# Caveats in Release 12.2(18)SXD and Rebuilds



## Open Caveats in Release 12.2(18)SXD7b

| Identifier | Technology | Description |
|---|---|---|
| CSCin77553 | ATM | ATM-IMA stops passing traffic after some time, rx_no_buffers seen |
| CSCef08790 | platform-76xx | PWAN-1:Hidden vlans overlap .1q vlans on same PWAN sub-intf |
| CSCuk41411 | Routing | HA: show cef linecard doesnt display RRP as expected |
| CSCuk49384 | Routing | Suppress t/bs for null fibidb->idb on newly active RP on SSO s/o |
| CSCeb29888 | Unknown | Bus error at chg_ipfib_excpbrg_entry |
| CSCed58661 | Unknown | High CPU due to FIB Control Task on SP |
| CSCee00311 | Unknown | Unexpected reload after clearing the routing table |
| CSCee09692 | Unknown | Sup720: IPX traffic rate limited based on mls rate limiters |
| CSCee22821 | Unknown | Bus error at stile_update_ad_tables |
| CSCee25454 | Unknown | SADB peering process leaks memory after overnight test |
| CSCee70075 | Unknown | after reset of module with DFC, PBR gets SW switched |
| CSCef20654 | Unknown | SP crashes due to Supervisor online diag failure-loading 0608 image |
| CSCef72939 | Unknown | SSO swover canot decode data desc. L1NULL0 msg when new stdby is up |
| CSCef75411 | Unknown | Traffic over TP tunnels stops after forced SSO switchover |
| CSCef77822 | Unknown | VRF: Crypto maps not downloaded, ACE PL struck... |
| CSCeg51793 | Unknown | MVPN: Address Error Exception after config change w/ Mvpn |
| CSCeg71317 | Unknown | changing CEF loadsharing to simple => all routes point to drop adj |
| CSCin78242 | Unknown | VLAN flooding when SPAN configured. |
| CSCsd98887 | Unknown | SP Memory Leak In mls-msc Process |

## Resolved Caveats in Release 12.2(18)SXD7b

### Resolved Infrastructure Caveats

- CSCsc64976—Resolved in 12.2(18)SXD7b

  A vulnerability exists in the IOS HTTP server in which HTML code inserted into dynamically generated output, such as the output from a show buffers command, will be passed to the browser requesting the page. This HTML code could be interpreted by the client browser and potentially execute malicious commands against the device or other possible cross-site scripting attacks. Successful exploitation of this vulnerability requires that a user browse a page containing dynamic content in which HTML commands have been injected.

  Cisco will be making free software available to address this vulnerability for affected customers. 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-20051201-http.html

### Resolved Management Caveats

- CSCsf07847—Resolved in 12.2(18)SXD7b

  **Symptoms:** Specifically crafted CDP packets can cause a router to allocate and keep extra memory. Exploitation of this behaviour by sending multiple specifically crafted CDP packets could cause memory allocation problems on the router.

  **Conditions:** This issue occurs in IOS images that has the fix for CSCse85200.

  **Workaround:** Disable CDP on interfaces where CDP is not required.

  **Further Problem Description:** Because CDP is a Layer-2 protocol, the symptom can only be triggered by routers that reside on the same network segment.

### Other Resolved Caveats in Release 12.2(18)SXD7b

| Identifier | Technology | Description |
|---|---|---|
| CSCse78963 | Infrastructure | adopt new default summer-time rules from EPA BADCODE BUG |
| CSCse04560 | IPServices | tftp-server allows for information disclosure . |
| CSCsd44517 | Unknown | flow control needs to be toggle off/on to become active after no shut |

## Resolved Caveats in Release 12.2(18)SXD7a

### Resolved Infrastructure Caveats

- CSCsf04754—Resolved in 12.2(18)SXD7a

  Multiple Cisco products contain either of two authentication vulnerabilities in the Simple Network Management Protocol version 3 (SNMPv3) feature. These vulnerabilities can be exploited when processing a malformed SNMPv3 message. These vulnerabilities could allow the disclosure of network information or may enable an attacker to perform configuration changes to vulnerable devices. The SNMP server is an optional service that is disabled by default. Only SNMPv3 is impacted by these vulnerabilities. Workarounds are available for mitigating the impact of the vulnerabilities described in this document.

  The United States Computer Emergency Response Team (US-CERT) has assigned Vulnerability Note VU#878044 to these vulnerabilities.

Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-0960 has been assigned to these vulnerabilities.

This advisory will be posted at

http://www.cisco.com/en/US/products/csa/cisco-sa-20080610-snmpv3.html

### Resolved LAN Caveats

- CSCsd34759—Resolved in 12.2(18)SXD7a

  **Symptom:** The VTP feature in certain versions of Cisco IOS software may be vulnerable to a crafted packet sent from the local network segment which may lead to denial of service condition.

