Resolved Caveats in Release 12.2(18)SXE

Resolved Infrastructure Caveats

- CSCee18471—Resolved in 12.2(18)SXE

  Symptom: v1/v2c users and snmp community acl is not synced to standby.

  Workaround: Use communities instead of v1/v2c users. There is no workaround for acl not being synced to standby.

  Condition: The device should support HA/SSO.

Resolved IPServices Caveats

- CSCee50294—Resolved in 12.2(18)SXE

  Cisco IOS devices running branches of Cisco IOS version 12.2S that have Dynamic Host Configuration Protocol (DHCP) server or relay agent enabled, even if not configured, are vulnerable to a denial of service where the input queue becomes blocked when receiving specifically crafted DHCP packets. Cisco is providing free fixed software to address this issue. There are also workarounds to mitigate this vulnerability. This issue was introduced by the fix included in CSCdx46180 and is being tracked by Cisco Bug ID CSCee50294.

  This advisory is available at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20041110-dhcp .

  There are multiple workarounds for this issue: There are four possible workarounds for this vulnerability:

  - Disabling the dhcp service
  - Control Plane Policing
  - Two versions of Access Control Lists

  Disabling the DHCP Service

  This vulnerability can be mitigated by utilizing the command:

  ```
  no service dhcp
  ```

  However, this workaround will disable all DHCP processing on the device, including the DHCP helper functionality that may be necessary in some network configurations.

  Control Plane Policing Feature

  The Control Plane Policy feature may be used to mitigate this vulnerability, as in the following example:

  ```
  access-list 140 deny   udp host 192.168.13.1 any eq bootps
  access-list 140 deny   udp any host 192.168.13.1 eq bootps
  access-list 140 deny   udp any host 255.255.255.255 eq bootps
  access-list 140 permit udp any any eq bootps

  class-map match-all bootps-class
    match access-group 140

  policy-map control-plane-policy
    class bootps-class

       police 8000 1500 1500 conform-action drop exceed-action drop

  control-plane
   service-policy input control-plane-policy
  ```

For this example 192.168.13.1 is a legitimate DHCP server.

Additional information on the configuration and use of the CPP feature can be found at this link:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_paper0900aecd804fa16a.html .

This workaround is only applicable to Cisco IOS 12.2S, as this feature is only available in Cisco IOS versions 12.2S and 12.3T. Cisco IOS 12.3T is not impacted by this advisory.

Access Lists - Two Methods

Access lists can be applied to block DHCP/BootP traffic destined to any router interface addresses, as in the following example:

In this example, the IP address192.168.13.1 represents a legitimate DHCP server, the addresses 10.89.236.147 and 192.168.13.2 represent router interface addresses, and 192.168.61.1 represents a loopback interface on the router.

In this example, any bootp/dhcp packets destined to the router interface addresses are blocked.

```
access-list 140 deny   udp host 192.168.13.1 any eq bootps
access-list 140 deny   udp any host 192.168.13.1 eq bootps
access-list 140 deny   udp any host 255.255.255.255 eq bootps
access-list 140 permit udp any any eq bootps

class-map match-all bootps-class
  match access-group 140

policy-map control-plane-policy
  class bootps-class

     police 8000 1500 1500 conform-action drop exceed-action drop

control-plane
 service-policy input control-plane-policy
```

For this example 192.168.13.1 is a legitimate DHCP server.

Additional information on the configuration and use of the CPP feature can be found at this link:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_paper0900aecd804fa16a.html .

This workaround is only applicable to Cisco IOS 12.2S, as this feature is only available in Cisco IOS versions 12.2S and 12.3T. Cisco IOS 12.3T is not impacted by this advisory.

Access Lists - Two Methods

Access lists can be applied to block DHCP/BootP traffic destined to any router interface addresses, as in the following example:

In this example, the IP address192.168.13.1 represents a legitimate DHCP server, the addresses 10.89.236.147 and 192.168.13.2 represent router interface addresses, and 192.168.61.1 represents a loopback interface on the router.

In this example, any bootp/dhcp packets destined to the router interface addresses are blocked.

```
access-list 100 remark permit bootps from the DHCP server
access-list 100 permit udp host 192.168.13.1 any eq bootps
access-list 100 remark deny bootps from any to router f1/0
access-list 100 deny   udp any host 10.89.236.147 eq bootps
access-list 100 remark deny bootps from any to router f0/0
access-list 100 deny   udp any host 192.168.13.2 eq bootps
access-list 100 remark deny bootps from any to router loopback1
```

```
access-list 100 deny   udp any host 192.168.61.1 eq bootps
access-list 100 remark permit all other traffic
access-list 100 permit ip any any

access-list 100 is applied to f0/0 and f1/0 physical interfaces.

interface FastEthernet0/0
 ip address 192.168.13.2 255.255.255.0
 ip access-group 100 in
interface FastEthernet1/0
 ip address 10.89.236.147 255.255.255.240
 ip access-group 100 in
 ip helper-address 192.168.13.1
```

An alternate configuration for the interface access-list workaround.

This example would also need to be applied to all physical interfaces, but deny statements for all of the IP addresses configured on the router are not necessary in this approach. In this example, the address 192.168.13.1 represents a legitimate DHCP server.

```
access-list 100 permit udp host 192.168.13.1 any eq bootps
access-list 100 permit udp any host 192.168.13.1 eq bootps
access-list 100 permit udp any host 255.255.255.255 eq bootps
access-list 100 deny   udp any any eq bootps

interface FastEthernet0/0
 ip address 192.168.13.2 255.255.255.0
 ip access-group 100 in
interface FastEthernet1/0
 ip address 10.89.236.147 255.255.255.240
 ip access-group 100 in
 ip helper-address 192.168.13.1
```

- CSCef84255—Resolved in 12.2(18)SXE

  Description: An IOS router that is NOT configured for MSDP and connected to a peer router that is configured for MSDP may see packets remaining in the input queue.

  Symptoms: The interface input queue of a router may fill with packets, denying further traffic from being received on that interface.

  Workarounds: MSDP traffic can be filtered from the offending peer, or appropriately configure MSDP on the affected device.

- CSCed78149—Resolved in 12.2(18)SXE

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP “hard” error messages
  2. Attacks that use ICMP “fragmentation needed and Dont' Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP “source quench” messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20050412-icmp.html

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected.

Resolved LAN Caveats

- CSCsa67294—Resolved in 12.2(18)SXE

  Symptom: A Cisco Catalyst Switch may reload upon receipt of a malformed VTP packet.

  Conditions: The malformed VTP packet must meet the following requirements:

  - Must be received on a port configured for ISL or 802.1q trunking AND
  - Must correctly match the VTP domain name

  This does not affect switch ports configured for the voice vlan.

  Affected platforms:

  - Cisco 2900XL Series
  - Cisco 2900XL LRE Series
  - Cisco 2940 Series
  - Cisco 2950 Series
  - Cisco 2950-LRE Series
  - Cisco 2955 Series
  - Cisco 3500XL Series
  - Cisco IGESM

  No other Cisco devices are known to be vulnerable to this issue.

  Workarounds: Customers may want to connect ports configured for trunking to known, trusted devices.

Resolved Management Caveats

- CSCdz54403—Resolved in 12.2(18)SXE

  Symptoms: A Cisco router may crash when IPSec IKE SNMP variables are retrieved, and a bus error and a traceback may be logged.

  Conditions: This symptom is observed when at least one SA is established. The symptom does not always occur, but when you retrieve the IPSec IKE SNMP variables once every 10 minutes, the router eventually crashes after a few hours.

  Workaround: The workaround is to block access to the CISCO-IPSEC-FLOW-MONITOR-MIB - [or just the cikeTunnelTable] using SNMP views so that no one walks this MIB and cause this crash.

- CSCed11835—Resolved in 12.2(18)SXE

  Symptoms: A Cisco 7200 VXR router that terminates a large number of IPSec tunnels may restart unexpectedly.

  Conditions: This symptom is observed when IKE MIB variables are being polled on the router.

  Workaround: Avoid polling of IKE MIB variables.

Resolved MPLS Caveats

- CSCsa52940—Resolved in 12.2(18)SXE

  Symptoms: A Cisco HE router running MPLS traffic engineering may crash with a memory corruption footprint or with a bus error. If the P and PE routers are running a release prior to 12.0(26)S or 12.2S Cascades, then all of the downstream midpoint routers may crash with similar symptoms.

  Conditions: More than 10 LSPs for a single MPLS-TE session must be signalled in a specific way, which is not supported nor used by Cisco IOS.

  Multiple LSPs for a single session will only happen when the router is under great stress because of many tunnels or breakage somewhere else in the network.

  Note that this is not a problem when MPLS-TE tunnels are signalled with verbatim LSPs, because Cisco routers signal verbatim LSPs do not use this type of signalling.

  Workaround: None

Resolved Routing Caveats

- CSCee67450—Resolved in 12.2(18)SXE

  A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DoS) attack from a malformed BGP packet. Only devices with the command bgp log-neighbor-changes configured are vulnerable. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet.

  Cisco has made free software available to address this problem.

  This issue is tracked by CERT/CC VU#689326.

  This advisory will be posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20050126-bgp.html

- CSCef48336—Resolved in 12.2(18)SXE

  OSPF is a routing protocol defined by RFC 2328. It is designed to manage IP routing inside an Autonomous System (AS). OSPF packets use IP protocol number 89.

  A vulnerability exists in the processing of an OSPF packet that can be exploited to cause the reload of a system.

  Since OSPF needs to process unicast packets as well as multicast packets, this vulnerability can be exploited remotely. It is also possible for an attacker to target multiple systems on the local segment at a time.

  Using OSPF Authentication can be used to mitigate the effects of this vulnerability. Using OSPF Authentication is a highly recommended security best practice.

  A Cisco device receiving a malformed OSPF packet will reset and may take several minutes to become fully functional. This vulnerability may be exploited repeatedly resulting in an extended DOS attack.

  Workarounds:

  - Using OSPF Authentication

    OSPF authentication may be used as a workaround. OSPF packets without a valid key will not be processed. MD5 authentication is highly recommended, due to inherent weaknesses in plain text authentication. With plain text authentication, the authentication key will be sent unencrypted over the network, which can allow an attacker on a local network segment to capture the key by sniffing packets.

Refer to http://www.cisco.com/en/US/tech/tk365/technologies_configuration_example09186a0080094069.shtml for more information about OSPF authentication.

- Infrastructure Access Control Lists

  Although it is often difficult to block traffic transiting your network, it is possible to identify traffic which should never be allowed to target your infrastructure devices and block that traffic at the border of your network. Infrastructure ACLs are considered a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for this specific vulnerability. The white paper "Protecting Your Core: Infrastructure Protection Access Control Lists" presents guidelines and recommended deployment techniques for infrastructure protection ACLs:

  http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml

- CSCef68324—Resolved in 12.2(18)SXE

  Cisco Internetwork Operating System (IOS) Software is vulnerable to a Denial of Service (DoS) and potentially an arbitrary code execution attack from a specifically crafted IPv6 packet. The packet must be sent from a local network segment. Only devices that have been explicitly configured to process IPv6 traffic are affected. Upon successful exploitation, the device may reload or be open to further exploitation.

  Cisco has made free software available to address this vulnerability for all affected customers.

  More details can be found in the security advisory that is posted at:

  http://www.cisco.com/en/US/products/csa/cisco-sa-20050729-ipv6.html

- CSCef61610—Resolved in 12.2(18)SXE

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages
  2. Attacks that use ICMP "fragmentation needed and Dont' Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP "source quench" messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20050412-icmp.html.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected.

- CSCeb88239—Resolved in 12.2(18)SXE

  Symptoms: A router that runs RIPng may crash after receiving a malformed RIPng packet, causing a Denial of Service (DoS) on the device.

  Conditions: This symptom is observed when the **ipv6 debug rip** command is enabled on the router. Malformed packets can normally be sent locally. However, when the **ipv6 debug rip** command is enabled, the crash can also be triggered remotely. Note that RIP for IPv4 is not affected by this vulnerability.

  Workaround: There is no workaround.

- CSCec85929—Resolved in 12.2(18)SXE

  Sympotom: Router may reload when users issue **show running-config**.

  Conditions: If users configures ISIS with tag name longer than 42 characters, router may reload when users issue **show running-config**

  Workaround: Use ISIS tag name short than 42 characters.

- CSCef60659—Resolved in 12.2(18)SXE

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP “hard” error messages
  2. Attacks that use ICMP “fragmentation needed and Dont' Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP “source quench” messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20050412-icmp.html.

- CSCec71950—Resolved in 12.2(18)SXE

  Cisco routers and switches running Cisco IOS or Cisco IOS XR software may be vulnerable to a remotely exploitable crafted IP option Denial of Service (DoS) attack. Exploitation of the vulnerability may potentially allow for arbitrary code execution. The vulnerability may be exploited after processing an Internet Control Message Protocol (ICMP) packet, Protocol Independent Multicast version 2 (PIMv2) packet, Pragmatic General Multicast (PGM) packet, or URL Rendezvous Directory (URD) packet containing a specific crafted IP option in the packet’s IP header. No other IP protocols are affected by this issue.

  Cisco has made free software available to address this vulnerability for affected customers.

  There are workarounds available to mitigate the effects of the vulnerability.

This vulnerability was discovered during internal testing.

