

Caveats in Release 12.2(17d)SXB and Rebuilds

- [Open Caveats in Release 12.2\(17d\)SXB11a, page 389](#)
- [Resolved Caveats in Release 12.2\(17d\)SXB11a, page 389](#)
- [Resolved Caveats in Release 12.2\(17d\)SXB11, page 390](#)
- [Resolved Caveats in Release 12.2\(17d\)SXB10, page 390](#)
- [Resolved Caveats in Release 12.2\(17d\)SXB9, page 391](#)
- [Resolved Caveats in Release 12.2\(17d\)SXB8, page 392](#)
- [Resolved Caveats in Release 12.2\(17d\)SXB7, page 394](#)
- [Resolved Caveats in Release 12.2\(17d\)SXB6, page 397](#)
- [Resolved Caveats in Release 12.2\(17d\)SXB5, page 398](#)
- [Resolved Caveats in Release 12.2\(17d\)SXB4, page 401](#)
- [Resolved Caveats in Release 12.2\(17d\)SXB3, page 402](#)
- [Resolved Caveats in Release 12.2\(17d\)SXB2, page 402](#)
- [Resolved Caveats in Release 12.2\(17d\)SXB1, page 404](#)
- [Resolved Caveats in Release 12.2\(17d\)SXB, page 406](#)



Note

Release 12.2(17d)SXB1 and later releases do not support XENPAK-10GB-ER units with Part No. 800-24557-01, as described in this external field notice (CSCee47030):

<http://www.cisco.com/en/US/ts/fn/200/fn29736.html>

Open Caveats in Release 12.2(17d)SXB11a

Identifier	Technology	Description
CSCee30050	Routing	FIB-3-FIBDISABLE Fatal error, no window message, LC to RP IPC non-op

Resolved Caveats in Release 12.2(17d)SXB11a

Resolved Routing Caveats

- [CSCec71950](#)—Resolved in 12.2(17d)SXB11a

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>

Other Resolved Caveats in Release 12.2(17d)SXB11a

Identifier	Technology	Description
CSCej21698	Unknown	EARL_L2_ASIC- SRCH_ENG_FAIL/ SCHED-DFC9-3-STILLWATCHING
CSCsb98702	Unknown	Breakpoint (signal 5 exception) when ltl profiling .
CSCsd50224	Unknown	FW: C2 fabric firmware improvements for Tetons3
CSCsd50881	Unknown	New fabric error recovery for 17SXB

Resolved Caveats in Release 12.2(17d)SXB11

Resolved AAA Caveats

- [CSCed09685](#)—Resolved in 12.2(17d)SXB11

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(17d)SXB11

Identifier	Technology	Description
CSCef87392	Unknown	Giants incorrectly counted on trunk with 67xx modules
CSCej52641	Unknown	LCP_FW_ERR: 67xx linecards reset due to packet buffer P2N EEC1 error
CSCsb90602	Unknown	After adding and removing SVI interfaces OSPF wont come up
CSCsc31677	Unknown	Enh: CLI to remove show inventory from show tech output

Resolved Caveats in Release 12.2(17d)SXB10

Identifier	Technology	Description
CSCee56573	Unknown	L3 traff s/w switched after removing/adding port channel
CSCeg29451	Unknown	standby and DFC in standby slot resets when doing write mem
CSCei76358	Unknown	cleanup of user interface data

Resolved Caveats in Release 12.2(17d)SXB9

Identifier	Technology	Description
CSCeg09691	AAA	dot1x EAP authentication not working with per-server radius key
CSCeb71693	Infrastructure	12.2S: issues with logging snmp-authfail command
CSCsa82886	Infrastructure	RP crashes when argument for tftp-server command longer than 67 char
CSCds33629	IPServices	Closing Telnet session crashes router..
CSCsa85588	MPLS	Per VRF Aggregate Label not in Ifib
CSCeg28814	Multicast	Duplicated mcast packet due to wrong FPOE in egress replication mode
CSCeg83460	Multicast	c6msfc:bidir pim df not elected with multiple RPs after link down
CSCeh95160	Multicast	bi-directional PIM DF winner may receive an incorrect unicast metric
CSCsb01188	QoS	ATM interface on FW/FW2 PA stops tx on add/remove service policy
CSCeh13489	Routing	BGP shouldn't propagate an update w excessive AS Path > 255
CSCsa78259	Routing	IOS reload due to specific BGP routing update
CSCed93264	Unknown	RP truncates the TOS byte to upper 3 bits on IP with option field
CSCee37771	Unknown	67xx: Rommon Upgrade Failure
CSCee40846	Unknown	egress multicast to slot 1 ports also goes to Sup slot
CSCef32513	Unknown	SPAN destination ports causing latency on adjacent Pinnacle ports
CSCef33051	Unknown	Part of the traffic blackholed when new link joins etherchannel
CSCef40249	Unknown	power inline command appears even after removed and reloaded system
CSCef47414	Unknown	VTP code fail to restore vlan database properly
CSCef66632	Unknown	Demand Aging clearing entries every 4 seconds, without contention
CSCef88685	Unknown	mcast ltl cleared out on WS-X6816-GBIC after NSF/SSO failover
CSCeg39091	Unknown	Abnormally long flooding with L2 DFC DEC
CSCeg48547	Unknown	fm_netflow_earl6.c: early return results in memory leak
CSCeh40945	Unknown	Same MAC addressees are learnt by different VLAN
CSCeh53682	Unknown	MACs Learned on EtherChannel across L2 Fwding Engine Get Off-sync
CSCeh54386	Unknown	Ucast flooding due to MACs losing PI_E flag when SPAN is configured
CSCeh54533	Unknown	IOS SLB with Egress ACL under SVI breaks L2 icmp traffic
CSCeh56398	Unknown	T48+, G+-CR2 in C+/Legacy configuration boot with multiple errors
CSCeh59654	Unknown	Ucast flooding due to +MN received on DFC/PFC when DEC is configured
CSCeh62522	Unknown	igmp snooping source only doesnt work for certain range of group ad
CSCeh73049	Unknown	telsh mode bypasses aaa command authorization check
CSCeh73110	Unknown	Ucast flooding due to +MN/-MN race condition
CSCei18018	Unknown	Diagnostics HM crash
CSCin72202	Unknown	Auth-Proxy do not work with ODM merge algorithm
CSCin78324	Unknown	PA-MC-8TE1+: check to drop runts packets missing in driver code
CSCsa49748	Unknown	sup720 reloads by software forced crash

Identifier	Technology	Description
CSCsa57081	Unknown	sup720 : static multicast CAM entry is not programmed after reload
CSCsa63184	Unknown	Crash TestSPRPInbandPing fail after MLS global enable with Dist. Etherch
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
CSCsa76812	Unknown	ICC gets stuck after reload if RM aging is configured to no_aging
CSCsa80358	Unknown	Connectivity lost on native vlan on etherchannel trunk betn 2 cat6ks
CSCsa96704	Unknown	MSFC3: Bus error while issuing the show mls netflow creation command
CSCsb04346	Unknown	crash l2_aging_proc after changing Spantree mode
CSCsb10662	Unknown	PI_E lost on Supervisor after +MN received on DEC with Plus
CSCsb16051	Unknown	traffic should not flood to all LC in L3 distrinuted port-channel
CSCsb16396	Unknown	Unicast flooding with Shut on one of the DEC members
CSCsb18038	Unknown	GE-WAN show interface in/out rate is always zero
CSCsb32028	Unknown	%CPU_MONITOR-2-NOT_RUNNING: CPU_MONITOR tracebacks and crash
CSCsb38273	Unknown	L3 Traffic flood over DEC due to incorrect Flood region FPOE
CSCdx86562	WAN	A interface of ntp source is changed by creating a interface

Resolved Caveats in Release 12.2(17d)SXB8

Resolved LAN Caveats

- [CSCsa67294](#)—Resolved in 12.2(17d)SXB8

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.