  **Conditions:** The packets must be received on a trunk enabled port.

  **Further Information** :On the 13th September 2006, Phenoelit Group posted an advisory containing three vulnerabilities:

  - VTP Version field DoS
  - Integer Wrap in VTP revision
  - Buffer Overflow in VTP VLAN name

  These vulnerabilities are addressed by Cisco IDs:

  - CSCsd52629/CSCsd34759 -- VTP version field DoS
  - CSCse40078/CSCse47765 -- Integer Wrap in VTP revision
  - CSCsd34855/CSCei54611 -- Buffer Overflow in VTP VLAN name

  Cisco's statement and further information are available on the Cisco public website at

  http://www.cisco.com/en/US/products/csr/cisco-sr-20060913-vtp.html

### Resolved Routing Caveats

- CSCsd40334—Resolved in 12.2(18)SXD7a

  Processing a specially crafted IPv6 Type 0 Routing header can crash a device running Cisco IOS software. This vulnerability does not affect IPv6 Type 2 Routing header which is used in mobile IPv6. IPv6 is not enabled by default in Cisco IOS.

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

  There are workarounds available to mitigate the effects of the vulnerability. The workaround depends on if Mobile IPv6 is used and what version on Cisco IOS is being currently used.

  This advisory is posted at

  http://www.cisco.com/en/US/products/csa/cisco-sa-20070124-IOS-IPv6.html

- CSCec71950—Resolved in 12.2(18)SXD7a

  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

### Resolved Unknown Caveats

- CSCsb52717—Resolved in 12.2(18)SXD7a

  **Symptom:** A Cisco router configured for multicast VPN may reload after receiving a malformed MDT data group join packet.

  **Conditions:** Affects all IOS versions that support mVPN MDT.

  **Workaround:** Filter out MDT Data Join messages from the router sending the malformed packet using a Receive Access Control List (rACL) feature. Note by doing this, the offending router will not be able to participate within the mVPN data trees.

  The following example shows how to block malformed MDT Data Join messages that are sent from the device's IP addresses using a receive ACL:

  ```
  !
  ip receive access-list 111
  !
  access-list 111 deny udp host <ip address of router sending malformed join
  request> host 224.0.0.13 eq 3232
  access-list 111 permit ip any any
  !
  ```

  **Note:** Ensure that the rACL does not filter critical traffic such as routing protocols or interactive access to the routers. Filtering necessary traffic could result in an inability to remotely access the router, thus requiring a console connection. For this reason, lab configurations should mimic the actual deployment as closely as possible.

  As always, Cisco recommends that you test this feature in the lab prior to deployment. For more information on rACLs, refer to "Protecting Your Core: Infrastructure Protection Access Control Lists" at

  http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a0a5e.shtml.

- CSCsd75273—Resolved in 12.2(18)SXD7a

  Cisco Catalyst 6500, 6500 series and Cisco 7600 series that have a Network Analysis Module installed are vulnerable to an attack, which could allow an attacker to gain complete control of the system. Only Cisco Catalyst systems that have a NAM on them are affected. This vulnerability affects systems that run Internetwork Operating System (IOS) or Catalyst Operating System (CatOS).

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

  A Cisco Security Advisory for this vulnerability is posted at
  http://www.cisco.com/en/US/products/csa/cisco-sa-20070228-nam.html

- CSCse52951—Resolved in 12.2(18)SXD7a

  Cisco Catalyst 6500, 6500 series and Cisco 7600 series that have a Network Analysis Module installed are vulnerable to an attack, which could allow an attacker to gain complete control of the system. Only Cisco Catalyst systems that have a NAM on them are affected. This vulnerability affects systems that run Internetwork Operating System (IOS) or Catalyst Operating System (CatOS).

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

  A Cisco Security Advisory for this vulnerability is posted at

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

#### Resolved Voice Caveats

- CSCsc60249—Resolved in 12.2(18)SXD7a

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

  This advisory is posted at

  http://www.cisco.com/en/US/products/csa/cisco-sa-20070808-IOS-voice.html.

#### Other Resolved Caveats in Release 12.2(18)SXD7a

| Identifier | Technology | Description |
|---|---|---|
| CSCsb11698 | AAA | Input Queue Wedge with TACACs |
| CSCsd34855 | LAN | VTP update with a VLAN name >100 characters causes buffer overflow . |
| CSCsc72722 | Security | CBAC - firewall resets TCP idle timer upon receiving invalid TCP packets |
| CSCej21698 | Unknown | EARL_L2_ASIC- SRCH_ENG_FAIL/ SCHED-DFC9-3-STILLWATCHING |
| CSCse73539 | Unknown | c7600 - crash of active sup720 after inserting a second one |

## Resolved Caveats in Release 12.2(18)SXD7

#### Resolved AAA Caveats

- CSCed09685—Resolved in 12.2(18)SXD7

  **Symptoms:** When command accounting is enabled, Cisco IOS routers will send the full text of each command to the ACS server. Though this information is sent to the server encrypted, the server will decrypt the packet and log these commands to the logfile in plain text. Thus sensitive information like passwords will be visible in the server's log files.

