enter credentials within 10 seconds of login prompt. 2) Save credentials on router so users don't need to enter them every time. 3) Downgrade to 15.1(4)M5 or earlier

- CSCul95089

  Symptom: AAA sessions are lingering for old connections.

  Conditions: Running Flex VPN server with accounting, clients are identified by email id

  Workaround: none

  Further Problem Description: Accounting sessions are not cleared when a client does reconnect from a different IP upon reception and parsing of the IKEv2 Initial Contact payload

- CSCum14041

  Symptom: QFP error logs not displayed on IOS console.

  Conditions: IOS-XE 3.10/15.3(3)S and forward releases.

  Workaround: None.

Resolved Caveats—Cisco IOS XE Release 3.10.1S

- CSCuh07934

  Symptom: No error-message for reason with restapi GET interface failure.

  Conditions: Restapi GET interface on CSR 1000v interface which has ipv6 address configured.

  Workaround: None

- CSCuc41531

  Symptoms: Forwarding loop is observed for some PfR-controlled traffic. Conditions: This symptom is observed with the following conditions: - Traffic Classes (TCs) are controlled via PBR. - The parent route is withdrawn on selected BR/exit.

  Workaround: This issue does not affect configured or statically defined applications, but only affects learned applications so this can be used as one workaround. Another option is to issue shut/no shut on PfR master or clear the related TCs with the **clear pfr master traffic-class** command (this fixes the issue until the next occurrence).

- CSCud49546

  Symptom: RP crashes with punted fragment-bit set multicast packet.

  Conditions: Fragment bit is set in the multicast packet

  Workaround: None

- CSCue89779

  Symptom: A FlexVPN spoke configured with an inside VRF and front-door VRF may have problems with spoke-to-spoke tunnels if they are not the same. During tunnel negotiation, two Virtual-access interfaces are created (while only one is needed), the one in excess may fail to cleanup correctly. As a result, the routes created by NHRP process may lead to loss of traffic, or traffic may continue to flow through the Hub.

  Conditions: This symptom occurs when the VRF used on the overlay (IVRF) and the VRF used on the transport (FVRF) are not the same.

  Workaround: There is no workaround.

- CSCuf56842

  Symptom: A reload may occur while using **show oer** and **show pfr** commands via SSH.

  Conditions: This symptom is observed when the show pfr master application detail command is used via SSH.

  Workaround: There is no workaround.

- CSCug69107

  Symptom: Crypto session does not comes up in EZVPN.

  Conditions: This symptom is observed when a Crypto session is being established.

  Workaround: There is no workaround.

- CSCug99771

  Symptom: OSPF N2 default route missing from Spoke upon reloading Hub. Hub has a static default route configured and sends that route over DMVPN tunnel running OSPF to spoke. When hub is reloaded, the default route is missing on Spoke. NSSA-External LSA is there on Spoke after reload, but the routing bit is not set. Hence, it is not installed in RIB on Spoke.

  Conditions: Default originated using command **area X nssa default-information-originate**.

Workaround: Removing & re adding **area X nssa default-information-originate** on Hub resolves the issue.

- CSCuh32177

  Symptom: The **no passive-interface** command will be added automatically after configuring the **ipv6 enable** command on the interface even though the **passive-interface default** command is configured for OSPFv3.

```
(config)#interface FastEthernet0/2/0
(config-if)#ipv6 enable (
config-if)#end #sh run | sec ipv6 router ospf ipv6 router ospf 100 router-id 10.1.1.1
passive-interface default no passive-interface FastEthernet0/2/0 <<< Added
automatically. ---
```

  Conditions: This symptom occurs when the **passive-interface default** command is configured for OSPFv3.

  Workaround: Adjust the configuration manually. In this example it would be **passive-interface FastEthernet0/2/0**.

- CSCuh43027

  Symptom: Prefixes withdrawn from BGP are not removed from the RIB, although they are removed from the BGP table.

  Conditions: A withdraw message contains more than one NLRI, one of which is for a route that is not chosen as best. If deterministic med is enabled, then the other NLRI in the withdraw message might not eventually be removed from the RIB.

  Workaround: Forcibly clear the RIB.

  Further Problem Description: This issue may also occur if BGP PIC is enabled and the withdraw message contains a route that is currently serving as a backup path.

- CSCuh94035

  Symptom: A watchdog timeout crash occurs.

  Conditions: This symptom occurs when DMVPN and IPv4/IPv6 EIGRP are configured. A crash occurs while DUAL is updating the EIGRP topology table.

  Workaround: There is no workaround.

- CSCuh97129

  Symptom: Losing EIGRP Extended communities on BGP L3VPN route.

  Conditions: This symptom is observed when Remote PE-CE connection is brought down and only backup EIGRP path remains in the BGP table.