Other Resolved Caveats in Release 12.2(17d)SXB8

Identifier	Technology	Description
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
CSCea25073	IPServices	IOS FTP client code rewrite
CSCec50485	IPServices	copy ftp flash fails with 3COM ftpserver
CSCef60452	Multicast	possible blackout when receiving Join on RPF interface (iif)
CSCee45508	platform-76xx	OSM CHOC-OC12 freezes up while processing PPP keepalives
CSCef19811	platform-76xx	MPLS:VPN:MLPPP:PE not receiving packets from connected CE
CSCeg77503	platform-76xx	SAA Packets do not hit the outbound service policer
CSCdv76375	Routing	OSPF neighbor command unsupported in VPN routing instance
CSCee16068	Routing	Equal cost default route remains in RT after changing interface cost
CSCef67660	Security	sshv2 malformed client ignore msg cause damage to router
CSCeh18999	Security	Second CRL is not checked with VPNSM
CSCsa67272	Security	Serial number in certificate subject is incorrect
CSCsa78580	Security	Crypto IKMP process can get blocked if router fails to fetch CRL
CSCsa81928	Security	CRL checking fails if PKI URI received for CDP is UPPER CASE
CSCed36177	Unknown	Cat6000 : RP may crash at tunnel_ip_les_fastswitch
CSCef36367	Unknown	MMLS: High CPU after Sparse->Bidir transition
CSCef76161	Unknown	ifInDiscards are resetting, causing counter problems
CSCef80423	Unknown	Sup3: watchdog fired incorrectly when reload/incorrect bootup cause
CSCef81281	Unknown	The value of cbQosPoliceConformedByte64 provided by SNMP decrease
CSCeg08562	Unknown	%IPC-3-NOBUFF: The main IPC message header cache is empty
CSCeg19103	Unknown	ALIGN-3-TRACEX : Error with debug netdr turned on
CSCeg41623	Unknown	CSM:Only configured vlans should be allowed on trunk
CSCeg55846	Unknown	MSFC3 HYB: msfc3 hybrid IOS does not implement some EMT calls
CSCeg62365	Unknown	rxHCDropEvents incrementing on 6704-10GE interface
CSCeg70376	Unknown	Sup720 : Ingress VSPAN is not working for VoIP VLAN
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-file systems causes supervisor to crash
CSCeh21723	Unknown	K+NAM:span monitor session stops forward traffic to NAM after SSO
CSCeh29617	Unknown	PP:Sup3:FRoMPLS:CHOC:pkts dropped on egr (PE-CE)link (ping fails)
CSCeh51906	Unknown	All hybrid image for Sup720 wont be able to config with STI NVRAM
CSCeh59181	Unknown	Fabric buffer reserve command does not work
CSCsa69590	Unknown	Teton3: after s/w, PWAN2 interface becomes UP for nonconnection port

Resolved Caveats in Release 12.2(17d)SXB7

Resolved Routing Caveats

- [CSCef68324](#)—Resolved in 12.2(17d)SXB7

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(17d)SXB7

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(17d)SXB7

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(17d)SXB7

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

- **CSCef44225**—Resolved in 12.2(17d)SXB7

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(17d)SXB7

Identifier	Technology	Description
CSCee26700	MPLS	memory leak caused by LSR MIB queries
CSCef37186	MPLS	cpuhog/watchdog-crash on mplsXCIndexNext mib query
CSCeb51147	Multicast	Stack overflow due to inf. rec in dual-RP/E4+ mic rel
CSCeg03144	platform-76xx	%EARL_L2_ASIC-SP-4-L2L3_SEQ_ERR on Sup720
CSCsa47099	platform-76xx	IPX broke on wan link of OSM-2OC12-ATM
CSCsa53708	platform-76xx	OSM crashes under stress when having to pad packets
CSCee72906	PPP	dLFIoLL mlp-qos:VIP crash when bundle is reset while traffic is ON
CSCeg57219	PPP	Unable to ping packets greater than 1022 across MLPPP after sup SW
CSCed51640	QoS	dWFQ isnt diplayed in sh run anymore, so is lost after reload
CSCeb40561	Routing	[SNMP] GGSN reloads during get next operation
CSCed63876	Routing	BGP: router crashes pointing to ed_decay_penalty
CSCef93215	Routing	router crash at ospf_build_one_paced_update
CSCeg08344	Routing	with cef/dcef enabled & compression on, tcp frames getting dropped
CSCeg19442	Routing	crash on pdb_ospf_hello_BLOCK
CSCsa59600	Routing	IPSec PMTUD not working [after CSCef44225]
CSCdv68743	Unknown	Inefficient code in qos/qoscli_match_packet.c:match_named_acl().
CSCed12393	Unknown	CPU-HOG in PIM,MLSM & MWheel and multi-device WATCHDOG crash
CSCee10005	Unknown	Cat6500 service module connectivity issue with crossmodule etherchan
CSCee30816	Unknown	TTL for decremented on the encap side when hardware switching
CSCee68381	Unknown	Packet drops on old rev WS-X6516-GBIC
CSCee86168	Unknown	active SP resets, sr7100 errata 11
CSCef58590	Unknown	Disable VTT major temp shutdown and change thresh 100/85 -> 115/100
CSCef82367	Unknown	IP traff not frwdd on G+CR2 port if toggled between routed/switched
CSCeg10174	Unknown	High CPU in QoS Mgr when changing long QoS access-list
CSCeg49196	Unknown	Excessive Overruns and lbusDrops due heavy flow control over fabric
CSCeg51793	Unknown	MVPN: Address Error Exception after config change w/ Mvpn
CSCeg52280	Unknown	CRCs caused by WS-X6704-10GE
CSCeg55565	Unknown	MMLS/MVPN: crash at mls_earl_show_scmdb -> chunk_lock
CSCeg56052	Unknown	Active and Standby SP crash due to GC Entry memoryleak
CSCeg65640	Unknown	Cat6000 with UDP turbo flood results in corrupted outgoing packets

Identifier	Technology	Description
CSCeh11095	Unknown	SUP720 not forwarding packets for certain prefix
CSCin87976	Unknown	Need to rate-limit EOS Error interrupts
CSCsa47020	Unknown	Sup720/FlexWAN: FRF.16 drops 64 byte packets above 2Mb
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
CSCin76078	WAN	ATM(Deluxe & IMA) driver code for Flexwan to prefer priority packets

Resolved Caveats in Release 12.2(17d)SXB6

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
CSCec63011	Infrastructure	Standby crashes in redundant systems
CSCeb40653	MPLS	Bus error crash at vrf_interface_print when deleting vrf config
CSCee37430	MPLS	Missing LFIB tag rewrite on LC after loss of /32 entry to its next-hop
CSCef12304	platform-76xx	PWAN2:Connectivity is broken between GE-WAN if one end shut/no shut
CSCef74227	platform-76xx	LAN GE of OSM incorrectly increments giants on dot1q trunk port
CSCef76828	platform-76xx	connectivity broken after config/unconfig tunnel interfaces
CSCeg10236	platform-76xx	PWAN2:GBIC type shown as not connected in show int
CSCeg47780	platform-76xx	RFC1483 Bridging broken on BT
CSCee22810	QoS	Router stops sending LMI with QOS configured
CSCee24349	QoS	Crash at fib_post_download_processing when reloading
CSCef06034	QoS	Sup720 crashes after SSO Failover with nbar configured
CSCef66517	QoS	packet drop on flexwan when traffic shaping
CSCeg49010	QoS	ISIS updates not sent when output qos police is set
CSCeb53542	Routing	Inconsistency between CEF adjacency and ARP tables; unicast pkt loss
CSCed26217	Routing	Unnecessary ARP was sent on OSPF non broadcast network
CSCed63342	Routing	RIP-Unicast updates not sent to configured RIP neighbors
CSCee59315	Routing	MPLS-VPN:Corrupted BGP table showing stale and/or poisoned paths
CSCeg26378	Routing	Dest CEF entry is missing in DCEF table. All pkts are punted to RP.
CSCee88654	Security	IOS requests an extra prompt for SSH key generation
CSCef61978	Security	SSHv2 session hangs with large command output until key press
CSCed25505	Unknown	reset of csm causes one of WS-X6248A-TEL to reset in a chassis
CSCed73700	Unknown	Vlan Translation does not work on WS-X6816-GBIC
CSCed82736	Unknown	SYS-2-GETBUF: Bad getbuffer, bytes= 65535
CSCee85152	Unknown	CEF Hardware switching produces ping failure on every other packet a