This advisory is available at:

http://www.cisco.com/en/US/products/csa/cisco-sa-20070124-crafted-ip-option.html

- CSCef67682—Resolved in 12.2(18)SXE

  Reception of certain IPv6 fragments with carefully crafted illegal contents may cause a router running Cisco IOS to reload if it has IPv6 configured. This applies to all versions of Cisco IOS that include support for IPv6.

  The system may be protected by installing appropriate access lists to filter all IPv6 fragments destined for the system. For example:

```
interface Ethernet0/0
  ipv6 traffic-filter nofragments in
!
ipv6 access-list nofragments
  deny ipv6 any <my address1> undetermined-transport
  deny ipv6 any <my address2> fragments
  permit ipv6 any any
```

  This must be applied across all interfaces, and must be applied to all IPv6 addresses which the system recognises as its own.

  This will effectively disable reassembly of all IPv6 fragments. Some networks may rely on IPv6 fragmentation, so careful consideration should be given before applying this workaround.

  We would recommend for customers to upgrade to the fixed IOS release. All IOS releases listed in IPv6 Routing Header Vulnerability Advisory at http://www.cisco.com/en/US/products/csa/cisco-sa-20070124-IOS-IPv6.html contain fixes for this issue.

Resolved Security Caveats

- CSCed65285—Resolved in 12.2(18)SXE

  Certain release trains of Cisco Internetwork Operating System (IOS), when configured to use the IOS Secure Shell (SSH) server in combination with Terminal Access Controller Access Control System Plus (TACACS+) as a means to perform remote management tasks on IOS devices, may contain two vulnerabilities that can potentially cause IOS devices to exhaust resources and reload. Repeated exploitation of these vulnerabilities can result in a Denial of Service (DoS) condition. Use of SSH with Remote Authentication Dial In User Service (RADIUS) is not affected by these vulnerabilities.

  Cisco has made free software available to address these vulnerabilities for all affected customers. There are workarounds available to mitigate the effects of the vulnerability (see the “Workarounds” section of the full advisory for details.)

  This advisory will be posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20050406-ssh.html

Resolved Unknown Caveats

- CSCee59999—Resolved in 12.2(18)SXE

  Symptoms: When auto-reconnect is configured on an EzVPN server and an EzVPN client attempts to connect, failures may occur in AAA accounting.

  The output of the **debug crypto isakmp aaa** command on the EzVPN server shows an error message such as the following:

```
ISAKMP AAA: Unable to send AAA Accounting Start %CRYPTO-4-IPSEC_AAA_START_FAILURE:
IPSEC Accounting was unable to send start record
```

Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.3 or Release 12.3(8)T or a later release and that functions as an EzVPN server.

Workaround: There is no workaround.

- CSCef90002—Resolved in 12.2(18)SXE

  Cisco Catalyst 6500 series systems that are running certain versions of Cisco Internetwork Operating System (IOS) are vulnerable to an attack from a Multi Protocol Label Switching (MPLS) packet. Only the systems that are running in Hybrid Mode (Catalyst OS (CatOS) software on the Supervisor Engine and IOS Software on the Multilayer Switch Feature Card (MSFC)) or running with Cisco IOS Software Modularity are affected.

  MPLS packets can only be sent from the local network segment.

  A Cisco Security Advisory for this vulnerability is posted at

  http://www.cisco.com/en/US/products/csa/cisco-sa-20070228-mpls.html

- CSCeg11009—Resolved in 12.2(18)SXE

  Symptoms: Platforms that support IPC may show IPC-2-INVALIDZONE error message:

  Conditions: This condition is not performance impacting

  Workaround: There is no workaround for this issue.

- CSCin82407—Resolved in 12.2(18)SXE

  Cisco Internetwork Operating System (IOS) Software release trains 12.2T, 12.3 and 12.3T may contain vulnerabilities in processing certain Internet Key Exchange (IKE) Xauth messages when configured to be an Easy VPN Server.

  Successful exploitation of these vulnerabilities may permit an unauthorized user to complete authentication and potentially access network resources.

  This advisory will be posted to
  http://www.cisco.com/en/US/products/csa/cisco-sa-20050406-xauth.html

- CSCsa54996—Resolved in 12.2(18)SXE

  Symptom: XAUTH may be bypassed if NAT is present between the client and concentrator

  Conditions: Concentrator and client are negotiating a VPN session with XAUTH.

  Workarounds: None.

- CSCsa67611—Resolved in 12.2(18)SXE

  For packets incoming MPLS Tagged and going out as untagged IP (tag to IP case) if output features (like egress ACL, egress WCCP) are applied upon a reload of a switch one may find that the egress features no longer get applied.

  This has been seen with 12.2(17b)SXB6 and 12.2(18d)SXD2.

  Packet impacted Concern : Incoming packet hitting the 6500 with sup720 with one label and exiting the switch on a non mpls int (tag to ip path) on which some output feature are configured (like output acl , output wccp or...)

  Impact : these packet should always be recirculated as there are some output feature. After a reload of the switch recirculation do not happen anymore and as a result all packet bypass the ACL or any output feature.

  Workaround: disable and reapply all output features on the output interface and output feature will start to work again.

- CSCef44225—Resolved in 12.2(18)SXE

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages
  2. Attacks that use ICMP "fragmentation needed and Dont' Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP "source quench" messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20050412-icmp.html.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected.

Other Resolved Caveats in Release 12.2(18)SXE

Identifier	Technology	Description
CSCed05135	AAA	12.2S:Enable encryped kerberos telnet cause switches crash
CSCed88768	AAA	console/vty/telnet password fails after upgrade to 12.2(18)S images
CSCeg06605	AAA	Radius Accounting record send with source port zero
CSCeg16606	AAA	Calling-station-ID twice in access-request with dot.1x authenticatio
CSCsa41535	AAA	show aaa servers, response time counter shows incorrect value
CSCsa74002	AAA	Input queue - wedged when traffic punted to the CPU
CSCed25363	Access	PA-MCT3 will not come online after being down with no cable attached
CSCed90084	Access	No SNMP trap Generated for Up/Down(looped) situation on 7500 Router
CSCee49862	Access	PA-MC-2T3+ does not adhere to ANSI T1.231 standard
CSCee70591	Access	PA-2T3+ does not adhere to the ANSI T1.231 standard
CSCee82681	Access	Counter: Counters stuck on serial interface
CSCef73120	Access	Pikespeak:Fw2 with E3 Serial PA:Interface BW does not get modified
CSCef85293	Access	E1 ports of a PA-MC-8TE1+ are up without any cable attached
CSCeg55131	Access	Spurious access @mip_unchain_idb while configuring t1 controller
CSCeg67788	Access	Interface counters incorrect with PA-MC-8ET1+
CSCeh16887	Access	FW2+PA-MC-2T3: RP crash without coredump after channel-group removed

Identifier	Technology	Description
CSCin60835	Access	Show controller serial not showing all 15 min intervals
CSCin76828	Access	Multi-channel T1 PA's in FlexWAN module fail boot-up diagnostics
CSCin79495	Access	FW2-HYB:%CWAN_RP-4-SEMAHOG observed with 256 channels on PA-MC-8TE1+
CSCin79544	Access	Large values of tx_polling_high cause high latency on ct3/ce3 PAs
CSCin88303	Access	Unchannelised mode of PA-MC-2t3+ Not working, Interfaces up/down
CSCsa46643	Access	input/output counters stop incrementing on serial interface counter
CSCdx79081	ATM	ATM vc bundle member adjacencies not getting deleted
CSCdy07583	ATM	scaling: loops in atm_pvc_range_command contribute to line card flap
CSCeb01205	ATM	LSNT:CPUHOG with Switch1 logged after clear interface sw1
CSCeb06797	ATM	error message %ATMPA-3-BADVCD after deleting & re-adding pvc
CSCec31381	ATM	Need message on OSM that UBR+ is unsupported.
CSCec51408	ATM	VBR-NRT Under PVC missing after reload router
CSCec80784	ATM	Memory leak in ATMSIG Input (atmSmap_enter_vcnum_in_map)
CSCed00033	ATM	oam-pvc manage 0 is broken after AIS
CSCed21813	ATM	SAR1 crash when VC QoS parameters are modified
CSCee04747	ATM	memory leak when removing ATM VCs
CSCee42236	ATM	Atm Static mapping not show up in configuration using in PVC bundle
CSCef10826	ATM	CAR broken on IMA with DCEF enabled
CSCef55463	ATM	VBR-NRT shaping not accurate under load
CSCef83201	ATM	ATM OAM F5 segment RDI not transmitted out ATM interface
CSCeg03153	ATM	ifAdminStatus does not follow cli for ATM sub-interface
CSCeg19298	ATM	Router crashes while sh run is issued after atm pvc bundle config
CSCeg83467	ATM	Router crash at atm_arp_process
CSCin31767	ATM	crash on show atm map after deleting subint with static map bundle
CSCin32888	ATM	Crash on removing bundle-member with ipx inarp config
CSCin41371	ATM	dLFIoATM : VIP crash on interface flap
CSCin65182	ATM	OAM PVC on IMA interface doesnt come up after OIR
CSCin77553	ATM	ATM-IMA stops passing traffic after some time, rx_no_buffers seen
CSCin79468	ATM	ATM SSO: PVC state not in sync between active/sdby after a sh/no-sh
CSCin84694	ATM	Workaround fix for PA-A3/A6 SAR hardware issue
CSCin86002	ATM	Quick shut/no-shut on member link reduces bandwidth of IMA-grp intf
CSCin86455	ATM	PA-A3/A6: Performance optimization and code cleanup
CSCea31640	Content	WCCP packet return handling - webpage is partially downloaded & hang
CSCeb28941	Content	IOS NAT and WCCP do not work together
CSCed16561	Content	DFP agent not able to send keepalives or weights to the manager
CSCee02118	Content	Reqs. from CE get sent back to the CE; CE configured with two ifaces
CSCee31118	Content	WCCP Bypass URl doesnt work with CEF/dCEF immediately after reload

Identifier	Technology	Description
CSCeh13292	Content	WCCP Multiple Configurations causes high CPU
CSCin79644	Content	Flowmask do not change when wccp redirection changed from L2 to GRE
CSCuk50878	Content	Spurious memory access in wccp_srvc_grp_find
CSCdk41322	Infrastructure	Cannot do show buff input-interface on virtual-access interface
CSCdx62060	Infrastructure	Interface names made to display full while show int summary done
CSCdy01705	Infrastructure	High cpu at process TTY Background
CSCdy32629	Infrastructure	cpmCPUTotalPhysicalIndex changes w/o OIR or Restart
CSCdz27562	Infrastructure	snmpwalk on loopback interface gets response from physical int. IP.
CSCdz60577	Infrastructure	Spurious memory access and Traceback after changing SNMP engine ID
CSCea20169	Infrastructure	erase nvram: is not prevented when issued with write mem
CSCea36491	Infrastructure	Input Wedged with SNMP traffic
CSCea62212	Infrastructure	ATA_status timeout errors
CSCea69601	Infrastructure	Disk Corruption on C6400 and/or RSP compatible platforms
CSCea87766	Infrastructure	<interface> is a static pool and cannot be tuned message displayed
CSCeb48835	Infrastructure	Bootvar does not update on PRP
CSCeb69892	Infrastructure	SNMP: traceback int timer_start
CSCeb79675	Infrastructure	SNMP reply packets do not use the correct source address
CSCec21583	Infrastructure	%SYS-3-CPUHOG: SNMP ENGINE
CSCec22574	Infrastructure	IPC-5-REGPORTFAIL: after rsh command executed on GSR LC
CSCec39376	Infrastructure	Flash Card is not recognized when its moved from Master to Slave
CSCec47356	Infrastructure	Active and Standby run-config essentially different
CSCec55147	Infrastructure	Memory leak in IFS
CSCec69091	Infrastructure	PCMCIA disk 0 is formatted from a diff router error
CSCed08172	Infrastructure	wr mem introduces 550ms latency in packet forwarding on npe-g1 PE
CSCed15410	Infrastructure	CLI:syscon IP longstring will crash router
CSCed16920	Infrastructure	Constant high CPU in TTY background
CSCed35964	Infrastructure	Interop issue observed reading Viking 48MB flash on 7200 routers
CSCed41231	Infrastructure	Fix alignment handler to use proper jump target register value
CSCed42330	Infrastructure	Unable to boot using IOS image in second flash partition
CSCed45942	Infrastructure	Bus error due to corrupted managed timer structure
CSCed46843	Infrastructure	compiler change breaks PUTLONGLONG macro
CSCed48158	Infrastructure	atomic_increment() leaks memory
CSCed51952	Infrastructure	Hotswapping linecards while configuring i/f can crash the box
CSCed54444	Infrastructure	Malloc failures and tracebacks on LAC when disconnecting L2TP sess
CSCed59079	Infrastructure	Modified FAT sectors written for wrong device
CSCed63357	Infrastructure	show disk#: and dir disk#: inconsistent
CSCed64664	Infrastructure	SYS-2-LINKED: Bad enqueue messages when terminating multilink vpdn