  **Conditions:** This problem happens only with command accounting enabled.

  **Workaround:** Disable command accounting.

### Other Resolved Caveats in Release 12.2(18)SXD7

| Identifier | Technology | Description |
|---|---|---|
| CSCsb09190 | MPLS | Next-hop label missing for non-vpn prefixes with dual RRs |
| CSCed94829 | Unknown | IOS reloads due to malformed IKE messages |
| CSCee84918 | Unknown | DHCP snooping on 3550 drops DHCPNAKs recieved when renewing old IP |
| CSCef66632 | Unknown | Demand Aging clearing entries every 4 seconds, without contention |
| CSCei37672 | Unknown | chevys/c2lc take ~ 180s before resetting following a mandatory proc exit |
| CSCsb12076 | Unknown | VPN-SM: GRE RP pkts coming to IPSec with tvlan causing route flaps |
| CSCsb50559 | Unknown | Need fix for MWAM for CSCee10005 |
| CSCsb98702 | Unknown | Breakpoint (signal 5 exception) when ltl profiling . |

## Resolved Caveats in Release 12.2(18)SXD6

| Identifier | Technology | Description |
|---|---|---|
| CSCdt12296 | QoS | RSVP Path message packets are process switched when data is CEF swit |
| CSCeh73049 | Unknown | tclsh mode bypasses aaa command authorization check |
| CSCei76358 | Unknown | cleanup of user interface data |

## Resolved Caveats in Release 12.2(18)SXD5

### Resolved AAA Caveats

- CSCee45312—Resolved in 12.2(18)SXD5

  Remote Authentication Dial In User Service (RADIUS) authentication on a device that is running certain versions of Cisco Internetworking Operating System (IOS) and configured with a fallback method to none can be bypassed.

  Systems that are configured for other authentication methods or that are not configured with a fallback method to none are not affected.

  Only the systems that are running certain versions of Cisco IOS are affected. Not all configurations using RADIUS and none are vulnerable to this issue. Some configurations using RADIUS, none and an additional method are not affected.

  Cisco has made free software available to address this vulnerability. There are workarounds available to mitigate the effects of the vulnerability.

  More details can be found in the security advisory which posted at the following URL http://www.cisco.com/en/US/products/csa/cisco-sa-20050629-aaa.html

### Resolved Unknown Caveats

- CSCsa67611—Resolved in 12.2(18)SXD5

  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.

### Other Resolved Caveats in Release 12.2(18)SXD5

| Identifier | Technology | Description |
|---|---|---|
| CSCsa74002 | AAA | Input queue - wedged when traffic punted to the CPU |
| CSCeg19038 | Infrastructure | The entCacheFlag should not be shared with several entity tables. |
| CSCeg64124 | Infrastructure | SAA not sending packets to line after a period of time |
| CSCin53807 | Infrastructure | Warm Reboot Decompression may fail for certain images |
| CSCeb47150 | LegacyProtocols | Unable to Establish DLSw Peer Connection Through VPN/NAT Tunnel |
| CSCeg28814 | Multicast | Duplicated mcast packet due to wrong FPOE in egress replication mode |
| CSCee24349 | QoS | Crash at fib_post_download_processing when reloading |
| CSCeg49010 | QoS | ISIS updates not sent when output qos police is set |
| CSCsa57155 | QoS | nbar makes RP in cat6k crash with memory corruption when doing sso |
| CSCeg62496 | Routing | Type-3 lsa not generated if Type-1 flaps coming from multiple areas |
| CSCeh13489 | Routing | BGP shouldn't propogate an update w excessive AS Path > 255 |
| CSCin84644 | Routing | Routes are not seen on neighbors after switchover on eigrp stub rtr |
| CSCsa74271 | Routing | OSPF NSF not working, traffic drops for a few seconds |
| CSCsa78259 | Routing | IOS reload due to specific BGP routing update |
| CSCsa80861 | Routing | BGP to IGP redistribution broken with mutual redistribution points |
| CSCec22308 | Security | mem allocated at PKI_ParseX500Dn(0x6207eb2c)+0x34 was leaked |
| CSCec32184 | Security | RSA-SIG IKE leaks memory |
| CSCee10005 | Unknown | Cat6500 service module connectivity issue with crossmodule etherchan |
| CSCee37771 | Unknown | 67xx: Rommon Upgrade Failure |
| CSCee78451 | Unknown | Native:Policing rate is not accurate with small packets |
| CSCee82867 | Unknown | Changing dot1x host-mode = multi causes An unknown operational error |
| CSCef10010 | Unknown | Ca6K - input errors on dot1Q trunks for pkts larger than 1496 |
| CSCef36367 | Unknown | MMLS: High CPU after Sparse->Bidir transition |
| CSCef56578 | Unknown | VPNSM: traffic counter broken for GRE interface terminated on VPNSM |
| CSCef82367 | Unknown | IP traff not frwded on G+CR2 port if toggled between routed/switched |
| CSCef93632 | Unknown | software force reload when slb swith mode |
| CSCeg11883 | Unknown | After RPR+ switchover standby keeps on crashing continuously |
| CSCeg56052 | Unknown | Active and Standby SP crash due to GC Entry memoryleak |