  Workaround: Clearing the problem route in the VRF will resolve the issue.

- CSCui07997

  Symptom: Route over OSPFv2 sham-link shows two next hop.

  Conditions: This symptom is observed when the route entry is ECMP route between the sham-link and another path.

  Workaround: Break ECMP by adjusting the OSPF cost.

- CSCui29499

  Symptom: ISIS going into INIT state.

Conditions: BFD flap leads to ISIS adjacency not coming up if the following conditions are true: 1.) In P2P mode only 2.) when local node supports RFC6213 and its remote neighbor does not support RFC6213 3.) The P2P link is down and adjacency is deleted on the remote neighbor and up again before the adjacency hold down timer expires on the local node that has the RFC6213 support.

Workaround: Any of the following work around will work. - Remove BFD on 903, wait for ISIS to come up and configure BFD again - Shut and no shut the interface on the local node with RFC6213 Or - Not to use P2P link at all

- CSCui89069

  Symptom: ISIS Flap on performing SSO.

  Conditions: with **nsf ietf** configured and one or more loopbacks configured as passive interfaces

  Workaround: Two workarounds are available: 1)use **nsf cisco** or 2) Continue to use **nsf ietf** but configure **ip router isis** *process_name* on the loopback interfaces.

Resolved Caveats—Cisco IOS XE Release 3.10.0S

- CSCud23158

  Symptom: On the Cisco CSR1000v an unexpected reset may occur when sending IPv4 small packet traffic at a high rate.

  Conditions: This is intermittently seen with a basic CEF configuration passing bi-directional 64 Byte traffic near 100% Gigabit Ethernet line-rate.

  Workaround: None

- CSCud71606

  Symptom: The LSMPI Tracebacks errors are seen while clearing IP routes multiple times.

  Conditions: This symptom is observed under the following conditions:

  - Configuring OSPF.
  - Has more than 1000 OSPF neighbors, which will make OSPF LSU packet get fragmented.
  - Clear ip ospf process * and OSPF will send an LSU packet, which triggers this error message.

  Workaround: None.

- CSCue39542

  Symptom: Tunnel interface states down and fail to carry traffic.

  Conditions: The tunnel interface stays down after the tunnel stay flaps. Can be from issuing “shut” and “no shut” commands manually, or the physical port state flaps. And the tunnel state might stay down forever after the event.

  Workaround: Delete and recreate the tunnel interface with the same config will bring this tunnel back to up state.

- CSCue41031

  Symptom: Extra flow is shown in **show crypto session** command.

  Conditions: None.

  Workaround: None.

- CSCue95542

  Symptom: A crash was observed after configuring ethernet CFM on the router. The crash occurred in the linux_iosd process.

Conditions: The crash was seen on the Cisco ISR4400 and the Cisco CSR1000v.

Workaround: Do not configure CFM.

- CSCuf09252

  Symptom: Incorrect error message is seen when giving no parameter-map type inspect-global.

  Conditions: Parameter-map type inspect global should be defined.

  Workaround: None.

- CSCuh20338

  Symptom: ucode crash @ ipv4_ipsec_tunnel_input

  Conditions: Bringup 10 FlexVPN sessions on Cisco CSR 100V.Workaround: Enter the **no ip source-route** command.

- CSCuh70383

  Symptom: The Cisco CSR 1000v is deployed from the OVF template, powered up until completion of the 1st time boot process, then powered down and a new vNIC is added while the router is offline. After the router is powered up again, the new interfaces are recognized but the Cisco CSR 1000v VM is observed at operating with 100% CPU usage. The router stays at 100% CPU as long as the newly added interface is in admin shutdown state. CSR CPU usage revert to normal once the interface is admin 'no shutdown'. Not all interface additions will result in this condition.

  Conditions: When adding a new vNIC to the Cisco CSR 1000v.

  Workaround: After the new interface is added, administer the **no shutdown** to the interface.

Open Caveats—Cisco IOS XE Release 3.10.0S

- CSCue33225

  Symptom: The **sh plat hard qfp act dat infr sw-hqf** output is truncated.

  Conditions: When 5 Gi interfaces are defined, the output is truncated

  Workaround: Use less than 5 Gi interfaces.

- CSCue75176

  Symptom: IDFW is not working for sgt replaced because of policy static sgt <sgt-num> command.

  Conditions: Configure policy static sgt <sgt-num> command on ingress interface and in FW do match for same sgt number given in this CLI.

  Workaround: None.

- CSCuf28574

  Symptom: Cisco CSR1000v running on XEN will see significantly lower throughput than on other hypervisors, i.e. ESXi.

  Conditions: Cisco CSR1000v running on XEN Server 6.02

  Workaround: None.