Identifier	Technology	Description
CSCed76117	Infrastructure	Unable to squeeze flash filesystem via snmp ciscoFlashMiscOpCommand
CSCed86286	Infrastructure	Software forced crash at ssh_process_message_events
CSCed88967	Infrastructure	NVRAM not protected from access by local app during write mem
CSCee00868	Infrastructure	ATA Format Flash increases verification/bootup time
CSCee12118	Infrastructure	ifs_remove / ifs_open with TRUNc mode doesnt work at startup
CSCee18018	Infrastructure	%Error opening nvram:/startup-config at reload
CSCee23750	Infrastructure	%Error formatting flash (Invalid DOS media or no media in slot)
CSCee29138	Infrastructure	ciscoMemoryPoolType returns wrong value
CSCee29214	Infrastructure	NRT: %Error formatting disk0: (No such device)
CSCee30986	Infrastructure	warm reboot command takes more than 500ms for nvgen
CSCee42363	Infrastructure	ip ftp username not used after username was previously used in URI
CSCee47120	Infrastructure	writ mem gives a prompt when saving config with 3 rsa keys
CSCee56618	Infrastructure	attach command may crash router
CSCee58083	Infrastructure	CSCed57948 breaks RPC-R fragmentation
CSCee63808	Infrastructure	CLI: router reloads at [show monitor event-trace merged-list ..]
CSCee66206	Infrastructure	Router crash when booting with bootimage 12.1(22.3)E1
CSCee66688	Infrastructure	status read error on Intel series 2+ cards due to CSCec21583
CSCee83183	Infrastructure	test ipc port remove should only remove Test ports
CSCee91044	Infrastructure	SNMP Trap Sent In Error Upon Every IKE Lifetime Expiry
CSCee96231	Infrastructure	CIP and xCPA ucode fail to load after CSCee13801
CSCef01725	Infrastructure	pak_realign driving up CPU usage
CSCef06881	Infrastructure	dir disk0: takes > 12 min. when easybake file system on disk0
CSCef28657	Infrastructure	Router crash at ip_snmp
CSCef49110	Infrastructure	disk operation fails with read_file/dir failed
CSCef63909	Infrastructure	Crashinfo not written to disk in some cases
CSCef68103	Infrastructure	Disk0 operations fails with NPE-G1 IO controller
CSCeg11566	Infrastructure	SNMP May Consume all the I/O Memory
CSCeg16786	Infrastructure	Device not loading with the image and SP crashes
CSCeg19038	Infrastructure	The entCacheFlag should not be shared with several entity tables.
CSCeg23300	Infrastructure	show mem 0x<addr> needs to be an internal command
CSCeg61032	Infrastructure	Memleak or dead memory when internal OS registry call is made
CSCeg64124	Infrastructure	SAA not sending packets to line after a period of time
CSCeh25393	Infrastructure	CSM:C2R2: memory leak if config and delete VLANs repeatly on msfc
CSCin39040	Infrastructure	Router crashes copying running config from/to tftp server
CSCin43799	Infrastructure	VFC option is missing in copy command
CSCin49362	Infrastructure	RSP16:%SERVER_CLOCK_SYNC-3-BADREQ: seen on rpr+ switchover
CSCin53807	Infrastructure	Warm Reboot Decompression may fail for certain images

Identifier	Technology	Description
CSCin55436	Infrastructure	software forced reload at ipc_open_port
CSCin80221	Infrastructure	FSCK crashes when number of sectors per cluster is zero in boot sect
CSCin86483	Infrastructure	RP crash on terminating router banner on same line with empty banner
CSCsa45568	Infrastructure	Changing RTR config causes Sup720 SSO getting out of sync
CSCsa49566	Infrastructure	%FIB-2-IF_NUMBER_ILLEGAL creating Virtual If (lpb,Virt) after CSCuk55348
CSCsa65096	Infrastructure	Router may crash when nv->textptr is dereferenced
CSCsa68352	Infrastructure	v1 view is attached to default community string
CSCuk51673	Infrastructure	malloc_aligned adds unnecessary padding
CSCdy31356	IPServices	as5300 crashes with DHCP stack overflow error
CSCea03340	IPServices	HSRP virtual address responds to traceroute
CSCea25073	IPServices	IOS FTP client code rewrite
CSCea81029	IPServices	show ip igmp int crashed router
CSCeb07106	IPServices	BGP and md5 authentication issues - TCP-6-TOOBIG
CSCec38667	IPServices	Unified configuration storage broken for 16 character hostname
CSCec50485	IPServices	copy ftp flash fails with 3COM ftpserver
CSCed21865	IPServices	TCP watchdog crash in tcp_putstring
CSCed52163	IPServices	Crash or CPUHOG when doing HSRP SNMP query
CSCed82551	IPServices	VRRP: problem with dynamic reconfiguration of secondary IP addresses
CSCed83616	IPServices	Simultaneously configuring and display HSRP crashes IOS
CSCef35459	IPServices	HSRP - Bogus Error message while adding Virtual IP address
CSCef46191	IPServices	Unable to telnet
CSCef66899	IPServices	Bridge-group causes OSPF neigh to go INIT/DROTHER
CSCef67721	IPServices	Prefix in binding but released in local pool
CSCeg82109	IPServices	VRRP stays in Init status after cable unplug/replug
CSCin78000	IPServices	LDP session in xmit state if MPLS flapped at high traffic on L2 SUP3
CSCin82758	IPServices	Disabled STP on an interface becomes enabled on reload
CSCsa52643	IPServices	The command ip dhcp limited-broadcast-address breaks DHCP forwarding
CSCee02270	LAN	show list cause router reload
CSCee82479	LAN	Tracebacks on cwan_poseidon_dot1q_encap and dot1q_encap_vlan_table
CSCef79968	LAN	snmpget shows No Such Instance for 4GE-SFP-LC sub-interface
CSCeg21175	LAN	ipv6 traffic not going on directly connected serial i/f of RSP
CSCsa52236	LAN	Spurious memory access at dec21140_fastsend after PA OIR
CSCdy43326	LegacyProtocols	Bus Error at address 0xD0D0D11
CSCed14392	LegacyProtocols	DLSW configuration breaks OSPF and HSRP
CSCed88563	LegacyProtocols	No Decnet routing causes buss error
CSCee88936	LegacyProtocols	Removing DECnet Routing causes %ALIGN-3-SPURIOUS error message
CSCef06820	LegacyProtocols	Remote-MAC of 1st TEST F is not converted with dlsw timer explorer-.

Identifier	Technology	Description
CSCea22886	Management	Memory leak in SNMP PING
CSCeb52330	Management	NVGEN-one-command o/p for interface commands is different than sh ru
CSCec25430	Management	IOS may reload from specific packet
CSCed57925	Management	CNS Events not getting generated for ATM PVC provisioning
CSCee58479	Management	Neighbor on PA-MC-8TE1 interface sometimes crashes - CDP traceback
CSCef88326	Management	cns config retrieve fails to pull a config
CSCeg71686	Management	Router crash with reset PWAN2 card - QoS Portchannel config.
CSCeg73883	Management	cikePeerLocalAddr is not augmenting properly
CSCdu28706	MPLS	ARP rejects requests from interfaces in different vrfs
CSCdv91301	MPLS	can not create vrf static route to global connected interface
CSCdx83597	MPLS	TDP running; needs TDP Identifier; no tag-enabled ints -- config OK
CSCdz33630	MPLS	Stanby RP crashes when SSO switchover in the HA MPLS co-existence
CSCdz85325	MPLS	TFIB not get updated after delete and re-add static route
CSCea41043	MPLS	LSR MIB: Would like to remove memory address XC indexing issue
CSCeb19802	MPLS	MPLS MIB Capability statements need to be updated
CSCeb40653	MPLS	Bus error crash at vrf_interface_print when deleting vrf config
CSCeb52414	MPLS	Notify Path Errors fatal to MPLS-TE LSP
CSCeb87433	MPLS	Follow-up on CSCdz75507
CSCec03017	MPLS	Need bundling enabled on VRF Checkpointing
CSCec10116	MPLS	MPLS VPN PE uses global addresses on some packets originated in VRF
CSCec45051	MPLS	VPN MIB: PerfRoutesAdded and PerfRoutesDeleted incorrect
CSCec86102	MPLS	Inconsistent tag info between RSP and VIP
CSCed03539	MPLS	IGP prefixes in the FRR database showing up as vpn prefixes
CSCed21063	MPLS	TE Tunnel Destination Label Missing
CSCed22837	MPLS	Bus error ALIGN-1-FATAL:Corrupted program counter
CSCed25539	MPLS	VRF maximum routes cmd causes pkt loss, drop
CSCed28093	MPLS	Enabling send-label under IPv6 causes LDP updates to BGP-IPv4
CSCed39059	MPLS	LFIB is inconsistent when P-AIS injected on APS interface
CSCed45746	MPLS	duplicate tag between 2 VRFs
CSCed52578	MPLS	vrf route thru recursive tagged loadshared global route bogus label
CSCed54416	MPLS	GRP crash in tfib when pos fiber is disconnected or connected
CSCed55962	MPLS	Connected subnet not in TFIB
CSCed57281	MPLS	CPU hog in CEF reloader while adding a vrf interface
CSCed68723	MPLS	MPLS VPN CEF entry does not have tag information
CSCed81317	MPLS	can not see bgp routes from CE after import map
CSCee00239	MPLS	F/R bridge-group and tag ip cannot coexist despite other subintf
CSCee07279	MPLS	TFIB NULLADJ errmsg triggered, fix root cause of null tagout_adj

Identifier	Technology	Description
CSCee12408	MPLS	%REDUNDACY-3-CONFIG_SYNC: Active and Standby lbl when config ldp nei
CSCee26700	MPLS	memory leak caused by LSR MIB queries
CSCee37430	MPLS	Missing LFIB tag rewrite on LC after loss of /32 entry to its next-hop
CSCee56225	MPLS	Alignment errors in tfib_request_all_tags
CSCee59585	MPLS	Duplicate label in sh ip cef on LC
CSCee62326	MPLS	TFIB-7-SCANSABORTED: TFIB Scan not completing error
CSCee67207	MPLS	Recursive route not labeled on E4/E4P if send-label configured
CSCee78118	MPLS	E3 4oc12: Linecard crashes at alpha_update_deaggregate_vrf
CSCee84732	MPLS	CPU 99 % with Tagcon Addr process taking up 80% to 90%
CSCee93228	MPLS	Process watchdog in ip_trace_show_extended
CSCef14446	MPLS	mpls vpn: recirculation vlan for agg label is not mapped to vpn
CSCef18515	MPLS	FRR:RP and LC not consistent after clear cef line.
CSCef22069	MPLS	Glean adjacency not completing arp for VRF interfaces
CSCef25866	MPLS	Blackholing of traffic during FRR reconnect with invalid cache adj
CSCef51239	MPLS	NRT:after remove ldp tcp block and toggle mpls ip, ping not worked
CSCef58522	MPLS	TFIB-7-SCANSABORTED: TFIB scan not completing. Unresolved adjacency
CSCef59275	MPLS	Traffic drop forever in FRR active state because of wrong FRR label
CSCef59507	MPLS	Dead LDP session still shows up after new session established
CSCef80349	MPLS	GSR midpoint rejects RESV after link flap
CSCef85231	MPLS	Standby will reload due to mpls ldp target command out of sync
CSCef89647	MPLS	memd alignment error and bus error @ rsp_drop_iptag_pkt
CSCef97536	MPLS	LDP label not populate in forwarding table after clear ip route
CSCeg03885	MPLS	TE label missed on MPLS TE tunnel
CSCeg12649	MPLS	A follow up to CSCef22069
CSCeg27836	MPLS	suspect vrf leak following foreign ebgp flap
CSCeg90033	MPLS	Missing labels in MPLS/VPN forwarding table
CSCeh23047	MPLS	TAG2IP traffic does not recover after SSO switchover ingress E3/E4+
CSCin35896	MPLS	Explicit withdraw of a Label causes IPv4 BGP to not update the LFIB
CSCsa53117	MPLS	MLS cef hardware Freeze
CSCsa77411	MPLS	RP crash at rrr_lm_unlock_bandwidth
CSCec03024	Multicast	NATing Payload of (S,G) Join in SSM Environment
CSCec19125	Multicast	Payload field have been changed after NAT
CSCec23559	Multicast	show ip msdp peer x.x.x.x advertised-SAs may cause reload
CSCec37022	Multicast	Join delay timer issue when receiving successive Prunes
CSCec58348	Multicast	SDP/SAP: need to implement support for payload-type in SAP
CSCec80252	Multicast	PIM:(S,G) join on RPF interface does not trigger a RPF check
CSCed12688	Multicast	PIM SSM Prune Latency Under Certain Topology