| Identifier | Technology | Description |
|---|---|---|
| CSCeg62365 | Unknown | rxHCDropEvents incrementing on 6704-10GE interface |
| CSCeh08451 | Unknown | Excessive Overruns and lbusDrops due heavy flow control over fabric |
| CSCeh29617 | Unknown | PP:Sup3:FRoMPLS:CHOC:pkts dropped on egr (PE-CE)link (ping fails) |
| CSCeh54533 | Unknown | IOS SLB with Egress ACL under SVI breaks L2 icmp traffic |
| CSCeh62522 | Unknown | igmp snooping source only doesnt work for certain range of group ad |
| CSCsa65200 | Unknown | Transmit power is output from admindown IF after system restart |
| CSCsa70835 | Unknown | SUp720 may see random packet loss when host leaves or joins; OIF +- 85 |
| 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 |
| CSCsa77211 | Unknown | Memory Corruption triggered while adding Microflow Policer ACL |
| CSCsa80358 | Unknown | Connectivity lost on native vlan on etherchannel trunk betn 2 cat6ks |
| CSCsa85123 | Unknown | Cisco 7609 :OSM-1CHOC12DS0-SI :RFI bit should be undefined for VC-12 |
| CSCsa87388 | Unknown | cat6000 : ciscoEnvMonTempStatusChangeNotif  to many traps - VDB inlet |
| CSCsa88102 | Unknown | Crash on Cat6K/Sup720 running 12.2(18)SXD3 due to the memory leak (FIB) |

## Resolved Caveats in Release 12.2(18)SXD4

### Resolved LAN Caveats

- CSCsa67294—Resolved in 12.2(18)SXD4

  **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)SXD4

  **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)SXD4

  **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 Routing Caveats

- CSCef68324—Resolved in 12.2(18)SXD4

  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)SXD4

  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.

CSCef60659—Resolved in 12.2(18)SXD4

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.

- CSCef67682—Resolved in 12.2(18)SXD4

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 Unknown Caveats

- CSCee59999—Resolved in 12.2(18)SXD4

  **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.

- CSCef44225—Resolved in 12.2(18)SXD4

  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)SXD4

| Identifier | Technology | Description |
|---|---|---|
| CSCin84694 | ATM | Workaround fix for PA-A3/A6 SAR hardware issue |
| CSCin86455 | ATM | PA-A3/A6: Performance optimization and code cleanup |
| CSCeh13292 | Content | WCCP Multiple Configurations causes high CPU |
| CSCed63357 | Infrastructure | show disk#: and dir disk#: inconsistent |
| CSCee91044 | Infrastructure | SNMP Trap Sent In Error Upon Every IKE Lifetime Expiry |
| CSCea25073 | IPServices | IOS FTP client code rewrite |
| CSCec50485 | IPServices | copy ftp flash fails with 3COM ftpserver |