Identifier	Technology	Description
CSCee95708	Unknown	MSFC2-3-TOOBIG on sup720 in MPLS/VPN environment
CSCef27359	Unknown	SW and HW cef adjacency inconsistency
CSCef35707	Unknown	L2 Forwarding Table ECC error handler not working properly
CSCef45495	Unknown	PIM Snooping: (s,g,r) prune handling cases
CSCef49330	Unknown	APS not working on the PA-MC-STM1
CSCef58323	Unknown	%EARLY-L2_ASIC-DFC-SRCH_ENG_FAIL T/B on Berytos with L2(10k mac)Traf
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
CSCef79592	Unknown	Class-default shows packets output 0; packet drops 0
CSCeg01297	Unknown	System crash caused by pkt of incorrect length/IP header checksum
CSCeg03423	Unknown	show int trans does not show ITU channel info for DWDM Xenpaks
CSCeg06698	Unknown	COS rewritten for routed multicast traffic
CSCeg08389	Unknown	Interface counters do not increment on a Virtual MFR interface
CSCeg09655	Unknown	VPN-SM: Error in GRE check
CSCeg11415	Unknown	PWAN2:Strange behaviour of the QoS in the module
CSCeg15012	Unknown	SP crash with bus error while processing multicast packet
CSCeg16684	Unknown	Some VPLS VCs fail to pass traffic after a link failure in the core
CSCeg19269	Unknown	gt 12L4 Oper in acl dest port doesnt expand corectly;pkts non-qos fw
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
CSCeg30437	Unknown	VPLS:ATOM:CWAN: Some VCs remain down, LFIB/TTFIB are ok
CSCeg38482	Unknown	MVPN one PE can not receive auto-RP information for one vrf
CSCeg40177	Unknown	Tag to Ip path has all zero src and dest mac
CSCeg40543	Unknown	some vcs do not pass traffic after supervisor switchover
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
CSCdz67208	WAN	CWPA: Pkts generated on this router are not getting matched
CSCef93103	WAN	bridge-vlan on Flexwan PVC floods BPDUs

Resolved Caveats in Release 12.2(17d)SXB5

Resolved Routing Caveats

- [CSCee67450](#)—Resolved in 12.2(17d)SXB5

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>

Resolved Unknown Caveats

- [CSCef90002](#)—Resolved in 12.2(17d)SXB5

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>

- [CSCin82407](#)—Resolved in 12.2(17d)SXB5

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(17d)SXB5

Identifier	Technology	Description
CSCeg11566	Infrastructure	SNMP May Consume all the I/O Memory
CSCef46191	IPServices	Unable to telnet
CSCea83675	MPLS	Enhance VRF protection while displaying VRFs
CSCed57281	MPLS	CPU hog in CEF reloader while adding a vrf interface
CSCed81317	MPLS	can not see bgp routes from CE after import map
CSCef14446	MPLS	mpls vpn: recirculation vlan for agg label is not mapped to vpn
CSCee72817	platform-76xx	BGP neighbor relationship flaps periodically between PEs and RRs
CSCef35398	platform-76xx	OSM-2OC12-ATM-SI+ - SRIC IPM parity error
CSCea64725	Routing	BGP does not send all updates to recently established peer-group mem
CSCec29953	Routing	retrans counter not getting cleared / continuous ospf neighbor flap
CSCee35125	Routing	RP crashed on rip_redist_check on clear ip route *
CSCec67602	Security	ssh: tb in process_watch_timer when sending big ssh packets
CSCdx91720	Unknown	12.1(12c):Qos:Request to support L4 port expansion in QM code

Identifier	Technology	Description
CSCed00394	Unknown	Directly connected mcast subnet are NOT programmed in the SP
CSCed35900	Unknown	:CWPA2 mpls QoS classification not working until re-add policy
CSCed52841	Unknown	In some circumstances, switch is not responding to SNMP requests
CSCed66865	Unknown	SP crash at earl7_force_crash
CSCee07395	Unknown	Const2:FIB Protocol Allocation mismatch
CSCee11672	Unknown	Some static mac entries missing in DFC after module reset
CSCee23058	Unknown	Incorrect Netflow Byte Counts With Large Flows
CSCee34416	Unknown	Supervisor may crash due to TestSPRPInbandPing
CSCee63221	Unknown	SP crash DIAG_PF_CONST2_TEST_HAS_FAILED
CSCee65953	Unknown	Incorrect Netflow Byte Counts With Large Flows
CSCee75620	Unknown	RP crashes after enable CBAC
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
CSCef05282	Unknown	Removing IP address, IP route cache cef still allows pkts to switch.
CSCef13797	Unknown	TCAM Capacity Exceeded with ACL on POS Interface
CSCef30308	Unknown	all zero source and dest mac address in show mls adj entry det
CSCef37026	Unknown	Running configuration is not synching between DR and NDR on MSFC3
CSCef41228	Unknown	SSO failover causes WS-X6816-GBIC reset
CSCef47466	Unknown	High latency and packet drop when any interface goes down on OSM
CSCef53290	Unknown	Using config mls ip ids causes switch to reload unexpectedly
CSCef58932	Unknown	VACL filter out STP BPDU
CSCef63549	Unknown	Multicast MET management fix and increase OIF above 1023 per flow
CSCef65827	Unknown	GRE o/v IPSec with VPNSM intermittently loses connectivity
CSCef67810	Unknown	get-bulk for portGrp causes cpu spike and delayed response
CSCef70298	Unknown	IFindex missing IDBs after deleting and adding T1 channels
CSCef72205	Unknown	vlan stops forwarding
CSCef73076	Unknown	ALIGN-SP-3-CORRECT seen in mcast_igmp_handle_igmp_pak
CSCef75501	Unknown	dot1x authentication not work perfectly in sup720.
CSCef75924	Unknown	packet drop for L3 traffic over dist. etherchannel with SPAN enabled
CSCef78235	Unknown	Disable egress span of vacl redirected packets
CSCef82797	Unknown	Distributed EtherChannel may caused packet loss
CSCef89139	Unknown	Adjacency pointers not Updated when 2nd Link Removed on 7600
CSCef91572	Unknown	Software forced crash at process pm_mp_notify_cp_port_admin_state
CSCeg01510	Unknown	Device crashes when we configure no vlan <vlan nu>
CSCeg03808	Unknown	Tetons: I/O Memory is getting depleted, IPC queue exhausted
CSCin79961	Unknown	Errdisable recovery not working with UFP.
CSCin82741	Unknown	PBR does not work if both PBR & SLB are applied on same interface

Identifier	Technology	Description
CSCuk49481	Unknown	GRE packets inot correctly processed (DF) on cat6500
CSCef91994	WAN	FLEXWAN - PA-A3 - packet drop when ping 1500bytes with MPLS

Resolved Caveats in Release 12.2(17d)SXB4

Resolved IPServices Caveats

- [CSCed78149](#)—Resolved in 12.2(17d)SXB4

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(17d)SXB4

Identifier	Technology	Description
CSCee43166	Routing	BGP: reduce CPU load for processing inbound VPNv4 updates
CSCef14934	Unknown	link up/down message is abnormal
CSCef48695	Unknown	UDLR:UDE: mis-config unidirectional mode causes tx counters to stick
CSCef55147	Unknown	DOM: global dom cli is broken, show int trans, returns null.
CSCin78110	Unknown	Some E1 controller does not come up if a large config on other LC

Resolved Caveats in Release 12.2(17d)SXB3

Identifier	Technology	Description
CSCef01725	Infrastructure	pak_realign driving up CPU usage
CSCeb61377	platform-76xx	CWTLC fabric related alignment correction
CSCec49042	QoS	IPP not being trusted using nbar type class map
CSCdt38401	Routing	Frame-relay packets processed by cpu due to CEF inconsistency
CSCdy33703	Unknown	Need span support for port 1/4 & 1/3
CSCed69233	Unknown	alignment error in qm_get_card_info_for_police_action
CSCee42657	Unknown	sup720 crashing after reload with large configuration
CSCee55233	Unknown	Large L3 port-channel config with stats collection caused high CPU
CSCee68052	Unknown	unsolicited igmp reports do not always reset host join timer
CSCee83655	Unknown	CPU_MONITOR-2-NOT_RUNNING_TB: CPU_MONITOR tracebackrate_limit_loop
CSCee89586	Unknown	VPN-SM:ICMP unreachable sent for pkt w/ iplen+ovhead eq mtu, DF set
CSCef07017	Unknown	VACL is not working for RSPAN traffic with mcast enabled
CSCef14106	Unknown	IDS2 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:
CSCin77443	Unknown	HYB:HA:Slave crashes on configuring Virtual-Template interface

Resolved Caveats in Release 12.2(17d)SXB2

Identifier	Technology	Description
CSCed92290	Content	CE4-NATIVE:wccp redirect issue after reloading the switch
CSCdz27562	Infrastructure	snmpwalk on loopback interface gets response from physical int. IP.
CSCea81029	IPServices	show ip igmp int crashed router
CSCec13278	IPServices	IGMP: IGMP_clear_cache() invoked crashed LC when LC OIRed
CSCec84887	IPServices	Sup720: Disabled STP for VLAN-bridge becomes to enable by shutdown
CSCec25430	Management	IOS may reload from specific packet
CSCdx80484	MPLS	C10720: Removing LDP before EoMPLS may cause a crash
CSCeb78347	MPLS	Cannot create a VRF
CSCea59359	Multicast	PIM stops sending Data-header Register packets
CSCeb57662	Multicast	Static mroute configuration does not take effect
CSCec40377	Multicast	Multicast router may stop sending PIM join msgs if low on I/O memory
CSCee88700	Multicast	TCAM entry not built for secondary subnet with multicast stub
CSCee89438	Multicast	MSDP doesnt build S,G state after rxing *,G join