Identifier	Technology	Description
CSCed45452	Multicast	PIM-DM state-refresh not working after reload
CSCed50220	Multicast	Const2:C2MCAST SP and RP mfib tables are not in sync.
CSCed85752	Multicast	router generating tracebacks when using qos/ipsec/multicast
CSCee02125	Multicast	syslog messages needed for pim neighbor loss
CSCee03081	Multicast	PIMv6: Source address for the register tunnel should be configurable
CSCee19831	Multicast	MLD EXCLUDE for SSM not ignored completely when explict-tracking
CSCee24899	Multicast	router crashed at mwheel_twheel_start
CSCee65066	Multicast	ciscoPimInvalidJoinPrune trap contains wrong VARBIND
CSCee66936	Multicast	Router reload, traceback at dvmrp_mbgp_walk
CSCee84457	Multicast	Uptime for VRF multicast routes dont go beyond 7w- sh ip mroute vrf
CSCee89438	Multicast	MSDP doesnt build S,G state after rxing *,G join
CSCee93574	Multicast	Unable to delete RP when groups are overlapped with another RP
CSCef36986	Multicast	no mls ip multicast non-rpf cef added to sup2/msfc2 by default
CSCef53297	Multicast	ip pim accept-register list does not deny ICMP registers
CSCef60452	Multicast	possible blackout when receiving Join on RPF interface (iif)
CSCef89240	Multicast	Crash in sh ipv6 pim topo command in pim_show_add_mroute
CSCeg28814	Multicast	Duplicated mcast packet due to wrong FPOE in egress replication mode
CSCeg39601	Multicast	IPV6 encap tunnel is always down
CSCeh15639	Multicast	crash due to freed nbr while sending PIM hello
CSCeh47667	Multicast	A ddts to commit CSCef60452 to pikespeak
CSCsa45490	Multicast	Spurious memory access at pim_receive_autorp_packet
CSCuk49673	Multicast	MRIB: No multicast forwarding after no ipv6 multicast; ipv6 multicas
CSCeb64018	platform-75xx	traceback at tagsw_forward_inline
CSCec24167	platform-75xx	Bus Error Crash while reading PCMCIA Flash: pcmcia_read()
CSCed33110	platform-75xx	VIP crash induces RSP to hold memory leading to a crash
CSCee35740	platform-75xx	FIB DISABLE after a VIP crash
CSCee65997	platform-75xx	Flapping GE on GSR P router causes PE POS int to flap
CSCec22452	platform-76xx	QOS/RT/DB: LC crashed with TxSOP Errors
CSCec46892	platform-76xx	OSM-ATM:Mcast pkts are dropped over 1483 bridged PVCs
CSCec59550	platform-76xx	OSM-POS crash @ sky4302_enter_drop_mode
CSCec62800	platform-76xx	20E:CWAN-QOS:Increased PQ latency when increasing default queue traf
CSCec74760	platform-76xx	7600 w/BRE configured replies to ARP even with Interface down/down
CSCed07253	platform-76xx	512 Meg SODIMM chip not recognized and shows 256 instead
CSCed19898	platform-76xx	:ATMoMPLS VCs freeze/vanallen error/w toggling core loopback
CSCed51835	platform-76xx	OSM/POS/BB1: OC12 IP 64 bytes performance may degrade
CSCed78077	platform-76xx	LRDI is not reported after reload on OSM-2OC12-ATM-SI PRDI is seen
CSCee14301	platform-76xx	OSM GE Autonegotiation interoperability issues with Ciena K2

Identifier	Technology	Description
CSCee45508	platform-76xx	OSM CHOC-OC12 freezes up while proccessing PPP keepalives
CSCee55056	platform-76xx	OSM interface byte counts are inaccurate
CSCef08790	platform-76xx	PWAN-1:Hidden vlans overlap .1q vlans on same PWAN sub-intf
CSCef12193	platform-76xx	FABRIC-SP-6-TIMEOUT_ERR: Fabric in slot 8 reported timeout error
CSCef12304	platform-76xx	PWAN2:Connectivity is broken between GE-WAN if one end shut/no shut
CSCef19811	platform-76xx	MPLS:VPN:MLPPP:PE not receiving packets from connected CE
CSCef35398	platform-76xx	OSM-2OC12-ATM-SI+ - SRIC IPM parity error
CSCef45881	platform-76xx	aps force from protect to working does not notify routing of change
CSCef74227	platform-76xx	LAN GE of OSM incorrectly increments giants on dot1q trunk port
CSCef76828	platform-76xx	connectivity broken after config/unconfig tunnel interfaces
CSCef82720	platform-76xx	add dot1Q subinterface in ifTable for GE-WAN card
CSCeg05604	platform-76xx	OSM-1CHOC12/T3-SI Detects False AIS when a Remote NM-1T3/E3 is Shut
CSCeg10236	platform-76xx	PWAN2:GBIC type shown as not connected in show int
CSCeg55750	platform-76xx	PP: L2 port on OSM-GE-WAN drop to err-disable when UPE is rebooted
CSCeg77503	platform-76xx	SAA Packets do not hit the outbound service policer
CSCeh11457	platform-76xx	NRT:during mpls testing, ge-wan interface not ocming up
CSCeh23737	platform-76xx	While using L2PT on ATM OSM BPDUs are not filtered
CSCsa47099	platform-76xx	IPX broke on wan link of OSM-2OC12-ATM
CSCsa53708	platform-76xx	OSM crashes under stress when having to pad packets
CSCeb07656	PPP	dMLP:Not receiving packets from multilink int until shut/no shut
CSCeb36360	PPP	Spurious access at ppp_notify_cb_configured
CSCed67708	PPP	IfStackTable is not updated when MLPPP interface is created
CSCee44086	PPP	Multilink PPP cant forward traffic after RP switch-over
CSCee69493	PPP	dMLP fails if control is given to IOS MLPPP
CSCee72906	PPP	dLFIoLL mlp-qos:VIP crash when bundle is reset while traffic is ON
CSCee94294	PPP	Spurious memory access with dLFI interface
CSCef15095	PPP	7500:dLFIoATM: VIP might crash under missed DLFI down events
CSCef44786	PPP	ATMPA-3-BADVCD seen when running MLPPP at low speed
CSCef94525	PPP	Linecard crashes when fib disabled with more than 37 MLP bundles
CSCeg57219	PPP	Unable to ping packets greater than 1022 across MLPPP after sup SW
CSCeg80996	PPP	Second PPP SSO switchover causes pings to fail
CSCeh20758	PPP	MLP interface stays shutdown post SSO switchover
CSCdw01772	QoS	Router may reload if distributed NBAR is configured
CSCeb63310	QoS	Bus Error increment_wred_matched_stats
CSCec23982	QoS	Packet fragmentation causes high CPU at interrupt level with NBAR
CSCec25534	QoS	Memory limit for NBAR wrong when over 214.8MB of free memory
CSCec26626	QoS	RSVP: crash in rsvp_db_msgid_compare() when memory is exhausted.

Identifier	Technology	Description
CSCec27278	QoS	Memory leak in hqf_rp_mlp_blt_setup
CSCec27338	QoS	NBAR should gracefully handle traffic streams with dropped fragments
CSCec46485	QoS	match dscp and match prec matches do not take effect.
CSCed12831	QoS	MQC: should block the non-supported acl with log
CSCed37615	QoS	Watchdog timeout after renaming policy-map.
CSCed46785	QoS	LC crashed at packet classify
CSCed51640	QoS	dWFQ isnt diplayed in sh run anymore, so is lost after reload
CSCed54236	QoS	Router reloads due to memory leak
CSCed54330	QoS	WFQ on virtual-template causes allocation error and tracebacks
CSCed55794	QoS	MSC-200-QOS: RP crashed @ipfib_apply_input_police after move police
CSCed60987	QoS	dCEF path broken when configuring output service-policy
CSCed62637	QoS	CWPA: priority traffic latency varies with default traffic load
CSCed65075	QoS	VIP4-80 crash at hqflayer_config
CSCed67734	QoS	MQC: set atm-clp causes packets to be dropped at receiving end
CSCed70198	QoS	malloc failure and Line protocol down when frame relay frag configur
CSCed76109	QoS	after pvc flap, some pvcs stay down with ATM interface up/up
CSCed79634	QoS	police percent conversions are incorrect in 2nd and 3rd lvl policies
CSCed88854	QoS	VIP crash with bus error in hqf_blt_delete_from_driver
CSCed89629	QoS	Applying service-policy crashes VIP4-80
CSCee05729	QoS	dCEF gets disable after QoS config
CSCee12235	QoS	Bus error when reapplying renamed policy-map to ATM PVC
CSCee18883	QoS	output stuck on interface causes cbus-complex and IPC timeout
CSCee22810	QoS	Router stops sending LMI with QOS configured
CSCee24349	QoS	Crash at fib_post_download_processing when reloading
CSCee31618	QoS	C2SUP2/FW2/CT3+:Voice packet drops at low rates with cRTP+LLQ conf
CSCee36050	QoS	VIP crash when re-use channel group with set service policy
CSCee38324	QoS	VIP crash at hqf_svip_ifc_dtq_consumer when traffic go through
CSCee47275	QoS	card resets due to [no] fair-queue cleanup loops
CSCee66909	QoS	ct3 spa: qos configs should be blocked on multilink member links
CSCef02160	QoS	long router boot time due to processing in stile_in_policymap
CSCef06034	QoS	Sup720 crashes after SSO Failover with nbar configured
CSCef25953	QoS	dwred statistics are not updated in show policy-map int output
CSCef46134	QoS	CPUHOG at CEF MQC IPC Background on SIP-600 on remove/apply qos
CSCef47829	QoS	Physical int out of BW: no error message that MQC policy cant apply
CSCef66517	QoS	packet drop on flexwan when traffic shaping
CSCef70739	QoS	MAXMEMORYUSED Error with 4 GB active links
CSCef91275	QoS	RSVP: policy does not retry outbound request after failure

Identifier	Technology	Description
CSCeg25493	QoS	VIP Bus error crash in get_same_id_actiongroup
CSCeg31912	QoS	QoS does not see correct interface bandwidth on dMLFR interfaces
CSCeg33229	QoS	VIP crash when service policy removed from MFR int with traffic
CSCeh13583	QoS	MQC: ipv6 acls changes not notified to the platform clients
CSCin52060	QoS	After the policy got rejected hqf was not cleaned on vip
CSCin61140	QoS	mfr: LC crahses with LFI/mqc enabled
CSCin70454	QoS	dLFIoAT : RSP is stuck at LCP timeout
CSCin72437	QoS	MQC: Concurrent access crashes the Flexwan during switchover
CSCin86096	QoS	Classification matching on IPv6 acl fails
CSCsa53001	QoS	vip crashes in hqf_svip_ifc_dtq_consumer after serial-subint flap
CSCuk49453	QoS	Traceback when configuring nbar
CSCdk23784	Routing	EIGRP next-hop is not used
CSCdt38401	Routing	Frame-relay packets processed by cpu due to CEF inconsistency
CSCdt51547	Routing	Packet drop with ip verify unicast reverse-path.
CSCdu59038	Routing	- show ip eigrp neighbor - may crash router
CSCdv12472	Routing	BGP does not remove confed-AS-path on eBGP links
CSCdv76375	Routing	OSPF neighbor command unsupported in VPN routing instance
CSCdv84363	Routing	Routes not installed across MPLS TE tunnels after clearing OSPF
CSCdv90022	Routing	Interface not recieve traffic after shut/no shut
CSCdw51691	Routing	ISIS MPLS TE adj pointer mem leak, may cause mem fragmentation
CSCdw78242	Routing	PE-CE: Backdoor link always preferred over VPN
CSCdy23644	Routing	ghost config in router after line card swap
CSCdy60008	Routing	NRT:rsp router crashed at ipigrp2_route_adjust+0x5c
CSCdy77097	Routing	RIP Jumbo fix for VPN and Performance
CSCdz38670	Routing	CEF adjacency for arp with alias keyword is lost after reload
CSCdz50424	Routing	Handling of ICMP Type 15 responses
CSCdz54344	Routing	static route adjustement trigger delay
CSCdz69672	Routing	unable to redistirbute secondary connected routes
CSCdz81659	Routing	CEF doesnt delete adjacency of Virtual IP on HSRP transition
CSCea01837	Routing	%SYS-2-NULLCHUNK in ip_apply_input_mac_acc
CSCea09852	Routing	%FIB-3-FIBBADXDRSLOT: Invalid XDR slot. Type/len/slot 30/77/7
CSCea15115	Routing	hybrid-cli doesnt work for v6-afs
CSCea19918	Routing	BGP: need to do multipath with different as-paths
CSCea31201	Routing	Crash in ip_fast_accumulate_acctg
CSCea33138	Routing	Packets dropped while building mGRE spoke-spoke link
CSCea47597	Routing	RIP Routes Stuck In Routing Table
CSCea49910	Routing	as-override breaks eBGP with multiple CE peers in the same VRF