| Identifier | Technology | Description |
|---|---|---|
| CSCeg73883 | Management | cikePeerLocalAddr is not augmenting properly |
| CSCdu28706 | MPLS | ARP rejects requests from interfaces in different vrfs |
| CSCdz85325 | MPLS | TFIB not get updated after delete and re-add static route |
| CSCef37186 | MPLS | cpuhog/watchdog-crash on mplsXCIndexNext mib query |
| CSCeg27836 | MPLS | suspect vrf leak following foreign ebgp flap |
| CSCeg90033 | MPLS | Missing labels in MPLS/VPN forwarding table |
| CSCsa53117 | MPLS | MLS cef hardware Freeze |
| CSCef60452 | Multicast | possible blackout when receiving Join on RPF interface (iif) |
| CSCeg47780 | platform-76xx | RFC1483 Bridging broken on BT |
| CSCef66517 | QoS | packet drop on flexwan when traffic shaping |
| CSCdv76375 | Routing | OSPF neighbor command unsupported in VPN routing instance |
| CSCed59370 | Routing | OSPF Type 5 LSA not updated when forwarding address changes |
| CSCef50427 | Routing | System crashed when show ip bgp XX. |
| CSCef65500 | Routing | ospf_db_timer_tick  cpuhog process OSPF |
| CSCef93215 | Routing | router crash at ospf_build_one_paced_update |
| CSCeg07725 | Routing | EIGRP redistributing BGP inconsistently after BGP topology changes |
| CSCeh07809 | Routing | BGP leaves a stale CEF entry |
| CSCeh12233 | Routing | 12.2SX: fibtype2fibmsg crash - backout CSCef30577 |
| CSCeh15802 | Routing | OSPF vrf config lost after reload |
| CSCsa40588 | Routing | Routes are not withdrawn from routing table after BGP routes are removed |
| CSCsa55048 | Routing | Static exported in vrf has wrong cef entry |
| CSCsa59600 | Routing | IPSec PMTUD not working [after CSCef44225] |
| CSCdu83050 | Security | ssh needs source-address |
| CSCef67660 | Security | sshv2 malform client ignore msg cause demage to router |
| CSCef98116 | Security | cat6500 12.2SX: SSH issues with privilege levels |
| CSCeb79090 | Unknown | snmp getmany of ciscoFlashFileTable crash the 7300 device |
| CSCed82736 | Unknown | SYS-2-GETBUF: Bad getbuffer, bytes= 65535 |
| CSCee67261 | Unknown | Memory leak on crypto_ikmp_peer_create |
| CSCef72013 | Unknown | unicast flooding due to purging of some mac-addres entry with dfc3/pfc3 |
| CSCef82884 | Unknown | Failed to delete billing plan errors |
| CSCef92360 | Unknown | Policy allowing 15 char. names, but not supported |
| CSCef93371 | Unknown | bpduguard broken when access and voice vlan enabled |
| CSCef96465 | Unknown | WS-X6704-10GE port shows up/up state while other side is shutdown |
| CSCeg16684 | Unknown | Some VPLS VCs fail to pass traffic after a link failure in the core |
| CSCeg26993 | Unknown | Cat6000/Cat6500 dot1Q sub-int return incorrect SNMP statistics. |
| CSCeg30437 | Unknown | VPLS:ATOM:CWAN: Some VCs remain down, LFIB/TTFIB are ok |
| CSCeg40543 | Unknown | some vcs do not pass traffic after supervisor switchover |

| Identifier | Technology | Description |
|---|---|---|
| CSCeg41623 | Unknown | CSM:Only configured vlans should be allowed on trunk |
| CSCeg48068 | Unknown | After gige sub-int was deleted, no counters in show main interface |
| CSCeg49196 | Unknown | Excessive Overruns and lbusDrops due heavy flow control over fabric |
| CSCeg51616 | Unknown | Bus error crash at adjacency_compute_hash |
| CSCeg67986 | Unknown | PA-POS-2OC3 interface 1 remains up/up with SLOS |
| CSCeg70376 | Unknown | Sup720 : Ingress VSPAN is not working for VoIP VLAN |
| CSCeg77040 | Unknown | Session Counts not decremented when processing IC |
| CSCeh05310 | Unknown | ATM OSM MPB: One PVC failed to TX PKT if the LC in slot/port 1/7 of 7613 |
| CSCeh13200 | Unknown | Active RP crash @ rf_proxy_fatal_error+0x60 when stby reloads |
| CSCin87976 | Unknown | Need to rate-limit EOS Error interrupts |
| CSCsa51770 | Unknown | Configuration of RSPAN on 12.2(18)SXD3 causes high CPU |
| CSCsa57079 | Unknown | C7600 PE does NOT send BPDU including dot1Q tag on EoMPLS |
| CSCsa59260 | Unknown | C7600 EoMPLS PE correctly does NOT send the COS value of BPDU |

## Resolved Caveats in Release 12.2(18)SXD3

### Resolved Unknown Caveats

- CSCef90002—Resolved in 12.2(18)SXD3

  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

### Other Resolved Caveats in Release 12.2(18)SXD3

| Identifier | Technology | Description |
|---|---|---|
| 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 |
| CSCef01725 | Infrastructure | pak_realign driving up CPU usage |
| CSCeg11566 | Infrastructure | SNMP May Consume all the I/O Memory |
| CSCed82551 | IPServices | VRRP: problem with dynamic reconfiguration of secondary IP addresses |
| CSCin83554 | Management | CDP doesnt propogates MWAM to Supervisor with 12.2(18)SXD1 image |
| CSCec10116 | MPLS | MPLS VPN PE uses global addresses on some packets originated in VRF |
| CSCed57281 | MPLS | CPU hog in CEF reloader while adding a vrf interface |
| CSCee37430 | MPLS | Missing LFIB tag rewrite on LC after loss of /32 entry to its next-hop |
| CSCef14446 | MPLS | mpls vpn: recirculation vlan for agg label is not mapped to vpn |