Identifier	Technology	Description
CSCec62800	platform-76xx	20E:CWAN-QOS:Increased PQ latency when increasing default queue traf
CSCee01868	platform-76xx	OSM-2+4GE-WAN+:Interface UP/UP with GBIC installed but not connected
CSCee54642	platform-76xx	OSM local bus out of SYNC after stress
CSCee55056	platform-76xx	OSM interface byte counts are inaccurate
CSCee59667	platform-76xx	GE-WAN+ MTU config inconsistent with other IOS devices
CSCee84887	platform-76xx	OSM interface byte counters broken with high pps + large route table
CSCec15517	QoS	RSP crash Unexpected exception, CPU signal 10
CSCee31618	QoS	C2SUP2/FW2/CT3+:Voice packet drops at low rates with cRTP+LLQ conf
CSCin52060	QoS	After the policy got rejected hqf was not cleaned on vip
CSCea35186	Routing	OSPF: DR not generating network LSA
CSCed60800	Routing	Routing Table not updated when BGP next hop is withdrawn
CSCee36721	Routing	OSPF does not adv Net LSA when two interfaces have same address
CSCeb58952	Unknown	FlexWAN II OC3 LLQ Profiling: latency and voice pkt loss issues
CSCee50884	Unknown	BGP Multipath failover takes very long time to cnvrge (500K)
CSCed38956	Unknown	Client Browsers see significant delay in retrieving content from ser
CSCed77602	Unknown	:All ports in the etherchannel being bounced on SSO
CSCed85411	Unknown	Rapid-PVST: Short loop forming when root moves
CSCee04176	Unknown	Mac-address-limiting inconsistent between LAN & VPLS
CSCee05653	Unknown	RPR+: Standby SP can not take over when Active SP fails
CSCee51501	Unknown	Excessive SCP retries and drops while doing shut/no shut repeatedly
CSCee53705	Unknown	cwpa2: Turn on FIFO flow control and EOS driver changes
CSCee54526	Unknown	SP: const_mpls_ios_set_hw_taginfo taginfo do not own rew, but ctagre
CSCee69687	Unknown	UDP fragments dropped with the VACL configured on the SVI
CSCee80365	Unknown	1st hop router randomly fail to add (s,g) flows oif in HW fib table
CSCee89232	Unknown	Configuring platform while in automore state crashes switch
CSCee90183	Unknown	Need to change RPC syslog in case of RPC request sent failure
CSCee95301	Unknown	Unhide and document mls rate-limit multicast non-rpf command
CSCef07965	Unknown	System crashed when accessing CVDM from the switch
CSCin68355	Unknown	:Marking with microflow policer not working with layer2 port
CSCin74123	Unknown	mst root id becomes 0 after switchover
CSCin76766	Unknown	Active SP reloads at ipc_send_rpc_blocked failed after RPR+ swover

Resolved Caveats in Release 12.2(17d)SXB1

Resolved Routing Caveats

- [CSCed40933](#)—Resolved in 12.2(17d)SXB1

Cisco Internetwork Operating System (IOS) Software is vulnerable to a Denial of Service (DoS) attack from crafted IPv6 packets when the device has been configured to process IPv6 traffic. This vulnerability requires multiple crafted packets to be sent to the device which may result in a reload upon successful exploitation.

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

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20050126-ipv6>.

Resolved Security Caveats

- [CSCed65285](#)—Resolved in 12.2(17d)SXB1

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>

- [CSCed93836](#)—Resolved in 12.2(17d)SXB1

A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

All Cisco products which contain TCP stack are susceptible to this vulnerability.

This advisory is available at

<http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-ios.html>, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS software.

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at <http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-nonios.html>.

Other Resolved Caveats in Release 12.2(17d)SXB1

Identifier	Technology	Description
CSCee04747	ATM	memory leak when removing ATM VCs
CSCec55147	Infrastructure	Memory leak in IFS
CSCed81154	Infrastructure	SNMP retrieve configuration file crash SUP720 RP
CSCee25000	Infrastructure	Fix for CSCeb22276 and CSCed68575
CSCee06948	IPServices	Sup720 running 12.2(17b)SXA is allowing connections to TCP port 514
CSCdz32659	Management	%SYS-2-MALLOCFAIL: -Process= CDP Protocol
CSCed40563	Management	malicious cfg reload neighbor routers by <show cdp entry * protocol>
CSCin67568	Management	Memory leak in CDP process with long host names
CSCed72764	MPLS	TE tunnel(s) fail to switchback to Explicit path option
CSCeb30338	Multicast	Mcast traffic loss each minute as MMLS entry deleted and reinstalled
CSCed95515	Multicast	Pkts drop in all VLANs when last host in one VLAN leave this group
CSCea57792	platform-76xx	13E5/GBIC:GE-WAN int with 1000baseT gbic is down after oir with traf
CSCed48085	platform-76xx	Stats incorrect for all BB2 OSMs with SUP720
CSCed86778	platform-76xx	: PQ problems with HQoS policy applied to 100 PWAN2 sub-intf
CSCee55056	platform-76xx	OSM interface byte counts are inaccurate
CSCed62633	QoS	RSVP: Install tag failure leaves RSB pointing to freed REQUEST
CSCee23845	QoS	Policer stops counting on egress after ingress poicy is reapplied.
CSCee02786	Routing	IPX EIGRP fails to set originating router id on startup
CSCee36622	Routing	Summary LSA stuck in database
CSCdz84583	Security	IOS fw allowing forged packets for a session initiated from inside
CSCed35253	Security	Router crash due to corrupted data in list with IOS-firewall
CSCed69858	Security	show ssh command issued repeatedly may crash the system
CSCin74155	Security	SSHv2:router crashes under heavy load at tcb_isvalid
CSCed06744	Unknown	software flood to fabric issues with cross-DFC etherchannels
CSCed63590	Unknown	GTP SLB doesnt work with GGSN R5.0 Call Admission Control function
CSCed65372	Unknown	RP/SP software forced reloaded after removing switchport from FE int
CSCed68821	Unknown	WS-X6548-GE-TX stops transmitting
CSCed75920	Unknown	When Glean Rate Limiter enabled Egress ACLs applied on Ingress Pkts
CSCed77519	Unknown	Sup720-3BXL:EoMPLS:VLAN_M dot1q tag handling for IPv6 pkt problem
CSCed79711	Unknown	:LTL_DEBUG_ASSERT: Failure on index + j
CSCed85276	Unknown	VPNSM does not correctly decapsulated nested IPsec traffic.
CSCed87264	Unknown	WS-X6148-45AF module resets randomly when IP phones are connected
CSCed89537	Unknown	DFC runs out of memory and reloads at L2 Aging Task
CSCed93359	Unknown	Startup config synched to stdby,BOOT_STRING_INVALID message appears
CSCed93707	Unknown	VPN-SM:Different comb of DF bit, PMTUD settings in GRE must be corre
CSCed94258	Unknown	Traffic routed on L2 DEC stops when other L2 DEC becomes non DEC

Identifier	Technology	Description
CSCee05413	Unknown	Memory leak in EARL VLAN stats subblock
CSCee10614	Unknown	DEV: FibTcamSSRAM test fails
CSCee13713	Unknown	test memory crashes the system
CSCee15581	Unknown	sss_mgr with invalid index into 2 arrays causes crash/traceback
CSCee17030	Unknown	Sporadic delay with multicast leave/joins on Spu 720
CSCee19156	Unknown	6PE does not obey mpls ttl propagation command
CSCee21772	Unknown	port-channel dflt results wrong after bootup
CSCee22362	Unknown	Multicast src only detection needs to happen faster
CSCee22993	Unknown	Sup720: Diags detect error on standby Sup after SSO failover
CSCee24422	Unknown	Tracebacks at tyfib_error_recovery and MLSCEF-SP-2-FREEZE
CSCee28215	Unknown	CLI to output actual pps performance
CSCee28288	Unknown	2 second delay in forwarding the 1st packet of mcast stream on 7600
CSCee32151	Unknown	Crossbar MIB not working correctly
CSCee33136	Unknown	MPLS packets duplicated in SRP ring (OSM-DPT)
CSCee35193	Unknown	OSPF sessions are not coming up using pos linecards in the core
CSCee36959	Unknown	Software Forced Reload:get_rp_cpu_info
CSCee39170	Unknown	Incorrect mask value set in ACL TCAM when matching on DSCP values
CSCee43090	Unknown	RLB subscriber packets may loop due to incorrect flow-mask.
CSCee44248	Unknown	Redundant Sup fails to come online after switchover
CSCee45404	Unknown	HSRP does not forward traffic correctly after primary back up
CSCee47030	Unknown	6704-10GE needs to be powered down with Intel ER Rev1 XENPAKs
CSCee54734	Unknown	Need to disable module if a real bad xenpak is plugged in.
CSCee54862	Unknown	High CPU load
CSCin74475	Unknown	Connectivity lost to MWAMs for resetting CSM/MWAM modules on switch
CSCee33103	WAN	CWPA2: CWPA2 reset by SUP due to SCP keepalive failure

Resolved Caveats in Release 12.2(17d)SXB

Resolved IPServices Caveats

- [CSCed27956](#)—Resolved in 12.2(17d)SXB

A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

All Cisco products which contain TCP stack are susceptible to this vulnerability.