Identifier	Technology	Description
CSCea56883	Routing	Router hangs due to bus error at network_check
CSCea58973	Routing	BGP NSF: Some VPNv4 BGP routes get purged after RP switchover
CSCea59206	Routing	Distribute-list command does not stay under address-family ipv4
CSCea64161	Routing	E3 ch/oc12: IS-IS Update CPUHOG for 840 ppp isis intfs
CSCea66299	Routing	%BGP-3-NEGCOUNTER messages appear during route flapping
CSCea76840	Routing	PER-USER cosmetic bug in SHOW IP PROTOCOL
CSCea78615	Routing	SFC at mgd_timer_first_running related to NHRP
CSCea80821	Routing	Eigrp topo not updated after redist if floating static present
CSCea83086	Routing	NHRP and VRFs do not interact well
CSCea85395	Routing	BGP supressed prefixes not reinstated after condition removed
CSCea92690	Routing	registration packet gets lost when tunnel protection comes up
CSCea92893	Routing	unknown gateway info. for sh ip proto vrf
CSCeb07288	Routing	Crash in NHRP managed timers
CSCeb08101	Routing	EIGRP: high bandwidth metrics are not nvgened properly
CSCeb27742	Routing	invalid input detected at exit-address-family after boot
CSCeb43353	Routing	Default-information originate in BGP shouldnt be tied to peer group
CSCeb53542	Routing	Inconsistency between CEF adjacency and ARP tables; unicast pkt loss
CSCeb54519	Routing	NHRP should retransmit registration requests
CSCeb57086	Routing	After issuing bgp upgrade-cli redundancy sync fails
CSCeb65685	Routing	ip cef load-sharing algorithm tunnel command lost upon reset of rpm-
CSCeb66602	Routing	peer-group nlri multicast command adds unicast in upgrade to25S1
CSCeb69972	Routing	Set Community None broken
CSCeb74105	Routing	Counters on the rules that are reflected are not updated
CSCeb75489	Routing	Named ACL does not allow duplicate remark statements
CSCeb77653	Routing	second vty freezes while editing prefix list
CSCeb84144	Routing	BGP aggregate route not cleared after removing from the config
CSCeb86068	Routing	passive-interface support needed for router ospf vrf
CSCec00165	Routing	RIP updates lost under heavy load
CSCec04708	Routing	OSPFv3: default-info originate not working properly with route-map
CSCec05264	Routing	BGP: Peer-group configuration is deleted, when last peer is removed
CSCec07566	Routing	Packets for interface with named ACL are not dcef switched
CSCec07592	Routing	NRT: With bgp deterministic med config, best path not chosen correct
CSCec07636	Routing	snmpwalk on ospfnbrrtrld does not display all switch1 interfaces
CSCec07941	Routing	%FIB-3-FIBDISABLE msg after booting while ip routing is disabled
CSCec08795	Routing	Memory leak in CEF process during deferred delete
CSCec16245	Routing	BGP set metric-type internal doesnt work with set metric +/- cmd
CSCec20352	Routing	BGP table version changes for locally sourced vpnv4 routes

Identifier	Technology	Description
CSCec21709	Routing	ping of 10.0.0.0/8 in the CEF path does not work
CSCec22723	Routing	Router may reload unexpectedly due to ISPF(OSPF)
CSCec23167	Routing	Interface input queue backs up during BGP scalability test
CSCec25744	Routing	reload when connecting spoke to spoke
CSCec27454	Routing	Watchdog reload at nhrp_cache_count_nbma_subr
CSCec30677	Routing	IOS device pauses indefinitely when reload command is issued
CSCec32738	Routing	IPCP: Install route to <IP address> is missing.
CSCec39973	Routing	RP crash at isis_add_is_neighbors_to_lsp
CSCec40535	Routing	BGP: a single slow peer impacts convergence of other peers
CSCec42871	Routing	clear adj and/or generate error mesg. when md5 auth. not matching
CSCec44271	Routing	MBGP: Route Reflector not advertise nlri multicast
CSCec47079	Routing	EIGRP variance should install equal cost route
CSCec48142	Routing	Unable to globally disable proxy ARP
CSCec48833	Routing	NRT:Load sharing verification failed
CSCec55608	Routing	BGP redistribution in IGP based on std communities/as-path not work
CSCec61594	Routing	Route-maps with continue fails to match a community list
CSCec67985	Routing	Clear ip bgp external vrf <name> cause all VRFs to flap
CSCec70664	Routing	BGP stays in READ_ONLY mode longer after CSCeb54512
CSCec73316	Routing	Load-balancing ratio over TE tunnels not the same as configured
CSCec79860	Routing	EIGRP unequal balancing breaks with MLPPP reducing bandwidth
CSCec82398	Routing	BGP needs to modify a route instead of delete/add
CSCec85207	Routing	DMZlink-BW for neighbor on ATM subinterface is set to 0
CSCec85804	Routing	router crashed at rip_onoff_idb under low mem test
CSCec90041	Routing	BGP: update generation deadlocked when outbound policy changed
CSCed02844	Routing	Adjs out of p2p interface fail to repopulate
CSCed15990	Routing	tag forwarding entry not deleted when BGP dampening is configured
CSCed17879	Routing	adtvertise ipv4 routes across ipv6 BGP peers not working
CSCed25969	Routing	NHRP shouldnt delete static cache entry upon route removal
CSCed26048	Routing	IP Background Process very high when OSPF or EIGRP catch-all present
CSCed28920	Routing	Dynamic NHRP cache entry deleted due to BGP peer change
CSCed36386	Routing	APS:Ping fail on alternate packets after revertive switching
CSCed41641	Routing	reload when removing tunnel interface with nhrp
CSCed43597	Routing	Add PRC for eigrp interface and nsf related commands
CSCed46066	Routing	%ALIGN-1-FATAL: Corrupted program counter after vpn-gre unconfig
CSCed46438	Routing	default-information originate not working for ISISv6
CSCed53358	Routing	Pings fail on ethernet to VLAN interworking over L2TPv3, irdp fails
CSCed59370	Routing	OSPF Type 5 LSA not updated when forwarding address changes

Identifier	Technology	Description
CSCed60289	Routing	delay in route update on interface down cause scalability issue
CSCed60800	Routing	Routing Table not updated when BGP next hop is withdrawn
CSCed61503	Routing	in dmvpn hub-spoke nhrp does not show spoke pre-nat private ip
CSCed62479	Routing	next-hop-unchanged does not work w confed ebgp
CSCed63342	Routing	RIP-Unicast updates not sent to configured RIP neighbors
CSCed63876	Routing	BGP: router crashes pointing to ed_decay_penalty
CSCed66144	Routing	EIGRP: next-hop self routes incorrectly deleted from RIB
CSCed72283	Routing	eigrp variance not considered under address-family
CSCed74812	Routing	A few packets loss when vpnv4-bgp switchback on RR redundancy
CSCed77612	Routing	network option missing in isis interface command
CSCed82706	Routing	tracebacks in ipigrp2_add_item when NAT configured
CSCed83891	Routing	BGP prefixes current field counter wrong in sh ip bgp neigh comman
CSCed86069	Routing	Software forced crash- crashdump is_chunk_bad checkchunk-
CSCed93630	Routing	router crashed at bgp4_format_mp_attr
CSCed94589	Routing	alignment error in ipigrp2_passive_interface_command upon reload
CSCed96206	Routing	Crash after <no neighbor> command
CSCee01550	Routing	Per-user access-lists disappear after first show ip access-lists
CSCee01628	Routing	conditiona debug ip packet display all ip packets
CSCee05779	Routing	CLNS partition avoidance not working
CSCee16068	Routing	Equal cost default route remains in RT after changing interface cost
CSCee19691	Routing	RP crashed on rip_process_mgd_timers on clear ip route *
CSCee19880	Routing	EIGRP routes stuck in routing table when using no ip-next-hop-self
CSCee21928	Routing	OSPF not installing multiple next hops to single neighbor
CSCee23517	Routing	Inconsistent Fib tables between RP and LCs
CSCee26387	Routing	Removal of static routes from the routing table may take 60 seconds
CSCee27357	Routing	bus error when configuring advertise-map with the set command
CSCee28466	Routing	set metric + or - does not correctly adjust MED metric for BGP
CSCee30718	Routing	BGP max community limit should be removed
CSCee39853	Routing	CEF getting disable on Standby PRE
CSCee40207	Routing	Memory leak in BGP Open Process After SSO RP Switchover
CSCee41172	Routing	BGP: maximum-path import purges wrong paths
CSCee42285	Routing	constant route flap with eigrp SOO if route not injected from eigrp
CSCee43166	Routing	BGP: reduce CPU load for processing inbound VPNv4 updates
CSCee50846	Routing	BGP: converge an update-group independently from other update-groups
CSCee52822	Routing	Process-switched RPFv6 doesnt check if CEFv6 is enabled
CSCee54672	Routing	ISIS does not function properly, creating loop, route flapping.
CSCee56976	Routing	rip non direct neighbor is broken

Identifier	Technology	Description
CSCee59315	Routing	MPLS-VPN:Corrupted BGP table showing stale and/or poisoned paths
CSCee63163	Routing	BGP IPv6 recursive lookup problems
CSCee70840	Routing	DMVPN: daisy-chained HUBs loose sockects between themselves
CSCee75996	Routing	SSO:IPv6:Spurious memory access at ipv6fib_find_fib
CSCee76562	Routing	Spurious Access traceback @ipigrp2_add_item_dest
CSCee83098	Routing	BGP deletes the static VPN route with global keyword in extranet
CSCee85202	Routing	Long delay for vrf to be removed from vrf table when un-configured
CSCee85488	Routing	Net LSA is not originated on PE-CE link
CSCee85676	Routing	BGP does not import updated prefixes into VPNv4 table
CSCee86530	Routing	MP-BGP fails to report martian next-hop when nh is all 1s or martian
CSCee88898	Routing	ALIGN-3-SPURIOUS in show_ipprotocol
CSCef00037	Routing	SSO:T/B DUAL-3-INTERNAL IP-EIGRP(0) internal error after S/W
CSCef00296	Routing	router crash at bgp_upd_candidate
CSCef00535	Routing	RP crash on validblock when neighbor did SSO switchover
CSCef08044	Routing	no clns route-cache broke vaccess subinterface
CSCef08797	Routing	static routes not advertised to BGP peers
CSCef10480	Routing	%IPC-5-INVALID: Dest Port 1020007 Invalid Port Index=0x0
CSCef11737	Routing	OSPF passive-interface default bleeds to OSPF VRF interfaces
CSCef16804	Routing	On switchover cef entries learned through uplink port dont purged
CSCef19137	Routing	arp table not flushing entries on idb flap and missing adjs
CSCef24703	Routing	default-information originate with route-map not working correctly
CSCef26976	Routing	Removing one vrf messes up ospf config of other vrf
CSCef29091	Routing	Redistributed RIPv2 Subnets Matching Major Net Not Sent
CSCef30437	Routing	dynamic arp entries not cleared on interface link down
CSCef39466	Routing	Redistributed RIPv2 Route Matching Major Net Not Sent
CSCef45830	Routing	Staled BGP route remains in table in bgp multipath testing.
CSCef50427	Routing	System crashed when show ip bgp XX.
CSCef57803	Routing	Missing iBGP refresh after fixing a duplicate address
CSCef65500	Routing	ospf_db_timer_tick cpuhog process OSPF
CSCef77174	Routing	NHRP fails on mGRE tunnel if network-id a multiple of 256
CSCef77648	Routing	Excessive replication of locally generated multicast on mGRE
CSCef81489	Routing	MPLS/VPN Inter-AS: Withdraw not sent on ASBR
CSCef89529	Routing	BGP neighbor advertisement-interval does not work
CSCef93215	Routing	router crash at ospf_build_one_paced_update
CSCef95026	Routing	Bus Error due to OSPF accessing freed LSDB entry
CSCef95474	Routing	static arp cannot be removed and other issues
CSCef95821	Routing	static with global next-hop marked as best in BGP but not in vrf RIB

Identifier	Technology	Description
CSCef96650	Routing	IS-IS passive-interface not work
CSCef97268	Routing	NHRP: Wrong NBMA address for spoke-spoke when hub behind NAT
CSCef97340	Routing	ipv6 mcast:mrib client not seen on sp/dfc on reload
CSCef97738	Routing	BGP/MVPN: incorrect update-source is passed from BGP to MVPN
CSCeg00610	Routing	PP: RP crash at isis_ispf_clean_one_list
CSCeg05830	Routing	BGP: Update peer-group remove-private-as functionality
CSCeg07725	Routing	EIGRP redistributing BGP inconsistently after BGP topology changes
CSCeg08344	Routing	with cef/dcef enabled & compression on, tcp frames getting dropped
CSCeg09032	Routing	ospf routes not updated when link cost changes and ispf enabled
CSCeg13958	Routing	peers missing from ibgp vpnv4 peer-group
CSCeg16620	Routing	PE-CE: Need deterministic path selection for equal cost routes on PE
CSCeg19442	Routing	crash on pdb_ospf_hello_BLOCK
CSCeg20212	Routing	ISIS process restarts upon receiving LSP with max sequence number
CSCeg21842	Routing	EIGRP BFD: crashes in igrp2_peer_destroy with lots of link flaps
CSCeg26378	Routing	Dest CEF entry is missing in DCEF table. All pkts are punted to RP.
CSCeg30291	Routing	BGP fails to send update/withdraw to some peers
CSCeg31951	Routing	BGP: Put peers with as-override & rem-pvt-as in separate updgrps
CSCeg35811	Routing	no ip routing cause the master sw to crash
CSCeg41363	Routing	OSPF SHAM-LINK ON PARRALLEL PATH DOESNT WORK
CSCeg41727	Routing	BGP wrongly sets next-hop for redistributed static routes
CSCeg49796	Routing	BGP peer wont stay shutdown
CSCeg52889	Routing	Rockies2: MPLS TE Tunnel dont come up after adding loopback int
CSCeg62496	Routing	Type-3 lsa not generated if Type-1 flaps coming from multiple areas
CSCeg70726	Routing	PP:mVPN:RP crashes on configuring mdt default @iprib_idb2tableid
CSCeg72989	Routing	IPv6 static neighbor broken
CSCeg74205	Routing	OSPF LSA Type 3 causes SPF execution every minute
CSCeg74772	Routing	Tunnel idbs not reused on the LC when clear cef linecard is issued
CSCeh00680	Routing	router may reload when isis mt is configured
CSCeh04837	Routing	Arp entries purged on SSO
CSCeh05567	Routing	Sham-Link cost changes cause wrong next-hop recalculation
CSCeh07510	Routing	Rockies2: OSPF Trace found after no router ospf command
CSCeh07809	Routing	BGP leaves a stale CEF entry
CSCeh11984	Routing	Missing prefix update when the recursive route is deleted.
CSCeh12233	Routing	12.2SX: fibtype2fibmsg crash - backout CSCef30577
CSCeh14015	Routing	Routes are not redistributed properly
CSCeh27783	Routing	IPv6: 500 manual tunnel script cause IOS crash
CSCeh28320	Routing	IPHC does not commuicate with RP after HA switchover