| Identifier | Technology | Description |
|---|---|---|
| CSCef80349 | MPLS | GSR midpoint rejects RESV after link flap |
| CSCeg03885 | MPLS | TE label missed on MPLS TE tunnel |
| CSCsa44122 | MPLS | Missing cef table and data structure error after deleting VRF |
| CSCef12304 | platform-76xx | PWAN2:Connectivity is broken between GE-WAN if one end shut/no shut |
| CSCef35398 | platform-76xx | OSM-2OC12-ATM-SI+ - SRIC IPM parity error |
| 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 |
| CSCeg03144 | platform-76xx | %EARL_L2_ASIC-SP-4-L2L3_SEQ_ERR on Sup720 |
| CSCeg10236 | platform-76xx | PWAN2:GBIC type shown as not connected in show int |
| CSCee22810 | QoS | Router stops sending LMI with QOS configured |
| CSCef06034 | QoS | Sup720 crashes after SSO Failover with nbar configured |
| CSCef47829 | QoS | Physical int out of BW: no error message that MQC policy cant apply |
| CSCed63342 | Routing | RIP-Unicast updates not sent to configured RIP neighbors |
| CSCed63876 | Routing | BGP: router crashes pointing to ed_decay_penalty |
| CSCee59315 | Routing | MPLS-VPN:Corrupted BGP table showing stale and/or poisoned paths |
| CSCee85202 | Routing | Long delay for vrf to be removed from vrf table when un-configured |
| CSCee88898 | Routing | ALIGN-3-SPURIOUS in show_ipprotocol |
| CSCef08797 | Routing | static routes not advertised to BGP peers |
| CSCef69650 | Routing | Spurious memory access during SNMP MIB walk |
| CSCef89294 | Routing | MPLS VPN EIBGP: Missing some multipath routes |
| CSCeg05830 | Routing | BGP: Update peer-group remove-private-as functionality |
| CSCeg08344 | Routing | with cef/dcef enabled & compression on, tcp frames getting dropped |
| CSCeg26378 | Routing | Dest CEF entry is missing in DCEF table.  All pkts are punted to RP. |
| CSCeg31951 | Routing | BGP: Put peers with as-override & rem-pvt-as in separate updgrps |
| CSCec00930 | Unknown | bus error at crypto_ipsec_clear_peer_sas |
| CSCed07367 | Unknown | Proton: show int serial input/output counters are 0 |
| CSCed25505 | Unknown | reset of csm causes one of WS-X6248A-TEL to reset in a chassis |
| CSCed45971 | Unknown | Unexpected Exception crash when EzVPN server fails connect to RADIUS |
| CSCee03625 | Unknown | FWSM:VFW: Jumbo frames dont make across through the fwsm |
| CSCee32365 | Unknown | MFR: LMI exchanges fail over MFR interfaces |
| CSCee55233 | Unknown | Large L3 port-channel config with stats collection caused high CPU |
| CSCee86168 | Unknown | active SP resets, sr7100 errata 11 |
| CSCef27359 | Unknown | SW and HW cef adjacency inconsistency |
| CSCef35707 | Unknown | L2 Forwarding Table ECC error handler not working properly |
| CSCef37026 | Unknown | Running configuration is not synching between DR and NDR on MSFC3 |
| CSCef42312 | Unknown | Ambiguous command:  snmp-server enable traps config |