- CSCug13606

  Symptom: Gigabit Ethernet interface counters show a value near 2 to the 64th.

  Conditions: Occurs on a Cisco CSR1000v router using VMXNET3 driver after an Etherchannel interface is configured.

  Workaround: Performing “clear counters” will reset the counter to zero.

- CSCug51917

  Symptom: Hot removal of an interface not possible in the case of CSR 1000v [installed on an ESXi server].

  Conditions: Issue seen when try to remove an interface from the Cisco CSR 1000v router when it is UP.

  Workaround: None.

- CSCuh12291

  Symptom: RESTAPI interface discovery will fail.

  Conditions: Having ipv6 address configured on interface and do RESTAPI GET interface.

  Workaround: None

- CSCuh28560

  Symptom: After booting up, two VMs came up with no installed licenses. Could not recover the licenses since the UDI of the VMs changed.

  Conditions: Reset all Cisco CSR 1000v VMs running on a server (4:1 CPU oversubscription). All VMs are 4 vCPU with 4 GB RAM and 3 NICs each.

  Workaround: Do not oversubscribe.

- CSCuh49807

  Symptom: IPsec transform set with esp-md5-hmac is not supported in this release. When esp-md5-hmac is used, though the IPsec tunnel is established, traffic can not pass through the tunnel. Inbound traffic will be dropped with HMAC error. Outbound traffic will reach to the peer, but will be dropped by the peer with HMAC error.

  The following error message is displayed:

  ```
  %IOSXE-3-PLATFORM: F0: cpp_cp: QFP:0.0 Thread:000 TS:00000002356612773534
  %IPSEC-3-HMAC_ERROR: IPSec SA receives HMAC error, DP Handle 5, src_addr 60.0.0.2,
  dest_addr 60.0.0.1, SPI 0xb98e9ee1
  ```

  Conditions: Whenever esp-md5-hmac is used in an IPsec transform set.

  Workaround: Use esp-sha-hmac, not esp-md5-hmac.

- CSCuh73332

  Symptom: Can show "Last reload reason: <NULL>"

  Conditions: CPP crash on CSR

  Workaround: None

- CSCui12606

  Symptom: If Gi1 interface does not exist on the CSR when the CSR boots up, the following error message is logged:

  ```
  *Jul 16 14:57:17.598: %IOSXE-4-PLATFORM: R0/0: kernel: TIPC: Bearer <eth:Gi1>
  rejected, enable failure (19)
  *Jul 16 14:57:18.722: %PMAN-3-PROCHOLDDOWN: F0: pman.sh:  The process
  wui-tipc-launch.sh has been helddown (rc 255)
  ```

  The Gi1 interface (usually vnic2 of the CSR VM) could disappear from CSR for any one of the following reasons:

  1) the vNIC is deleted from vSphere then the CSR is rebooted

  2) the MAC address of the vNIC is changed from vSphere

Conditions: Gi1 interface does not exist on the CSR.

Workaround: If the CSR has multiple vNICs, use the 'clear platform software vnic-if nvtable' command to remap the vNICs to interfaces mapping, then reboot the CSR. Note that the command might remap the interfaces not in the order shown on vSphere for the CSR VM. Use with care.

- CSCui41279

  Symptom: When the CSR1000v boots in premium mode, cannot configure throughput level or install a new premium throughput level license. Throughput will be set to 2500 kbps.

  Conditions: CSR boot in premium mode with premium license.

  Workaround: Reload the router.

Caveats—Cisco IOS XE Release 3.9S

Resolved Caveats—Cisco IOS XE Release 3.9.2S

None.

Resolved Caveats—Cisco IOS XE Release 3.9.1S

- CSCuc11849

  Symptom: Packets of smaller lengths (less than 100 bytes) may be dropped occasionally when a shaper is configured.

  Conditions: This issue happens when a shaper is configured on CSR1000v and traffic consisting of smaller packet lengths (less than 100 bytes) are sent below the configured shape rate.

  Workaround: There is no known workaround.

- CSCue04941

  Symptom: When CSR1000v is being used as a VPN gateway and BFD session, the number of stable BFD sessions is lower than expected.

  Conditions: When CSR1000v is being used as a VPN gateway and BFD session, the number of stable BFD sessions is lower than expected.

  Workaround: None.

- CSCuf29962

  Symptom: Getting aggressive alert is seen when no alert is set.

  Conditions: ZBFW is on and alert is seen after disabling the parameter-map type inspect global and clearing drops.

  Workaround: None

- CSCuf86458

  Symptom: Crash kernel does not work on ESXi.

Conditions: When main kernel crashes, it does not dump core.

Workaround: None

Open Caveats—Cisco IOS XE Release 3.9.0aS

- CSCuf51492

  Symptom: All of the IPSEC sessions didn't come up after ISAKMP Rekey

  Conditions: Noticed in a scaled DMVPN topology.