Identifier	Technology	Description
CSCin33082	Routing	problem with changing distance for static routes
CSCin73487	Routing	BGP Conditional advertisement broken
CSCin84644	Routing	Routes are not seen on neighbors after switchover on eigrp stub rtr
CSCin87277	Routing	FEonCWPA2:%SYS-3-CPUHOG due to process = OSPF for scaled subints
CSCsa39998	Routing	NHRP shouldn't trigger CEF to refresh an NHRP Registration Entry
CSCsa40588	Routing	Routes are not withdrawn from routing table after BGP routes are removed
CSCsa43135	Routing	NHRP: Incomplete mapping entry stays in table too long
CSCsa44181	Routing	ospf virtual-link (DC) flaps during md5 key rollover
CSCsa51951	Routing	Virtual-Link stuck in extstart/exchange
CSCsa53911	Routing	OSPF type3 LSA filtering for 0.0.0.0/0 not effect immediately
CSCsa55048	Routing	Static exported in vrf has wrong cef entry
CSCsa59600	Routing	IPSec PMTUD not working [after CSCef44225]
CSCsa60015	Routing	OSPF: <no ip ospf> issued in interface mode removes global ospf config
CSCuk41411	Routing	HA: show cef linecard doesnt display RRP as expected
CSCuk45392	Routing	BGP ipv6 neighbor cannot inherit peer-policy template
CSCuk45501	Routing	BGPv6: Route-reflector cannot change nexthop for iBGP prefixes
CSCuk46249	Routing	IPv6 CEF: debug ipv6 cef ... not recognised
CSCuk48925	Routing	Adjacency update with invalid fibidb messages detected on VIP
CSCuk49384	Routing	Suppress t/bs for null fibidb->idb on newly active RP on SSO s/o
CSCuk49694	Routing	6PE: Ignoring label update from peer
CSCuk50159	Routing	DCEF not running on VIP if reconfigured after switchover
CSCuk52062	Routing	RIB link failure after memory exhaustion
CSCuk52253	Routing	IPv6 static route missing tag argument
CSCuk53957	Routing	IPv6 routes via intf stay in RIB even intf has been removed by OIR
CSCdu83050	Security	ssh needs source-address
CSCdy25784	Security	CEF switching mGRE tunnel drops packets every NHRP holdtime
CSCdz64323	Security	Software forced crash in CRL code
CSCea16871	Security	Need to improve GRE tunnel int. selection for incoming GRE pkts.
CSCea59073	Security	Downloading CRL by SCEP GetCRL fails and sometimes crashes router
CSCeb25416	Security	Router crash at C_DeleteObject(0xb905d8)+0x34 on 804 & 805
CSCeb64967	Security	IKE SA fail to come up with Solaris Unity Client using cert
CSCeb83287	Security	crypto key zeroize crashes router with http secure-server
CSCec01500	Security	CDP not supported over GRE tunnel
CSCec22308	Security	mem allocated at PKI_ParseX500Dn(0x6207eb2c)+0x34 was leaked
CSCec22391	Security	ca_req deadlock after CRL expires
CSCec31053	Security	sh cry ca cert xx causes %ALIGN-1-FATAL: Illegal access to a low add
CSCec32184	Security	RSA-SIG IKE leaks memory

Identifier	Technology	Description
CSCec32192	Security	Trustpoint source interface command rejected only on reload.
CSCec35857	Security	PKI: crash when authenticating a sub CA after auth the root
CSCec76781	Security	12.3.3 %SYS-3-CPUHOG in Crypto PKI RECV
CSCec88399	Security	CS: Enrollment request without extension fails
CSCed35711	Security	IKE fails when receiving CERT_REQ without CA issuer name
CSCed54769	Security	sh cry ca timers can crash the router
CSCed56270	Security	Box reloads on HTTPS File Get
CSCed60664	Security	import DOS-formatted text file might fail
CSCed81049	Security	PKI: not able to delete trustpoint after doing IKE
CSCed83180	Security	PKI: query mode feature is not working
CSCed91119	Security	multiple certs in SCEP CertResp might crash router
CSCed93963	Security	Enrolling with invalid subject name CA might crash router
CSCee04732	Security	Re-enroll using terminal does not replace the existing router cert.
CSCee27987	Security	CDP on Tunnel interface reports duplicate in neighbor table
CSCee39637	Security	Gre & shaping can get large output rate above physical interface
CSCee72828	Security	Router running IOS-SSHv2 doing SCP hangs
CSCef26840	Security	Router hangs after reapplying nhrp config on the tunnel interface
CSCef67660	Security	sshv2 malform client ignore msg cause demage to router
CSCef98116	Security	cat6500 12.2SX: SSH issues with privilege levels
CSCeg00663	Security	ip mtu config change not reflected in IPSec data path
CSCeg15922	Security	DMVPN:crypto socket is not open until shut/noshut tunnel interface.
CSCin70986	Security	UUT crashes when due to memory corruption when EzSDD is Configured
CSCsa42726	Security	DMVPN: Crypto socket not deleted when p-pGRE tunnel in up/down state
CSCsa59906	Security	VPNSM: Malloc failure in IPSEC key engine and router crashed
CSCuk54386	Security	Delete/create of GRE tunnel causes fixup to be disabled.
CSCdv68743	Unknown	Inefficient code in qos/qoscli_match_packet.c:match_named_acl().
CSCdy33703	Unknown	Need span support for port 1/4 & 1/3
CSCdz66609	Unknown	cat6k & ons155xx interop issues with Y-cable APS
CSCdz83100	Unknown	Multicast pkts should not be policy routed in CEF
CSCea16744	Unknown	GBIC optical 7500 router crash on attach queueing output policy
CSCea28043	Unknown	Nvgen_one_command o/p has an extra ip prefix
CSCea31672	Unknown	ping wont go through due to encapsulation failed on 7500+vip router
CSCea51450	Unknown	Incorrect number of CPUs in CISCO-PROCESS-MIB cmpCPUTotalTable
CSCeb53380	Unknown	benchmarked call setup rate ~75% of fullsail cco image (4/28)
CSCeb56814	Unknown	SUP1A connectivity problem :CAM learn 15/2 in ieee/dec and mls rp ip
CSCeb64745	Unknown	Missing RIP update when executing show run command
CSCeb65576	Unknown	Router crash in cls, used with llc2, dlsw ect.

Identifier	Technology	Description
CSCeb65671	Unknown	Wrong local vc label is programmed for data plane
CSCeb79911	Unknown	AToM: Incorrect Runt checking causes valid packets to be dropped
CSCec00930	Unknown	bus error at crypto_ipsec_clear_peer_sas
CSCec30836	Unknown	Image Verification: %SIGNATURE-4-NOT_PRESENT
CSCec34010	Unknown	OSM2-GE 64 bit main interface counters stay 0
CSCec47779	Unknown	Remove inapplicable RESETNXI errmsg and change to debug info
CSCec65024	Unknown	Multicast VPN not supported in -vz- images
CSCec72813	Unknown	Traceback at ipaccess_match_duplicate (CPUHOG)
CSCec89704	Unknown	Multicast not forwared in fast path with tunnel sequence-datagrams
CSCed07367	Unknown	Proton: show int serial input/output counters are 0
CSCed08725	Unknown	sonetMediumInvalidIntervals GET-NEXT returns errStat too big
CSCed12659	Unknown	LSNT:LSC crash,bad address for refcount
CSCed12722	Unknown	SVI bridge-group adversely impacts EIGRP when PIM config removed
CSCed33793	Unknown	Mcast uflow policer does not work on LAN for > certain rates
CSCed35960	Unknown	TETONS2: Ch/OC12DS0 crash when unconf/reconf MFR access uninit mem
CSCed45971	Unknown	Unexpected Exception crash when EzVPN server fails connect to RADIUS
CSCed50556	Unknown	memory leak in Crypto IKMP
CSCed66843	Unknown	dNBAR on 7500 with redundant RP causes ipc seat manager crash
CSCed72285	Unknown	IOS and CatOS have different tresholds to errdisable a port
CSCed82736	Unknown	SYS-2-GETBUF: Bad getbuffer, bytes= 65535
CSCed83129	Unknown	VIP crashed at vip_ip_fib_flow_fs when mdt receive info expires.
CSCed92374	Unknown	T/B seen on defaulting config on a range of ports
CSCed93264	Unknown	RP truncates the TOS byte to upper 3 bits on IP with option field
CSCed94829	Unknown	IOS reloads due to malformed IKE messages
CSCed95701	Unknown	HSRP incorrectly tracks 2 instances of the same interface
CSCee04176	Unknown	Mac-address-limiting inconsistent between LAN & VPLS
CSCee05413	Unknown	Memory leak in EARL VLAN stats subblock
CSCee09692	Unknown	Sup720: IPX traffic rate limited based on mls rate limiters
CSCee09820	Unknown	show mls cef exact-route displays wrong info on Sup2/MSFC2
CSCee10005	Unknown	Cat6500 service module connectivity issue with crossmodule etherchan
CSCee15581	Unknown	sss_mgr with invalid index into 2 arrays causes crash/traceback
CSCee15798	Unknown	CEF entries not installed on LC/SP after SSO switchover
CSCee20888	Unknown	ipv6 over isdn/serial and atm interfaces broken: could not ping
CSCee21730	Unknown	Array declaration on stack causes stack overflow
CSCee22045	Unknown	MSC-200-QOS: Traceback @vip_fr_update_idb_info when add/remove class
CSCee23087	Unknown	Router may reload when configured for Server Load Balancing (SLB)
CSCee27203	Unknown	IDBs getting mixed up on channelized interfaces on a PA-MC-8TE1+

Identifier	Technology	Description
CSCee32365	Unknown	MFR: LMI exchanges fail over MFR interfaces
CSCee33923	Unknown	IOS/SLB conn debugging causes dropped connections.
CSCee34121	Unknown	17aSX1: No crashinfo file for RP, SP crash @ make_ios_dnld_instance
CSCee37771	Unknown	67xx: Rommon Upgrade Failure
CSCee41186	Unknown	router crashed at ip_policy_forward
CSCee42657	Unknown	sup720 crashing after reload with large configuration
CSCee43191	Unknown	SLB TCAM entries not programmed properly after SSO
CSCee47766	Unknown	c2rls3 ATM PVC configuration lost after a switchover
CSCee49035	Unknown	mVPN: MTI uses a non-PIM interface as a Tunnel source address
CSCee49194	Unknown	MPLS echo replies need to be sent with echo req udp source port
CSCee54446	Unknown	PP: cant ping after FR PVC removed and reconfigured
CSCee55233	Unknown	Large L3 port-channel config with stats collection caused high CPU
CSCee55297	Unknown	EM: Failed to create event for applet 1: error from operarting sys
CSCee56009	Unknown	SP crashes in fibtype2fibmsg
CSCee56269	Unknown	Add support for the lowerLayerDown value for ifOperStatus
CSCee57336	Unknown	IPC-5-INVALID traceback on mlppp config in multicast
CSCee58127	Unknown	PBR become S/W when Security-ACL set up in same I/F
CSCee65993	Unknown	Command maxconns x sticky-override not saved in config
CSCee66778	Unknown	PBR: set next-hop conflict with IGP advertised /32 host route in CEF
CSCee67261	Unknown	Memory leak on crypto_ikmp_peer_create
CSCee68057	Unknown	MPLS TE Tunnel counters are not working with MPLS VPN CSC BGP+label
CSCee70024	Unknown	LSPV: Misinterpretation of the Vendor Enterprise Code TLV
CSCee70075	Unknown	after reset of module with DFC, PBR gets SW switched
CSCee70293	Unknown	FWLB: Intermittent creation of conns on a firewallfarm.
CSCee71793	Unknown	More stringent len check reqd during LSP ping/trace echo pkt decode
CSCee73959	Unknown	Need HW support for set interface null0 for Earl6 with a new CLI
CSCee75620	Unknown	RP crashes after enable CBAC
CSCee76272	Unknown	MPLS iBGP load balancing problem
CSCee77136	Unknown	sup720: SPAN dest port should not be shown as notconnected
CSCee78323	Unknown	Duplicate packets in ingress SPAN/RSPAN with 6516A or 6548-GE-TX
CSCee78451	Unknown	Native:Policing rate is not accurate with small packets
CSCee79753	Unknown	GLBP:Preempt behavior is different between each state change
CSCee85152	Unknown	CEF Hardware switching produces ping failure on every other packet a
CSCee86168	Unknown	active SP resets, sr7100 errata 11
CSCee89227	Unknown	%C6K_PLATFORM-SP-4-BADFLASH: Unsupported flash type in the bootflash
CSCee89232	Unknown	Configuring platform while in automore state crashes switch
CSCee89326	Unknown	SNMP cardType for Flexwan2 returns value for Flexwan1