This advisory is available at

<http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-ios.html>, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS software.

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at <http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-nonios.html>. ION is also impacted.

- **CSCed38527**—Resolved in 12.2(17d)SXB

A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

All Cisco products which contain TCP stack are susceptible to this vulnerability.

This advisory is available at

<http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-ios.html> and it describes this vulnerability as it applies to Cisco products that run Cisco IOS software.

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at <http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-nonios.html>

Resolved MPLS Caveats

- **CSCeb56909**—Resolved in 12.2(17d)SXB

Cisco Routers running Internetwork Operating System (IOS) that supports Multi Protocol Label Switching (MPLS) are vulnerable to a Denial of Service (DoS) attack on MPLS disabled interfaces.

The vulnerability is only present in Cisco IOS release trains based on 12.1T, 12.2, 12.2T, 12.3 and 12.3T. Releases based on 12.1 mainline, 12.1E and all releases prior to 12.1 are not vulnerable.

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

<http://www.cisco.com/en/US/products/csa/cisco-sa-20050126-les.html>

Resolved Unknown Caveats

- **CSCed30113**—Resolved in 12.2(17d)SXB

A malformed Internet Key Exchange (IKE) packet may cause the Cisco Catalyst 6500 Series Switch or the Cisco 7600 Series Internet Router to crash and reload.

This vulnerability is documented as Cisco bug ID **CSCed30113**. There are workarounds available to mitigate the effects of this vulnerability. Cisco is providing fixed software at no charge.

This advisory will be posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20040408-vpnsm>

Other Resolved Caveats in Release 12.2(17d)SXB

Identifier	Technology	Description
CSCed08399	Access	NRT:Spurious Accesses seen on 7500 router (etext) for QoS tests
CSCea80820	ATM	Alignment correction at atm_arp_process
CSCeb56457	ATM	IMA and ATM-deluxe PAs drop packets with certain patterns
CSCec12294	ATM	cfg_atm_vcmode_bcs_func is broken
CSCin53126	ATM	Router crashed at abort during OIR of ATM OC3 MM PA
CSCin65182	ATM	OAM PVC on IMA interface doesnt come up after OIR
CSCec87661	Infrastructure	CHUNKBOUNDS errmsg in wrong circumstance - NAT shortcuts not install
CSCea60559	MPLS	lsr mib snmp agent consumes 99% cpu forever
CSCea65827	MPLS	RP/VIP Crash: OIR Flexwan/loose IGP Route to BGP next hop router
CSCeb05519	MPLS	MPLS forwarding table has incorrect label for prefix
CSCeb26389	MPLS	BGP allocates same local label to two VPN prefixes
CSCeb27452	MPLS	Bus error at tagsw_send_icmp process
CSCeb36929	MPLS	Tunnel : bus error when performing tag imposition
CSCeb46191	MPLS	VPN labels get swapped for two iBGP neighbors on a PE-CE shut/noshut
CSCeb76642	MPLS	sh ip cef crashes the RP
CSCec15733	MPLS	MPLS LDP: router crashed while handling tagcon work item
CSCed47409	MPLS	PRP crashes when remove large number of routes
CSCuk47482	MPLS	crash after no mpls ip
CSCec59728	platform-12000	SSO: Standby RP reloads once it is fully-up
CSCec03984	platform-76xx	GE-WAN+ MPLS MTU config inconsistent with other IOS devices
CSCed19431	platform-76xx	GigabitEthernet negotiation is broken on 7600
CSCed49872	platform-76xx	SYS-2-GETBUF: Bad getbuffer SCP Hybrid process tracebacks
CSCed51835	platform-76xx	OSM/POS/BB1: OC12 IP 64 bytes performance may degrade
CSCin66010	PPP	dLFIoFR+QoS:Toggling FR encap can cause router crash
CSCin67741	PPP	RP crashes on removing encap from multilink interface
CSCeb61825	QoS	VIP quantum not updated when MTU changed on PA-A3
CSCec28505	QoS	Need to remove error msg showing when bootup w/ low-speed ifc
CSCed62637	QoS	CWPA: priority traffic latency varies with default traffic load
CSCeb17467	Routing	BGP: RP crashes on clearing the BGP table
CSCeb30370	Routing	Crash at ospf_flush_area_summary_lsa after no ip vrf vpn1
CSCeb52270	Routing	Missing receive entry in CEF table
CSCeb77038	Routing	System returned to ROM by bus error on MPLS/PE router
CSCec14415	Routing	BGP next-hop not being set properly amongst peer-groups
CSCec42160	Routing	OSPF Hello processing interrupted during CPU intensive activity
CSCec44556	Routing	RIP updates not sent over ATM subints
CSCec85322	Routing	router crashed at i_up during ospfv3 negative testing

Identifier	Technology	Description
CSCec86420	Routing	Undebug all stops traffic with IPsec+GRE+CEF (Also see CSCeb56909)
CSCed06329	Routing	BGP-v6: Version number churns when multipath configured on BGP-v6
CSCed20042	Routing	IPv6 CEF crash when encountering a recursion loop
CSCed29557	Routing	Static routes are not deleted when PEs VRF interface is shut
CSCed57077	Routing	Crash on displaying expired reflexive ACL entries
CSCed62835	Routing	IPV6FIB-SP-4-RECURSION,CEF IPC STACKLOW msg followed by crash
CSCed51674	Security	Software-forced reload:no crypto map GRE on physical interface
CSCea57452	Unknown	SLCP Not Responding...Resetting Module 1
CSCea66218	Unknown	PA-MC-STM1 - Alarmed VCs can bring other VCs down
CSCea78589	Unknown	20E:Crash at ether_getlink on SP
CSCea80003	Unknown	IPSec HA RRI injected routes not deleted on hsrp state change
CSCeb06765	Unknown	Request for Global command to enable Syslog
CSCeb61695	Unknown	RSPAN (CAT6000 Native): VACLs cant be applied on RSPAN vlan traffic
CSCeb72859	Unknown	Bulk Config Sync triggered every exit command
CSCec08364	Unknown	Const2:EoMPLS:L2VPN vpn_num configured as zero, all pkts blocked
CSCec30649	Unknown	QoS:trust port state on 6148-rj45
CSCec36978	Unknown	router crash after no shut sonet interface
CSCec43605	Unknown	dfc: unicast flooding after aging
CSCec55377	Unknown	IOS-SLB: no inservice on RLB vserver may cause reload.
CSCec62406	Unknown	Micorflow policing drops should not charge ag hi policer bucket
CSCec68585	Unknown	CWPA/CWPA2 RP fails to recognize all Flexwans using S9 rommon image
CSCec70454	Unknown	RSPAN on SUP720 running IOS causes spanning tree loop.
CSCec74016	Unknown	Const2:Router crash when ipv6 ACL removed after remove isataptunnel
CSCec90162	Unknown	tracebacks seen after enabling gre keepalive
CSCed00441	Unknown	Rapid-PVST: loop occuring when root bridge expires
CSCed04988	Unknown	6548 + DFC module not recognized with IDPROM message
CSCed05332	Unknown	ws-x6816 reports minor error after reload
CSCed06462	Unknown	%Error opening nvram:/startup-config (Invalid Checksum)
CSCed14506	Unknown	OIR of 6816 without DFC crashes switch to rommon
CSCed20333	Unknown	Dynamic MAC Entries May Not Age Out After Cessation of Traffic
CSCed20566	Unknown	Traffic forwarded in one direction after valn change
CSCed22387	Unknown	Ibc input queue drops constantly incrementing on SP
CSCed22494	Unknown	VPNSM: fail to insert RRI route if dynamic cmap added on the fly
CSCed29594	Unknown	6500 may not unicast flood packets to rp with fallback bridging
CSCed30061	Unknown	entPhysicalSerialNum does not show value for vendor modules.
CSCed33380	Unknown	IPC failure with show mls netflow ip
CSCed34788	Unknown	Small buffer leak @ icc_get_req_pak and leak in SNMP ENGINE