  Workaround: None

Resolved Caveats—Cisco IOS XE Release 3.9.0aS

- CSCsr10335

  Symptoms: A router loses its default gateway during autoinstall.

  Conditions: This issue was seen on Cisco IOS Release 12.4(15)T5, but should affect every Cisco IOS version.

  Workaround:

  1. Manually do a **shut** followed by a **no shut** on the interface.

  2. Create an EEM script, for example:

```
event manager applet Check-Default-Route event syslog pattern "CNS-3-TRANSPORT:
CNS_HTTP_CONNECTION_FAILED"

 action 1.0 cli command enable
 action 1.1 cli command config term
 action 1.2 cli command interface GigabitEthernet0/0<
 action 1.3 cli command shut
 action 1.4 cli command no shut
 action 1.5 cli command end
 action 1.6 cli command write ! end
```

  3. In the network configuration, configure **ip address dhcp** for the interface which is supposed to get the default gateway from DHCP.

- CSCuc17133

  Symptom: The CSR router would crash at IPSec code if a DMVPN session is up and running for some time.

  Conditions: Usually happens within an hour. No traffic is needed.

  Workaround: None.

- CSCuc45115

  Symptoms: EIGRP flapping is seen continuously on the hub. A crash is seen at nhrp_add_static_map.

  Conditions: This symptom is observed in the case where there are two Overlay addresses of a different Address Family on the same NBMA (such as IPv4 and IPv6 over Ipv4). This issue is observed after shut/no shut on the tunnel interface, causing a crash at the hub. A related issue is also seen when there is no IPv6 connectivity between the hub and spoke, causing continuous EIGRP flapping on the hub.

  Workaround: There is no known workaround.

- CSCuc99788

  Symptom: ERSPAN traceback

  Conditions: Configured 2k sub-interfaces.

  Workaround: None

- CSCud02391

  Symptoms: The EIGRP routes do not come up after removing and reenabling the tunnel interface.

  Conditions: This symptom is observed when EIGRP routes do not populate properly.

  Workaround: There is no workaround.

- CSCud03863

  Symptom: ESP crashes on CSR

  Conditions: Crash occurs when sending traffic through a non gig 0 interface

  Workaround: No workaround as this is caused by unsupported CPUs with missing features. As per the data sheet (http://www.cisco.com/c/en/US/prod/collateral/routers/ps12558/ps12559/data_sheet_c78-705395.pdf), the CPU requirement is “Intel Nehalem or AMD Barcelona CPU with clock frequency 1.8GHz” or higher.

- CSCud23158

  Symptom: On the CSR1000v an unexpected reset may occur when sending IPv4 small packet traffic at a high rate.

  Conditions: This is intermittently seen with a basic CEF configuration passing bi-directional 64 Byte traffic near 100% Gigabit Ethernet line-rate.

  Workaround: None

- CSCud67970

  Symptom: Provisioned QoS service is not honored.

  Conditions: When fair-queue is removed from the class on-the-fly, the rates, i.e., bandwidth and shape, are no longer configured in the hardware.

  Workaround: Remove the fair-queue class and re-add it without fair-queue.

- CSCud71606

  Symptom: LSMPI Tracebacks/Errors seen while clearing IP routes multiple times.

  Conditions: ASR- GIG-------IXIA >> 2K vlans on GIGE and IXIA subi-intfs >> OSPF neighbour hood was properly achieved with 1000 Vlans

  Workaround: None

- CSCud93920

  Symptom: QFP errors on applying AVC to MPLS interfaces.

  Conditions: AVC is not supported on an MPLS interface so this is a misconfiguration.

  Workaround: Not applicable.

- CSCue36106

  Symptom: This warning message would be emitted on the IOS console on Cisco CSR1000v installed on the VMWARE ESXi with VMXNET3 network adapter.

Conditions: When the Cisco CSR1000v is over-subscribed and ESXi is not be able to handle the traffic.

Workaround: This is a warning message and VMXNET3 driver recovers from this condition.

Make sure that the Cisco CSR1000v is not over-subscribed to avoid this.

- CSCue39542

  Symptom: Tunnel interface stays down and fails to carry traffic.

  Conditions: The tunnel interface stays down after the tunnel stay flaps. Can be from issuing **shut** and **no shut** commands manually, or the physical port state flaps. And the tunnel state might stay down forever after the event.

  Workaround: Deleting and recreating the tunnel interface with the same configuration will bring this tunnel back to up state.

Related Documentation

For information about the Cisco CSR 1000v Series and associated services, see: *Documentation Roadmap for Cisco CSR 1000v Series, Cisco IOS XE 16*.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.