| Identifier | Technology | Description |
|---|---|---|
| CSCef47466 | Unknown | High latency and packet drop when any interface goes down on OSM |
| CSCef48810 | Unknown | MAC Address entries learned via DFC3A not forwarded to SUP720 |
| CSCef53290 | Unknown | Using config mls ip ids causes switch to reload unexpectedly |
| CSCef58323 | Unknown | %EARLY-L2_ASIC-DFC-SRCH_ENG_FAIL T/B on Berytos with L2(10k mac)Traf |
| CSCef58932 | Unknown | VACL filter out STP BPDU |
| CSCef70298 | Unknown | IFindex missing IDBs after deleting and adding T1 channels |
| CSCef79592 | Unknown | Class-default shows packets output 0; packet drops 0 |
| CSCef82309 | Unknown | Cache error caused standby SP crashed @ data_cache_inv after reload |
| CSCef87392 | Unknown | Giants incorrectly counted on trunk with 67xx modules |
| CSCef88685 | Unknown | mcast ltl cleared out on WS-X6816-GBIC after NSF/SSO failover |
| CSCef91572 | Unknown | Software forced crash at process pm_mp_notify_cp_port_admin_state |
| CSCef95365 | Unknown | Crash with Real cache error detected on show platform asicreg |
| CSCeg01297 | Unknown | System crash caused by pkt of incorrect length/IP header checksum |
| CSCeg01510 | Unknown | Device crashes when we configure no vlan <vlan nu> |
| CSCeg02873 | Unknown | Netflow v9 config crashes router |
| CSCeg06570 | Unknown | PA-MC-STM1: %CBUS-3-CCBCMDFAIL1: Controller 2, cmd (62 0x0000000E) |
| CSCeg06698 | Unknown | COS rewritten for routed multicast traffic |
| CSCeg08389 | Unknown | Interface counters do not increment on a Virtual MFR interface |
| CSCeg19269 | Unknown | gt 12L4 Oper in acl dest port doesnt expand corectly;pkts non-qos fw |
| 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 |
| CSCeg24675 | Unknown | cannot modify class-map in PQ when plicy is applied to OSM |
| CSCeg26382 | Unknown | wireless client not able to browse the Internet due to MSS issue |
| CSCeg31792 | Unknown | Sup2 crash with AGSM |
| CSCeg40177 | Unknown | Tag to Ip path has all zero src and dest mac |
| CSCeg41762 | Unknown | VPN-SM: MSFC3 sup720 crash managing the Crypto-ACE IPsec stats cache |
| CSCeg43827 | Unknown | At duplex half and speed 10, RCP failed to copy image. |
| CSCeg43854 | Unknown | Taking Accounting no inservice also takes other Accounting no inserv |
| CSCej52641 | Unknown | LCP_FW_ERR: 67xx linecards reset due to packet buffer P2N EEC1 error |
| CSCin65698 | Unknown | %INTERFACE_API-3-NODESTROYSUBBLOCK msg on reconfiguring Potent PA |
| CSCin83972 | Unknown | Dot1x Scalability issue - Port from Tetons-2 |
| CSCin84750 | Unknown | IP address in ACE ignored while doing l4op expansion |
| CSCsa40962 | Unknown | Memory leak in Crypto IKMP process on IOS EzVPN server . |
| CSCef91994 | WAN | FLEXWAN - PA-A3 - packet drop when ping 1500bytes with MPLS |
| CSCef93103 | WAN | bridge-vlan on Flexwan PVC floods BPDUs |

## Resolved Caveats in Release 12.2(18)SXD2

### Resolved Routing Caveats

- CSCee67450—Resolved in 12.2(18)SXD2

  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

### Other Resolved Caveats in Release 12.2(18)SXD2

| Identifier | Technology | Description |
|---|---|---|
| CSCea19918 | Routing | BGP: need to do multipath with different as-paths |
| CSCef63549 | Unknown | Multicast MET management fix and increase OIF above 1023 per flow |
| CSCef70677 | Unknown | CSG Module switches to CSM when trying to change ruleset |
| CSCef72205 | Unknown | vlan stops forwarding |
| CSCef73076 | Unknown | ALIGN-SP-3-CORRECT seen in mcast_igmp_handle_igmp_pak |
| CSCef82797 | Unknown | Distributed EtherChannel may caused packet loss |
| CSCef89139 | Unknown | Adjacency pointers not Updated when 2nd Link Removed on 7600 |
| CSCef95789 | Unknown | Switch Interfaces stop forwarding Traffic |
| CSCeg05819 | Unknown | CPP does not get applied in Hardware after reloading the router |
| CSCin82979 | Unknown | Flow mask changed from full flow to destination on switchover |