Identifier	Technology	Description
CSCed35745	Unknown	ARP from CSM to real servers not sent downstream after reload
CSCed35960	Unknown	TETONS2: Ch/OC12DS0 crash when unconf/reconf MFR access uninit mem
CSCed38862	Unknown	g1/1 of WS-X6748-GE-TX not link up after changing speed 10M or 100M
CSCed40129	Unknown	6500 running supervisor IOS may not establish DLSW connection
CSCed47381	Unknown	Cat6k: Autostate may not properly shut down vlan int in Native IOS
CSCed48718	Unknown	DEC workaround and SPAN reflector to be mutually exclusive
CSCed49423	Unknown	Temp. values not updated in show environment temperature
CSCed49574	Unknown	12.2S: traffic loss if in/out PO bundled Active/Plus LC
CSCed51894	Unknown	Egress Span doesnt work after removing RSPAN Src Session
CSCed53899	Unknown	Session struct not cleared on deleting Rspan Sessions
CSCed55342	Unknown	Jumbo frames fail across etherchannel routed on the same vlan
CSCed58110	Unknown	Memory leak under stress condition
CSCed58891	Unknown	wrong mistral timing config value for bootflash
CSCed61632	Unknown	SUP720 may not ARP after SRM-SSO failover with bridging enabled
CSCed62337	Unknown	OSPF adjacencies fail to come up with Sup720, PFC3a and MPLS
CSCed62866	Unknown	VPN-SM-C2:collapse crypto update toggles & reuse vlanidb for gre tun
CSCed63897	Unknown	shut/unshut edge port cause TC to be initiated
CSCed78815	Unknown	BT:Shaping with class-default does not work on ATM pvc
CSCed79519	Unknown	Breakpoint exception due to RPC mismatch timeout
CSCed79694	Unknown	C2SUP2: Multi-Link FR fails to forward.
CSCin41024	Unknown	c2sup2:CWPA:DMLFR:FR Relay entry (sh fr map) is taking lot of time
CSCin61989	Unknown	C2SUP2:RSPAN session not restored on source OIR.
CSCin67400	Unknown	FRF12: Checksum errors with POS, ping fails
CSCin67419	Unknown	A shut of any of the member link or cont traff brings down MFR intf
CSCed62698	WAN	CWPA: ATM: DSCP bits 4-6 set to zero
CSCin34959	WAN	RP fails to recognize bay 1 ATM PA after bay 0 was test crashed
CSCin68724	WAN	set atm-clp bit not set on outgoing packets but QoS stats increment

Caveats in Release 12.2(17b)SXA and Rebuilds

- [Open Caveats in Release 12.2\(17b\)SXA and Rebuilds, page 411](#)
- [Resolved Caveats in Release 12.2\(17b\)SXA2, page 411](#)
- [Resolved Caveats in Release 12.2\(17b\)SXA, page 411](#)

Open Caveats in Release 12.2(17b)SXA and Rebuilds

Identifier	Technology	Description
CSCec74016	Unknown	Const2:Router crash when ipv6 ACL removed after remove isataptunnel
CSCed35900	Unknown	CWPA2 mpls QoS classification not working until re-add policy
CSCee09692	Unknown	Sup720: IPX traffic rate limited based on mls rate limiters

Resolved Caveats in Release 12.2(17b)SXA2

Resolved Security Caveats

- [CSCed93836](#)—Resolved in 12.2(17b)SXA2

A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

All Cisco products which contain TCP stack are susceptible to this vulnerability.

This advisory is available at

<http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-ios.html>, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS software.

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at <http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-nonios.html>.

Other Resolved Caveats in Release 12.2(17b)SXA2

Identifier	Technology	Description
CSCdz84583	Security	IOS fw allowing forged packets for a session initiated from inside
CSCed35253	Security	Router crash due to corrupted data in list with IOS-firewall

Resolved Caveats in Release 12.2(17b)SXA

Resolved MPLS Caveats

- [CSCeb16876](#)—Resolved in 12.2(17b)SXA

Symptoms: A Cisco router may generate a “SYS-2-GETBUF” message during the “Tag Input” process and may subsequently reload unexpectedly.

Conditions: This symptom is observed when the router fragments a Multiprotocol Label Switching (MPLS) packet.

Workaround: There is no workaround.

Resolved Routing Caveats

- [CSCeb88239](#)—Resolved in 12.2(17b)SXA

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.

Resolved Security Caveats

- [CSCec46274](#)—Resolved in 12.2(17b)SXA

New vulnerabilities in the OpenSSL implementation for SSL have been announced.

An affected network device running an SSL server based on the OpenSSL implementation may be vulnerable to a Denial of Service (DoS) attack when presented with a malformed certificate by a client. The network device is vulnerable to this vulnerability even if it is configured to not authenticate certificates from the client. There are workarounds available to mitigate the effects of these vulnerabilities.

This advisory will be posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20030930-ssl>.

Resolved Unknown Caveats

- [CSCed30113](#)—Resolved in 12.2(17b)SXA

A malformed Internet Key Exchange (IKE) packet may cause the Cisco Catalyst 6500 Series Switch or the Cisco 7600 Series Internet Router to crash and reload.

This vulnerability is documented as Cisco bug ID [CSCed30113](#). There are workarounds available to mitigate the effects of this vulnerability. Cisco is providing fixed software at no charge.

This advisory will be posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20040408-vpnsn>

Other Resolved Caveats in Release 12.2(17b)SXA

Identifier	Technology	Description
CSCec42594	AAA	Spurious access on Sup720 during configuration
CSCeb34203	Access	TX Ring Limit appears to be broken for PA-MC-E3
CSCec06146	Access	Channelized interfaces fail to come up after reconfiguration or flap
CSCec79579	Access	CWPA crash due to pas interrupt
CSCin38177	Access	C2SUP3:T3 Serial PA in Flexwan crashed @ pas_init_stub_nmi_handler
CSCin60835	Access	Show controller serial not showing all 15 min intervals
CSCdx79081	ATM	ATM vc bundle member adjacencies not getting deleted
CSCea80820	ATM	Alignment correction at atm_arp_process
CSCeb64384	ATM	ATM subif created on (OC3-SMI PA) break snmp agent
CSCec68740	Content	Remove wccp commands from CLI for SUP720

Identifier	Technology	Description
CSCec42069	Infrastructure	Service Password encryption not hashing the password
CSCec87661	Infrastructure	CHUNKBOUNDS errmsg in wrong circumstance - NAT shortcuts not install
CSCin57765	Infrastructure	appending to files on disks can crash/hang system
CSCea81952	IPServices	NAT crash due to h225/h245 without RAS
CSCec10494	IPServices	Router may crash after issuing show ip igmp tracking detail
CSCin35940	IPServices	Bridging Failed when BRI interface Encapsulation is PPP
CSCdw76355	MPLS	Clear ISIS *, RRR not announce back tunnel with fast-reroute
CSCdx39482	MPLS	MPLS TE: Explicit tunnel takes wrong outgoing interface
CSCdz04196	MPLS	Encapsulation fixup flags incorrect for MPLS TE tunnels
CSCea29102	MPLS	RP crash in BGP when clear ip bgp * and OIR/flap interfaces
CSCea83647	MPLS	Invalid tag Exp-null new incoming tag at tfib_route_tag_change
CSCeb37966	MPLS	GRP crash when configuring frr for ATOM tunnel
CSCeb68673	MPLS	IAS: tfib missing entry when VRF unconfig from ASBR-PE
CSCeb79576	MPLS	eBGP+Label: label binding present in BGP, but not in LFIB and LIB
CSCeb86270	MPLS	remote systems crash when local system reloaded
CSCec26563	MPLS	GSR crashes when configuring mpls traffic-eng tunnels
CSCec31206	MPLS	Get and Set same values on MPLS MIBs caused memory leak
CSCin53682	MPLS	IAS:router crash @ neighbor flexwan oir
CSCdx32947	Multicast	FS-HYB: static RP changes to bidir by itself, 100% CPU, AutoRP loop
CSCec41693	Multicast	RP never sends register stops
CSCec73078	Multicast	sup720: egress replication breaks mcast over secondary sup uplinks
CSCeb86171	platform-76xx	Bad EEPROM GBICs force line protocol down on WAN ports
CSCec18366	platform-76xx	OSM-ATM crashes when traffic goes through
CSCec22452	platform-76xx	QOS/RT/DB: LC crashed with TxSOP Errors
CSCec39689	platform-76xx	CHOC-12/DS3 doesnt come up when remote end change status to up/up
CSCec46892	platform-76xx	OSM-ATM:Mcast pkts are dropped over 1483 bridged PVCs
CSCec48974	platform-76xx	OSM: show contr pos pm shows incorrect optics information
CSCec52228	platform-76xx	POS-OC12+ crash after interface configured
CSCec74760	platform-76xx	7600 w/BRE configured replies to ARP even with Interface down/down
CSCec79460	platform-76xx	OSM-4GE-WAN GBIC int stays up/up though connected NPE-G1 int is down
CSCec89414	platform-76xx	pos controller increments coaps rregardless of APS configuration
CSCed00781	platform-76xx	Write erase causes SLOTSCACHE to be erased
CSCec22252	PPP	MLP, PE VIP crashed after shut down 1 of the 2 phisical int (MU).
CSCec25317	PPP	VIP crash disabling dCEF on MLP interface
CSCec34606	PPP	ALIGN-1-FATAL crash while deconfiguring cRTP on Frame Relay
CSCec61738	PPP	MLP:Pkts dropped at ingress of pe under 1ce-2pe topolog
CSCec86131	PPP	STMPA crashes continously @ vip_mlp_ll_fastsend