Identifier	Technology	Description
CSCee91509	Unknown	Standby IP address unusable after deleting interface VLAN
CSCee92191	Unknown	PBR works in sofware if vlan id changes during linecard reloads
CSCee92719	Unknown	Duplicates in NDE on the Sup720
CSCee93286	Unknown	ipMRouteInterfaceOutMcastOctets not incrementing correctly
CSCee93511	Unknown	Chassis crash in crypto_ikmp_peer_struct_unlock with Gre/Ipsec
CSCee93931	Unknown	EEM(IOS): application ED doesnt work as expected
CSCee95301	Unknown	Unhide and document mls rate-limit multicast non-rpf command
CSCee95359	Unknown	disable aggressive aging timer for non-RPF
CSCee95708	Unknown	MSFC2-3-TOOBIG on sup720 in MPLS/VPN environment
CSCef00575	Unknown	enable cache parity for sup720
CSCef00888	Unknown	Cat6k: Need MIB support for CPU and memory info per DFC
CSCef01043	Unknown	T/B DFC3-5-INVALID: Sequence Structure Dest Port
CSCef02439	Unknown	FW2 reloads with Module failed SCP download
CSCef03290	Unknown	sh run does not display properly VLANs allowed in MWAM port
CSCef03723	Unknown	HA Coexistence:MPLS:VPN:VRFs not in sync between primary and standby
CSCef05282	Unknown	Removing IP address, IP route cache cef still allows pkts to switch.
CSCef05643	Unknown	SLB-MIB slbStickyObjectTableEntry view through SNMP not working
CSCef07848	Unknown	VRF over GRE traffic is s/w switched after remove/add mls mpl tu-rec
CSCef07965	Unknown	System crashed when accessing CVDM from the switch
CSCef08097	Unknown	IP RIB Update can hog memory after bgp flap leading to fib disable
CSCef08728	Unknown	slave default-slot config gives HA-3-SYNC_ERROR and reloads stby
CSCef09594	Unknown	CWPA2: High number of spurious interrupts increasing
CSCef09622	Unknown	CWPA2: Spurious access with show mpls cwlc-vpn adjacency
CSCef10192	Unknown	SSO: Standby failed with mismatch config on reading FW slot cache
CSCef13797	Unknown	TCAM Capacity Exceeded with ACL on POS Interface
CSCef14106	Unknown	IDSM2 stops detecting attack after 2nd failover
CSCef14780	Unknown	WCCP switch to software mode after applying redirect acl globally
CSCef14934	Unknown	link up/down message is abnormal
CSCef19894	Unknown	Tests on standby fab. cause min. error on fab-enable cards on swover
CSCef20654	Unknown	SP crashes due to Supervisor online diag failure-loading 0608 image
CSCef21575	Unknown	Sup720 - ACL Incorrectly Denies Packets in HW
CSCef23302	Unknown	Native vlan programmed wrong on pinnacle - register 0x0134
CSCef23498	Unknown	storm control config becomes invisible when channel-group configured
CSCef25427	Unknown	Improve the handling of EarlRecoveryPatchReset
CSCef25429	Unknown	NetflowTCAM test failed on Chevyslite err code 0x1,passed Chevys
CSCef25710	Unknown	EOS error handling changes
CSCef26512	Unknown	WS-X6582-2PA :Unable to read cwan<slot>/0-disk0:

Identifier	Technology	Description
CSCef26926	Unknown	VSEC:VPN-SM:router crashed in get_ipsec_attributes
CSCef27359	Unknown	SW and HW cef adjacency inconsistency
CSCef29929	Unknown	Exceed pkt count in CLI, but not count in SNMP police stats table
CSCef30308	Unknown	all zero source and dest mac address in show mls adj entry det
CSCef30392	Unknown	VPLS/PWAN2: SC CRC errors and VA length mismatch errors with traffic
CSCef32513	Unknown	SPAN destination ports causing latency on adjacent Pinnacle ports
CSCef33051	Unknown	Part of the traffic blackholed when new link joins etherchannel
CSCef33064	Unknown	PIM process took 64M of IO memory on SP, crash.
CSCef33311	Unknown	Flowcontrol inconsistency on Cat6000/Cat6500 native
CSCef34328	Unknown	Crash after the qos policy configuration
CSCef35707	Unknown	L2 Forwarding Table ECC error handler not working properly
CSCef35774	Unknown	Random DOM gbic missing in the show int tranc output
CSCef36367	Unknown	MMLS: High CPU after Sparse->Bidir transition
CSCef37026	Unknown	Running configuration is not synching between DR and NDR on MSFC3
CSCef39977	Unknown	Mac-addr static and no mac-addr static CLI allows diff portchann #s
CSCef40249	Unknown	power inline command appears even after removed and reloaded system
CSCef41934	Unknown	LSPV: LSP Ping packets processed in non-MPLS interfaces
CSCef42133	Unknown	HC counters stack in OSM POS
CSCef42312	Unknown	Ambiguous command: snmp-server enable traps config
CSCef43000	Unknown	Rockies1A SNMP:Traceback/Corrupt vlan db when set vlan 1002..1005 na
CSCef45495	Unknown	PIM Snooping: (s,g,r) prune handling cases
CSCef46652	Unknown	VPN-SM: IPSec SA encrypt counters incorrect
CSCef46923	Unknown	Group of 4 ports on WS-X6516-xx modules may stop forwarding traffic
CSCef47414	Unknown	VTP code fail to restore vlan database properly
CSCef47466	Unknown	High latency and packet drop when any interface goes down on OSM
CSCef47639	Unknown	no redirect-vserver REDIR1 crashes SUP
CSCef48810	Unknown	MAC Address entries learned via DFC3A not forwarded to SUP720
CSCef49330	Unknown	APS not working on the PA-MC-STM1
CSCef49811	Unknown	Router crashes while freeing memory in ace_hapi_pkt_proc
CSCef51783	Unknown	VPN Services Module does not report invalid SPI to MSFC
CSCef52858	Unknown	Any newly configured tunnels, makes the existing tunnels go down
CSCef53290	Unknown	Using config mls ip ids causes switch to reload unexpectedly
CSCef53846	Unknown	MVPN + MDS broken, all packets get punted.
CSCef55147	Unknown	DOM: global dom cli is broken, show int trans, returns null.
CSCef55352	Unknown	FIBDISABLE and IPC timeout after APS swithover on CHOC-12 OSM
CSCef56578	Unknown	VPNSM: traffic counter broken for GRE interface terminated on VPNSM
CSCef57019	Unknown	Some fabric svc-modules shouldnt force ingress mcast replication

Identifier	Technology	Description
CSCef57061	Unknown	PBR packets punted to RP after reloading the switch
CSCef58323	Unknown	%EARLY-L2_ASIC-DFC-SRCH_ENG_FAIL T/B on Berytos with L2(10k mac)Traf
CSCef58590	Unknown	Disable VTT major temp shutdown and change thresh 100/85 -> 115/100
CSCef62158	Unknown	V4/V6 qos display shows de-installed qos, while qos tcam is prgmd
CSCef62539	Unknown	PP:Router crash after powering linecard with mismatch wattage on PS
CSCef62936	Unknown	Spurious memory access at show_dss_command
CSCef63549	Unknown	Multicast MET management fix and increase OIF above 1023 per flow
CSCef64755	Unknown	Port Security: packet get lost when aging timer expires
CSCef65827	Unknown	GRE o/v IPSec with VPNSM intermittently loses connectivity
CSCef66632	Unknown	Demand Aging clearing entries every 4 seconds, without contention
CSCef67810	Unknown	get-bulk for portGrp causes cpu spike and delayed response
CSCef68801	Unknown	IPP rewritten to zero for rp originated packets
CSCef70083	Unknown	Spurious memory access made at ipfib_policy_forward
CSCef70298	Unknown	IFindex missing IDBs after deleting and adding T1 channels
CSCef70677	Unknown	CSG Module switches to CSM when trying to change ruleset
CSCef71913	Unknown	MVPN: 3 minutes duplication in Data-MDT (by SSM) redundancy
CSCef72013	Unknown	unicast flooding due to purging of some mac-addres entry with dfc3/pfc3
CSCef72117	Unknown	show crypto session detail enc/dec counters are reversed
CSCef72205	Unknown	vlan stops forwarding
CSCef72233	Unknown	no nat server cmd not taken into config with 12.2(18)SXD
CSCef72939	Unknown	SSO swover canot decode data desc. L1NULL0 msg when new stdby is up
CSCef73076	Unknown	ALIGN-SP-3-CORRECT seen in mcast_igmp_handle_igmp_pak
CSCef73256	Unknown	isolated pvlan not associated with VRF - packet-loss experienced
CSCef74373	Unknown	SW forced crash on cat6k
CSCef75411	Unknown	Traffic over TP tunnels stops after forced SSO switchover
CSCef75501	Unknown	dot1x authentication not work perfectly in sup720.
CSCef76161	Unknown	ifInDiscards are resetting,causing counter problems
CSCef77822	Unknown	VRF: Crypto maps not downloaded, ACE PL struck...
CSCef78235	Unknown	Disable egress span of vacl redirected packets
CSCef78240	Unknown	SIBYTE correctable ECC error should not logged at emergency level
CSCef78798	Unknown	OSM-CHOC-DS0:After rtr reload,2 interface line protocol down
CSCef79815	Unknown	OSM-CHOC-DS0:PSE incrementing on all STS.
CSCef80423	Unknown	Sup3: watchdog fired incorrectly when reload/incorrect bootup cause
CSCef81281	Unknown	The value of cbQosPoliceConformedByte64 provided by SNMP decrease
CSCef82367	Unknown	IP traff not frwded on G+CR2 port if toggled between routed/switched
CSCef82884	Unknown	Failed to delete billing plan errors
CSCef83162	Unknown	portEntPhysicalIndex not instantiated for WS-X6316-GE-TX

Identifier	Technology	Description
CSCef84129	Unknown	L2 entries not purged correctly during OIR with DFCs in the system
CSCef84162	Unknown	Should handle power glitches gracefully
CSCef85101	Unknown	VSEC:VPN-SM:HA and B2B replay update out of sync
CSCef85222	Unknown	policy based routing packet loss sup720 with reflexive access-list
CSCef86799	Unknown	ifType for ppp bcp on POS is wrong to propvirtual
CSCef86980	Unknown	CAT6500/7600 OSM egress policymap rejected without error message
CSCef88685	Unknown	mcast ltl cleared out on WS-X6816-GBIC after NSF/SSO failover
CSCef89139	Unknown	Adjacency pointers not Updated when 2nd Link Removed on 7600
CSCef92360	Unknown	Policy allowing 15 char. names, but not supported
CSCef93371	Unknown	bpduguard broken when access and voice vlan enabled
CSCef93632	Unknown	software force reload when slb swith mode
CSCef93909	Unknown	T/B c6k_proCMIB-SP-IPC_PORTOPEN_FAIL after SSO switchover
CSCef94120	Unknown	%MSFC2-3-IDB_INCORRECT_UNTHROTTLE_VECTOR
CSCeg00085	Unknown	DMVPN:multicast routing packets fail to be Txed on mGRE of 6k
CSCeg00687	Unknown	warning message needed for ip unreachables leaking to RP
CSCeg00698	Unknown	EOS-2-EOS_INT system error message is undocumented
CSCeg01297	Unknown	System crash caused by pkt of incorrect length/IP header checksum
CSCeg01510	Unknown	Device crashes when we configure no vlan <vlan nu>
CSCeg01543	Unknown	MLFR VIP crash in vip_fr_decode_encapsulation
CSCeg02873	Unknown	Netflow v9 config crashes router
CSCeg02893	Unknown	multicast traffic not being software switched with static NAT
CSCeg03423	Unknown	show int trans does not show ITU channel info for DWDM Xenpaks
CSCeg04004	Unknown	Netflow Data Export (NDE) from the SP disabled after reload
CSCeg05819	Unknown	CPP does not get applied in Hardware after reloading the router
CSCeg06292	Unknown	CPP: Traceback on attaching a service-policy to control-plane
CSCeg06570	Unknown	PA-MC-STM1: %CBUS-3-CCBCMDFAIL1: Controller 2, cmd (62 0x0000000E)
CSCeg06698	Unknown	COS rewritten for routed multicast traffic
CSCeg07617	Unknown	PP:Spurious Acesss when sh/no sh mlfr intf
CSCeg08389	Unknown	Interface counters do not increment on a Virtual MFR interface
CSCeg08562	Unknown	%IPC-3-NOBUFF: The main IPC message header cache is empty
CSCeg09655	Unknown	VPN-SM: Error in GRE check
CSCeg10174	Unknown	High CPU in QoS Mgr when changing long QoS access-list
CSCeg11883	Unknown	After RPR+ switchover standby keeps on crashing continuously
CSCeg13661	Unknown	MLS consistency-checker doesnt fix an inconsistency for (*,g)
CSCeg15192	Unknown	Increase period of statistics collection to lessen CPU load
CSCeg17132	Unknown	Sup720 inconsistency between MCAST GCE and MSC GCE datebase
CSCeg19103	Unknown	ALIGN-3-TRACEX : Error with debug netdr turned on