## Resolved Caveats in Release 12.2(18)SXD1

### Resolved IPServices Caveats

- CSCed78149—Resolved in 12.2(18)SXD1

  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 Routing Caveats

- CSCef48336—Resolved in 12.2(18)SXD1

  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

### Resolved Unknown Caveats

- CSCin82407—Resolved in 12.2(18)SXD1

  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

### Other Resolved Caveats in Release 12.2(18)SXD1

| Identifier | Technology | Description |
|---|---|---|
| CSCed88768 | AAA | console/vty/telnet password fails after upgrade to 12.2(18)S images |
| CSCee82681 | Access | Counter: Counters stuck on serial interface |
| 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+ |
| CSCin79468 | ATM | ATM SSO: PVC state not in sync between active/sdby after a sh/no-sh |
| CSCeb28941 | Content | IOS NAT and WCCP do not work together |
| CSCef46191 | IPServices | Unable to telnet |
| CSCin78000 | IPServices | LDP session in xmit state if MPLS flapped at high traffic on L2 SUP3 |
| CSCed21063 | MPLS | TE Tunnel Destination Label Missing |
| CSCed54416 | MPLS | GRP crash in tfib when pos fiber is disconnected or connected |
| CSCef25866 | MPLS | Blackholing of traffic during FRR reconnect with invalid cache adj |
| CSCed19898 | platform-76xx | :ATMoMPLS VCs freeze/vanallen error/w toggling core loopback |
| CSCee72817 | platform-76xx | BGP neighbor relationship flaps periodically between PEs and RRs |
| CSCef12193 | platform-76xx | FABRIC-SP-6-TIMEOUT_ERR: Fabric in slot 8 reported timeout error |
| CSCef63516 | platform-76xx | OSM crash: POSLC-3-SOP: TxSOP-0 SOP. (source=0x1, halt_minor0=0x8002 |
| CSCef83690 | platform-76xx | FRoMPLS:Connectivity broken if the ping packet size is < 58 byte |
| CSCee85257 | PPP | cRTP does not work with CEF on FlexWAN controller. |
| CSCef44786 | PPP | ATMPA-3-BADVCD seen when running MLPPP at low speed |
| CSCec22723 | Routing | Router may reload unexpectedly due to ISPF(OSPF) |
| CSCec82398 | Routing | BGP needs to modify a route instead of delete/add |
| CSCed36386 | Routing | APS:Ping fail on alternate packets after revertive switching |
| CSCed77612 | Routing | network option missing in isis interface command |
| CSCee43166 | Routing | BGP: reduce CPU load for processing inbound VPNv4 updates |
| CSCef44976 | Routing | MPLS traffic not forwarded from 1 vlan in multi vlan vrf |
| CSCdy33703 | Unknown | Need span support for port 1/4 & 1/3 |
| CSCee42657 | Unknown | sup720 crashing after reload with large configuration |
| CSCee43191 | Unknown | SLB TCAM entries not programmed properly after SSO |

| Identifier | Technology | Description |
|---|---|---|
| CSCee54446 | Unknown | PP: cant ping after FR PVC removed and reconfigured |
| CSCee68057 | Unknown | MPLS TE Tunnel counters are not working with MPLS VPN CSC BGP+label |
| CSCee70293 | Unknown | FWLB: Intermittent creation of conns on a firewallfarm. |
| CSCee75620 | Unknown | RP crashes after enable CBAC |
| CSCee83655 | Unknown | CPU_MONITOR-2-NOT_RUNNING_TB: CPU_MONITOR tracebackrate_limit_loop |
| CSCee93511 | Unknown | Chassis crash in crypto_ikmp_peer_struct_unlock with Gre/Ipsec |
| CSCee95708 | Unknown | MSFC2-3-TOOBIG on sup720 in MPLS/VPN environment |
| CSCef02439 | Unknown | FW2 reloads with Module failed SCP download |
| CSCef07017 | Unknown | VACL is not working for RSPAN traffic with mcast enabled |
| CSCef07848 | Unknown | VRF over GRE traffic is s/w switched after remove/add mls mpl tu-rec |
| CSCef08097 | Unknown | IP RIB Update can hog memory after bgp flap leading to fib disable |
| 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 |
| CSCef21575 | Unknown | Sup720 - ACL Incorrectly Denies Packets in HW |
| CSCef23843 | Unknown | Module reset in getting CBL info |
| CSCef25710 | Unknown | EOS error handling changes |
| CSCef26512 | Unknown | WS-X6582-2PA :Unable to read cwan<slot>/0-disk0: |
| CSCef26926 | Unknown | VSEC:VPN-SM:router crashed in get_ipsec_attributes |
| CSCef30308 | Unknown | all zero source and dest mac address in show mls adj entry det |
| CSCef41228 | Unknown | SSO failover causes WS-X6816-GBIC reset |
| CSCef43000 | Unknown | Rockies1A SNMP:Traceback/Corrupt vlan db when set vlan 1002..1005 na |
| CSCef47414 | Unknown | VTP code fail to restore vlan database properly |
| CSCef47639 | Unknown | no redirect-vserver REDIR1 crashes SUP |
| CSCef49330 | Unknown | APS not working on the PA-MC-STM1 |
| CSCef49811 | Unknown | Router crashes while freeing memory in ace_hapi_pkt_proc |
| CSCef52858 | Unknown | Any newly configured tunnels, makes the existing tunnels go down |
| CSCef65249 | Unknown | VPN-SM: ACE crashes with certain class of ACL |
| CSCef65827 | Unknown | GRE o/v IPSec with VPNSM intermittently loses connectivity |
| CSCef67810 | Unknown | get-bulk for portGrp causes cpu spike and delayed response |
| CSCef72233 | Unknown | no nat server cmd not taken into config with 12.2(18)SXD |
| CSCef75924 | Unknown | packet drop for L3 trafic over dist. etherchannel with SPAN enabled |
| CSCef78235 | Unknown | Disable egress span of vacl redirected packets |
| CSCin74811 | Unknown | user startup config rejected at bootup with > 1 acl match in Vacl |
| 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 |

| Identifier | Technology | Description |
|---|---|---|
| CSCin78773 | Unknown | UFP not working after SSO with 6816 and uplink ports. |
| CSCef60434 | WAN | Need to prevent hyperion reset on receiving corrupt packets |