Identifier	Technology	Description
CSCin62978	PPP	C2SUP2:dLFI+dCRTP:FW2 crash@ ct3sw_tx_interrupt on continous traffic
CSCdy77717	QoS	removing MPLS-TE tail Loopback I/F causes crash
CSCea84387	QoS	Two simultaneous policy map displays cause problems
CSCec32573	QoS	MQC:Input Marking is based on Outgoing classification
CSCec46485	QoS	match dscp and match prec matches do not take effect.
CSCec74699	QoS	NBAR not running distributed on FlexWAN
CSCin61140	QoS	mfr: LC crashes with LFI/mqc enabled
CSCdz67496	Routing	OSPF thinks Tunnel interface is down after reload.
CSCeb04048	Routing	Upgrading/reloading IOS may cause OSPF interfaces/neighbors down
CSCeb19730	Routing	Const2:RP crash at isis_install_one_ip_route under traffic stress
CSCeb30370	Routing	Crash at ospf_flush_area_summary_lsa after no ip vrf vpn1
CSCeb61700	Routing	OSPFv3: no passive-int <int-name> incorrectly added for ipv6 int
CSCec15095	Routing	Ospf database not updated completely on shut/noshut of Interface
CSCec29868	Routing	OSPFv3 adjacency flap after switchover when standby sup comes online
CSCec30212	Routing	OSPF adjacency bounces when area <x> stub
CSCec33773	Routing	OSPFv3 does not update routes when shut interface,virt-link configur
CSCec35322	Routing	RP crashed after configuring IPv6 ACL
CSCec38322	Routing	CEF reloader holding up memory when toggling DCEF-CEF-DCEF
CSCec39973	Routing	RP crash at isis_add_is_neighbors_to_lsp
CSCec40548	Routing	OSPF not installing route in RT after removing MPLS TE area config
CSCec45770	Routing	OSPFv3 not able free lsdb_chunks after reload requested
CSCec48816	Routing	Router crash at ospf_clean_if after removing network command
CSCec49499	Routing	IOS reload hangs when OSPF is configured
CSCec64382	Routing	IPv6: Adjs failed to repopulate correctly on interface flap
CSCec68467	Routing	Memory leak in OSPFv3
CSCed06329	Routing	BGP-v6: Version number churns when multipath configured on BGP-v6
CSCeb55703	Security	Cannot ssh to router -- crc comparison failed
CSCuk39887	Security	Fixup disabled on adjacencies for tunnel interfaces
CSCdw41639	Unknown	ls1010 Silently Drops OAM F5 with oam intercept enabled
CSCdx22158	Unknown	VSEC:Stress testing crashes the router after 4hrs
CSCdz55955	Unknown	Unity: client XAUTH fails if user domain name doesnt match group nam
CSCea51081	Unknown	group lock can still allow users into wrong group
CSCea69116	Unknown	L2/L3 switched counters remain 0 in sh int vlan
CSCea85342	Unknown	19E:Uplink ports on standby fail after switchover
CSCea86396	Unknown	6500 MSFC may not program static Null 0 route into HW
CSCeb21815	Unknown	FW Some of the E1/T1 channels of a STM PA protocol goes down on rel
CSCeb49514	Unknown	Const2: Distributed port channel does not forward traffic

Identifier	Technology	Description
CSCeb54694	Unknown	C2:MSFC3: Add support for NVRAM: private-config for ARIEL Platform
CSCeb57474	Unknown	FBs do not bootup after reload in both rpr+ and handover-split modes
CSCeb61144	Unknown	C2-HYB: configuring config file to flash: causes nvram failure
CSCeb64666	Unknown	SPURIOUS mem at isakmp_send send_nat_keepalive in nat
CSCeb67996	Unknown	CE2-NATIVE:mcast traffic s/w switched for few groups with intf reset
CSCeb83650	Unknown	L2 Etherchannel across DFCs has intermittent packet loss
CSCeb86653	Unknown	CE2-HYB: MSFC2 crashed at fm_tcpintrept_find_conn_info
CSCec00570	Unknown	VLAN without SVI set to redirect instead of bridge
CSCec08629	Unknown	RLS3(ios):C6K222:SP crash while clearing lcp session to 6816 module
CSCec08973	Unknown	Invalid counters on PA-MC-STM-1SMI
CSCec14054	Unknown	Allow users to enable/disable BPDU filtering on FWSM ports
CSCec15149	Unknown	Co-existence of distributed etherchannels and mac-move notification
CSCec27686	Unknown	CSM channel does not trust DSCP (Supervisor IOS)
CSCec30461	Unknown	13E4: MPLS - BGP Learnt Prefixes incorrectly using IP mac-sa
CSCec31276	Unknown	MPLS-tagged pkts sourced from the RP are not prioritized correctly
CSCec32173	Unknown	VSEC:VPN-SM-C2: Traffic is lost if the tunnel mac address is changed
CSCec33663	Unknown	20E:Mac addresses not learnt on convertng PO auto to trunk
CSCec36559	Unknown	20E:Traffic dropped for 40-50secs when 6816 comes up
CSCec37069	Unknown	Multicast Netflow stats being exported on Cat6k
CSCec37464	Unknown	CWAN-QOS:HQoS, Vtms Qs are not proper with microcode reload
CSCec37803	Unknown	Need scp error counters per nmp for Mcast group 5
CSCec38516	Unknown	6kIOS CLI only accepts 1st command when multi remote command run
CSCec39383	Unknown	SWITCH-ENGINE-MIB,Traceback msg when mibwla cseTcamUsageTab
CSCec39937	Unknown	MSFC fails to boot when system is rebooted
CSCec40719	Unknown	Using NBAR and SRM crashes redundant MSFC
CSCec45398	Unknown	Align error on SP- Traceback: mcast_mld_accept_group
CSCec47779	Unknown	Remove inapplicable RESETNXI errmsg and change to debug info
CSCec48379	Unknown	Const2: pak expansion on rate limit index causes resets
CSCec48393	Unknown	SYS log msg is needed & power should be denied for unsupported cards
CSCec49438	Unknown	ALIGN-1-FATAL at dyntrk_set_tot when configure trunk over port-chan
CSCec50577	Unknown	Some multicast L2 entries not propagated to DFCs after reload
CSCec50648	Unknown	auto-MDIX doesnt work on ws-x6548-rj-21
CSCec51288	Unknown	13E11,20E:DFC cards fail to learn mac addresses
CSCec54433	Unknown	Sup720: SP alignment errors and MSFC crash in heartbeat_fatal
CSCec54471	Unknown	Const2:RPR+ IPC-SP-STDBY-5-WATERMARK msgs are seen continously.
CSCec55650	Unknown	Output packets not dcef switched on multilink interface
CSCec57672	Unknown	Unable To Retrieve Counters From Vlan Interface