Identifier	Technology	Description
CSCeg19269	Unknown	gt 12L4 Oper in acl dest port doesnt expand corectly;pkts non-qos fw
CSCeg20856	Unknown	CONST-FIB: send_batched_packet() : cant allocate pak
CSCeg21028	Unknown	PFINIT-SP-1-CONFIG_SYNC_FAIL when primary attempts to sync to Sec.
CSCeg21548	Unknown	7200 crashes after link flap with 100 BFD/EIGRP sessions
CSCeg21620	Unknown	Inconsistencies in handling CSM configurations
CSCeg22198	Unknown	VSEC:VPN-SM:DF bit set will break Blade to Blade failover
CSCeg24287	Unknown	LDP does not recover after link failure between two NPEs in a networ
CSCeg26382	Unknown	wireless client not able to browse the Internet due to MSS issue
CSCeg26993	Unknown	Cat6000/Cat6500 dot1Q sub-int return incorrect SNMP statistics.
CSCeg29357	Unknown	Supw standby crashes after TestSPRPInbandPing failure
CSCeg29451	Unknown	standby and DFC in standby slot resets when doing write mem
CSCeg30437	Unknown	VPLS:ATOM:CWAN: Some VCs remain down, LFIB/TTFIB are ok
CSCeg32986	Unknown	CAT6500: Last output timestamp in show int for a SVI is never
CSCeg37929	Unknown	Unable to configure framed-ip sticky on conventional vservers
CSCeg38482	Unknown	MVPN one PE can not receive auto-RP information for one vrf
CSCeg38970	Unknown	sup720 in 7600 crashes on sh mpls l2transport hw-cap interface
CSCeg39091	Unknown	Abnormally long flooding with L2 DFC DEC
CSCeg40177	Unknown	Tag to Ip path has all zero src and dest mac
CSCeg40543	Unknown	some vcs do not pass traffic after supervisor switchover
CSCeg40801	Unknown	Configuring/Unconfiguring channel-group on SPA-T1E1 causes mem leak
CSCeg41623	Unknown	CSM:Only configured vlans should be allowed on trunk
CSCeg41762	Unknown	VPN-SM: MSFC3 sup720 crash managing the Crypto-ACE IPsec stats cache
CSCeg43854	Unknown	Taking Accounting no inservice also takes other Accounting no inserv
CSCeg45759	Unknown	Switch does not response to CDP packet with trigger TLV set
CSCeg48068	Unknown	After gige sub-int was deleted, no counters in show main interface
CSCeg48196	Unknown	Buffer overflow vulnerability in oakley_final_qm
CSCeg48512	Unknown	Out-Discard and Rcv-Octet counters increment on notconnect ports
CSCeg48547	Unknown	fm_netflow_earl6.c: early return results in memory leak
CSCeg51793	Unknown	MVPN: Address Error Exception after config change w/ Mvpn
CSCeg52076	Unknown	MVPN: crash in ip_show_mroute -> mem_lock while deleting VRFs
CSCeg52280	Unknown	CRCs caused by WS-X6704-10GE
CSCeg53985	Unknown	Cat6500 does not populate smonCapabilities correctly.
CSCeg55387	Unknown	EEM regression test composite cleanup
CSCeg55565	Unknown	MMLS/MVPN: crash at mls_earl_show_scmdb -> chunk_lock
CSCeg55846	Unknown	MSFC3 HYB: msfc3 hybrid IOS does not implement some EMT calls
CSCeg56052	Unknown	Active and Standby SP crash due to GC Entry memoryleak
CSCeg60530	Unknown	IOS crash on removing secondary vlan (pvlan configuration)

Identifier	Technology	Description
CSCeg65640	Unknown	Cat6000 with UDP turbo flood results in corrupted outgoing packets
CSCeg66729	Unknown	Memory corruption crash when setting TapStreamIpEntry (v3 cTAPMib)
CSCeg67986	Unknown	PA-POS-2OC3 interface 1 remains up/up with SLOS
CSCeg70376	Unknown	Sup720 : Ingress VSPAN is not working for VoIP VLAN
CSCeg71209	Unknown	Traceroute mpls or ping mpls cause %SCHED-3-THRASHING using SSH
CSCeg72385	Unknown	Power supply failure syslogs should have higher severity as in CatOS
CSCeg73678	Unknown	PR+:bandwidth is not guaranteed for dscp traffic
CSCeg74312	Unknown	getbulk on ciscoSlbExtMIB causes Spurious mem access and Traceback
CSCeg74597	Unknown	Further restrict power limit of CISCO7609/WS-C6509-NEB-A to 4536W
CSCeg77040	Unknown	Session Counts not decremented when processing IC
CSCeg77264	Unknown	CSM:C2R2: Resetting CSM cause system crash
CSCeg80506	Unknown	Need flowcontrol receive off support for 6704-10GE module
CSCeg82615	Unknown	Pinnacle SRAM SEL Recovery
CSCeg90349	Unknown	Both ends of the link are in loop-inc and will not recover
CSCeh05310	Unknown	ATM OSM MPB: One PVC failed to TX PKT if the LC in slot/port 1/7 of 7613
CSCeh08451	Unknown	Excessive Overruns and lbusDrops due heavy flow control over fabric
CSCeh11253	Unknown	dir /recursive all-filesystems causes supervisor to crash
CSCeh13200	Unknown	Active RP crash @ rf_proxy_fatal_error+0x60 when stby reloads
CSCeh17417	Unknown	IOS SLB not injecting VIP route when backup sfarm takes over
CSCeh43531	Unknown	CAT6K: router reloaded under stress
CSCeh50877	Unknown	Ondemand test for 144-bit fails sometimes
CSCeh51395	Unknown	Trunk vlan wont revert to the original when reconfigured
CSCin41024	Unknown	c2sup2:CWPA:DMLFR:FR Relay entry (sh fr map) is taking lot of time
CSCin65698	Unknown	%INTERFACE_API-3-NODESTROYSUBBLOCK msg on reconfiguring Potent PA
CSCin71744	Unknown	CCB_PLAYBACK and Insuff resources to create channel grp on 8TE1+
CSCin72469	Unknown	Pkts are not trusted for nbar type class though configured in HW
CSCin73206	Unknown	Ping fails on Ch-STM1 interface
CSCin74811	Unknown	user startup config rejected at bootup with > 1 acl match in Vacl
CSCin76284	Unknown	strict RPF works like strict RPF with allow default
CSCin76433	Unknown	Traceback at slb_backup_uname_fill_update
CSCin76456	Unknown	BRE Config/Unconfig IP on VLAN intf stops ARP response w/ fake MAC
CSCin76635	Unknown	SP crashes due to Supervisor online diag failure-loading 0608 image
CSCin76766	Unknown	Active SP reloads at ipc_send_rpc_blocked failed after RPR+ swover
CSCin77310	Unknown	Delete pending Src only GCE entry not deleted after SSO S/w over
CSCin77443	Unknown	HYB:HA:Slave crashes on configuring Virtual-Template interface
CSCin78110	Unknown	Some E1 controller does not come up if a large config on other LC
CSCin78137	Unknown	Traceback and %SCHED-SP-3-THRASHING on port-security

Identifier	Technology	Description
CSCin78242	Unknown	VLAN flooding when SPAN configured.
CSCin78773	Unknown	UFP not working after SSO with 6816 and uplink ports.
CSCin79691	Unknown	Hqf info. on LC disappears after LC reload/int sh-noshut
CSCin82741	Unknown	PBR does not work if both PBR & SLB are applied on same interface
CSCin82941	Unknown	Policer not programmed if module is powered on after switchover
CSCin83211	Unknown	TFTP gets terminated and RP goes to boot mode if CNTL-C given
CSCin83972	Unknown	Dot1x Scalability issue - Port from Tetons-2
CSCin84703	Unknown	Standby does not come up if active is 12.1E based software
CSCin84712	Unknown	Incorrect VMR entries programmed in TCAM for ICMP/IGMP fragments.
CSCin85077	Unknown	Inline power error-disabled interfaces do not recover at enough powe
CSCin87976	Unknown	Need to rate-limit EOS Error interrupts
CSCsa27033	Unknown	Half duplex displayed on 1000 Mbps ports
CSCsa39767	Unknown	mls ip multicast connected entries not set for secondary net after reset
CSCsa40934	Unknown	Strict priority queue drops are not accounted in output drops in sh int
CSCsa40962	Unknown	Memory leak in Crypto IKMP process on IOS EzVPN server .
CSCsa43724	Unknown	OSM-CHOC12: When changing E3 to E1, E1s stay down
CSCsa44926	Unknown	ifInNUcastPkts and ifOutNUcastPkts are missing for Vlan Interfaces
CSCsa44933	Unknown	CRONOS: MLPPP-QoS - LC crash during pxf stats update
CSCsa45335	Unknown	ESM causes memory leak in IP Input and ESM Logger
CSCsa45786	Unknown	VPN-SM: rp crash triggered by aaa_req_set_context
CSCsa46887	Unknown	LSPV: Invalid Echo Reply with Pad TLV in some scenarios
CSCsa47020	Unknown	Sup720/FlexWAN: FRF.16 drops 64 byte packets above 2Mb
CSCsa47573	Unknown	Memory leak in medium buffers
CSCsa49267	Unknown	mplsvrfIfUp trap refers to hidden instance of the ifTable
CSCsa49748	Unknown	sup720 reloads by software forced crash
CSCsa50132	Unknown	Both crypto and l3 mobility reg_add to MGRE tunnel_source_idb_change
CSCsa50515	Unknown	TTL=1 unicast may be dropped when mix TTL failure rate-limit and CoPP
CSCsa51770	Unknown	Configuration of RSPAN on 12.2(18)SXD3 causes high CPU
CSCsa53954	Unknown	Fix SB_RMON_OVRFL errmsg in sys/src-sibyte/sysctlr/msg_sb.c
CSCsa54711	Unknown	MVPN: Data MDT Encap incorrect after disable/enable ip mcast-routi CLI
CSCsa56770	Unknown	Crash during boot with: No memory available for capi_rp
CSCsa58470	Unknown	show epld slot command causes silent reload
CSCsa59260	Unknown	C7600 EoMPLS PE correctly does NOT send the COS value of BPDU
CSCsa62845	Unknown	Traffic leaks between PVLANs and Mac learning when VLAN is shutdown,
CSCsa63184	Unknown	Crash TestSPRPInbandPing fail after MLS global enable with Dist. Etherch
CSCsa65200	Unknown	Transmit power is output from admindown IF after system restart
CSCsa67836	Unknown	ct3 spa: all sequenced traffic dropped after mlp lfi bundle flap

Identifier	Technology	Description
CSCsa74464	Unknown	Bus error after config synch of CSM
CSCsa76031	Unknown	6748-GE-TX: Transmit fails on port hardcoded to 10/100/1000 or auto mode
CSCsa76137	Unknown	Komoto+Fornax:FWSM lost connectivity after sso switchover
CSCsa76290	Unknown	Inter-fabric throughput in MPLS CE to PE is much lower than 18SXD.
CSCdy64412	WAN	CE1-HYB: %CWAN_RP-4-SEMAHOG
CSCdz38539	WAN	Crash when configuring ntp
CSCdz67208	WAN	CWPA: Pkts generated on this router are not getting matched
CSCea30197	WAN	Frame Relay Autosensing with lmi-n391dte less than 3 not working
CSCea70822	WAN	SONET statistics are not saved in interval table
CSCec08821	WAN	:CWPA:FR:Output counters not updated in sh fr pvc
CSCec27867	WAN	PA-POS: Interface remains down/down when enabled with critical alarm
CSCec47371	WAN	%ALIGN-3-CORRECT:Alignment correction
CSCec69756	WAN	Not able to configure MTU under Virtual-Template.
CSCec70790	WAN	Bus error at mfr_input_control_paks
CSCed06290	WAN	Invalid host route in CEF table after changing frame-relay ip addr
CSCed52817	WAN	A removed frame-relay cmd from the config, reappear after switchover
CSCed95585	WAN	Frame relay map-class add/remove issues on subinterface
CSCee40223	WAN	ifStackTable goes into a loop if MFR subinterfaces are configured
CSCee53018	WAN	crash or alignment error in show frame lmi after delete MFR interfac
CSCee68930	WAN	MLFR bundle bounces when a local loop is is put on one T1 (2xT1 WIC)
CSCee84611	WAN	NTP Broadcast Client Fails to Sync
CSCef68547	WAN	MFR E0 6*CT3 & 2*ChOC3 bundles not recovering link removal/reconf
CSCef77523	WAN	Random MFR links stay down after reconfig or reload
CSCef82683	WAN	MFR inconsistent bundle when remove link lost
CSCef91994	WAN	FLEXWAN - PA-A3 - packet drop when ping 1500bytes with MPLS
CSCeg06304	WAN	CWPA:DRACO_SCP unsupported feature-id in SET_PORT_FEATURE msg 0x24
CSCeh34067	WAN	FlexWAN+PAs: SUP3 RP crash at mfr_set_output_seq() under stress
CSCin54713	WAN	CWAN SSO:CT3 Mailbox hogging CCB Block semaphore on bootup
CSCin73381	WAN	RBE Support on Flexwan/Flexwan2
CSCin79140	WAN	Router crahes at fr_subidb_class_add
CSCuk50643	WAN	Router reloads on setting ntp server association via snmp