Identifier	Technology	Description
CSCec58834	Unknown	dot1q vlan on subintf not usable if remove card & reinsert
CSCec59341	Unknown	PIM snooping command results in traceback
CSCec62406	Unknown	Micorflow policing drops should not charge ag hi policer bucket
CSCec62587	Unknown	giants on dot1q trunk with sup720 uplink ports
CSCec62788	Unknown	Flow dscp become 255 if agg.policy conform action modified
CSCec62945	Unknown	C2MCAST:STP doesnt work for both ieee and dec specification
CSCec63033	Unknown	v4 acl in team serialised mode removed on config v6acl(excep)
CSCec63462	Unknown	Support of CISCO-SYSLOG-MIB,its CLI missing from PS but in JK9S img
CSCec64282	Unknown	Failed to sync port asic on WS-6516A-GBIC and WS-6548-GE-TX
CSCec65070	Unknown	Software needs to limit total power by chassis
CSCec67234	Unknown	Multicast not working thru VPN when outside port is in routed mode
CSCec68570	Unknown	mls rate-limit unicast acl vaci-log rate limiter cfg lost on reload
CSCec68585	Unknown	CWPA/CWPA2 RP fails to recognize all Flexwans using S9 rommon image
CSCec68645	Unknown	SP crash on doing dir disk0:
CSCec77448	Unknown	System crash in idprom_ps_get_info (PS not fully inserted)
CSCec78265	Unknown	Several debugs are turned on on RP & SP after each reload
CSCec80654	Unknown	Hardware shortcuts installed without RPF traffic
CSCec80868	Unknown	lcp failed to go online after system reset
CSCec82732	Unknown	Max power limit should be increased for 6500-E chasses
CSCed13751	Unknown	VSEC:VPN-SM: Duplicate IKE sa when PIX501 is rebooted
CSCed14506	Unknown	OIR of 6816 without DFC crashes switch to rommon
CSCed15587	Unknown	System controller resets causes high cpu with 2 flow dest configured
CSCea19885	Voice	Bus error at address 0xD0D0D0B, Process CCH323_CT
CSCeb78836	Voice	h323: software forced crash if bad packet received and debug opened
CSCin56408	Voice	Tracebacks found when receiving invalid H323 setup packet
CSCeb33417	WAN	MFR: router crash during unconfiguration on MFR
CSCec59440	WAN	Small X.25 Packets Corrupted in Frame-Relay Switching on FlexWAN
CSCin53115	WAN	C2:MFRoMPLS:MFR interface goes DOWNn/DOWN on sh/no sh with AToM VCs

Caveats in Release 12.2(17a)SX and Rebuilds

- [Open Caveats in Release 12.2\(17a\)SX and Rebuilds, page 417](#)
- [Resolved Caveats in Release 12.2\(17a\)SX4, page 417](#)
- [Resolved Caveats in Release 12.2\(17a\)SX3, page 417](#)
- [Resolved Caveats in Release 12.2\(17a\)SX2, page 418](#)
- [Resolved Caveats in Release 12.2\(17a\)SX1, page 419](#)
- [Resolved Caveats in Release 12.2\(17a\)SX, page 419](#)

Open Caveats in Release 12.2(17a)SX and Rebuilds

Identifier	Technology	Description
CSCec50469	Unknown	Ethertype config accepted but not applied on 6502-10GE cards
CSCec74016	Unknown	Const2:Router crash when ipv6 ACL removed after remove isataptunnel

Resolved Caveats in Release 12.2(17a)SX4

Resolved Security Caveats

- [CSCed93836](#)—Resolved in 12.2(17a)SX4

A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

All Cisco products which contain TCP stack are susceptible to this vulnerability.

This advisory is available at

<http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-ios.html>, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS software.

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at <http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-nonios.html>.

Other Resolved Caveats in Release 12.2(17a)SX4

Identifier	Technology	Description
CSCdz84583	Security	IOS fw allowing forged packets for a session initiated from inside
CSCed35253	Security	Router crash due to corrupted data in list with IOS-firewall

Resolved Caveats in Release 12.2(17a)SX3

Identifier	Technology	Description
CSCed38862	Unknown	g1/1 of WS-X6748-GE-TX not link up after changing speed 10M or 100M
CSCed79519	Unknown	Breakpoint exception due to RPC mismatch timeout

Resolved Caveats in Release 12.2(17a)SX2

Resolved IPServices Caveats

- [CSCed27956](#)—Resolved in 12.2(17a)SX2

A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

All Cisco products which contain TCP stack are susceptible to this vulnerability.

This advisory is available at

<http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-ios.html>, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS software.

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at <http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-nonios.html>. ION is also impacted.

- [CSCed38527](#)—Resolved in 12.2(17a)SX2

A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

All Cisco products which contain TCP stack are susceptible to this vulnerability.

This advisory is available at

<http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-ios.html> and it describes this vulnerability as it applies to Cisco products that run Cisco IOS software.

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at <http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-nonios.html>

Other Resolved Caveats in Release 12.2(17a)SX2

Identifier	Technology	Description
CSCed15587	Unknown	System controller resets causes high cpu with 2 flow dest configured
CSCed49091	Unknown	Breakpoint Exception after 6724-SFP module problems

Resolved Caveats in Release 12.2(17a)SX1

Identifier	Technology	Description
CSCec42594	AAA	Spurious access on Sup720 during configuration
CSCec42069	Infrastructure	Service Password encryption not hashing the password
CSCdz04196	MPLS	Encapsulation fixup flags incorrect for MPLS TE tunnels
CSCec33773	Routing	OSPFv3 does not update routes when shut interface,virt-link configur
CSCec35322	Routing	RP crashed after configuring IPv6 ACL
CSCec45770	Routing	OSPFv3 not able free lsdbs_chunks after reload requested
CSCec48816	Routing	Router crash at ospf_clean_if after removing network command
CSCeb55703	Security	Cannot ssh to router -- crc comparison failed
CSCuk39887	Security	Fixup disabled on adjacencies for tunnel interfaces
CSCeb49514	Unknown	Const2: Distributed port channel does not forward traffic
CSCec42766	Unknown	WS-F6K-VPWR-GE/WS-F6K-PWR should power down devices req > 7000mW
CSCec45398	Unknown	Align error on SP- Traceback: mcast_mld_accept_group
CSCec48379	Unknown	Const2: pak expansion on rate limit index causes resets
CSCec48393	Unknown	SYS log msg is needed & power should be denied for unsupported cards
CSCec54433	Unknown	Sup720: SP alignment errors and MSFC crash in heartbeat_fatal
CSCec65070	Unknown	Software needs to limit total power by chassis
CSCec68645	Unknown	SP crash on doing dir disk0:

Resolved Caveats in Release 12.2(17a)SX

Resolved Infrastructure Caveats

- [CSCdz29724](#)—Resolved in 12.2(17a)SX

Symptoms: IOS Exec sessions return an error message of “login invalid”

Condition: If the username does not exist in the local username database when using local authentication.

Workaround: This bug fix will modify the behavior to wait for the password to be entered before returning the same error message as would be used if the password is incorrect.

Resolved IPServices Caveats

- [CSCea34745](#)—Resolved in 12.2(17a)SX

Symptom: A Cisco device running IOS and enabled for Hot Standby Router Protocol (HSRP) may reset with a SYS-2-WATCHDOG error from a specifically crafted malformed HSRP packet. The HSRP protocol is not enabled by default.

Conditions: The specifically crafted malformed HSRP packet would require local attachment to a segment that supports the HSRP group. This issue does not affect IOS releases 12.3 and later This issue affects in 12.2, 12.2T and 12.2S versions of IOS. This issue affects 12.1E releases prior to 12.1(23)E.

Workaround: There is no workaround.

Resolved Multicast Caveats

- [CSCea58105](#)—Resolved in 12.2(17a)SX

Symptoms: The interface of a Cisco router that functions as a Protocol Independent Multicast (PIM) Rendezvous Point may stop receiving traffic. The output of the **show interfaces** privileged EXEC command may show input queue drops.

Conditions: This symptom is observed after the interface has received PIM register packets with the Router Alert option.

Workaround: Reload the port adapter or line card with the affected interface.

Resolved PPP Caveats

- [CSCdz22366](#)—Resolved in 12.2(17a)SX

In a Virtual Private Dial-up Network (VPDN) environment, if the LAC is not configured for authentication and the user does not provide any authentication information, the authentication on the LNS may be bypassed. This problem will not occur if the LAC is configured properly to authenticate the users.

In the case of client initiated tunnels (<http://www.cisco.com/warp/public/471/l2tp-win2k-cit.html>), where there is no separate LAC, all authentication may be bypassed.

Only the IOS devices that are acting as LNS are affected. The IOS devices that are not acting as LNS are not affected.

An attacker may exploit this vulnerability to gain unauthorized access to network resources if authentication is not configured on the LAC.

The workaround is to configure “lcp renegotiation always” command in virtual private dialup network (VPDN) group configuration mode.

Resolved Security Caveats

- [CSCdy68457](#)—Resolved in 12.2(17a)SX

Symptoms: Spurious memory accesses may occur on a Cisco router, and the router may reload.

Conditions: This symptom is observed on a Cisco router that is configured for authentication proxy.

Workaround: Disable the authentication proxy feature.

- [CSCdz12098](#)—Resolved in 12.2(17a)SX

Symptom: When auth-proxy is enabled in an environment where DOS attacks from CodeRed or Nimda are present, it may be possible to exhaust resources if more than 40 DOS machines are attacking the router where auth-proxy is enabled.

Conditions: See above

Workaround: Disable auth-proxy or monitor auth-proxy cache to see attacking machines and clear viruses off machines.

- [CSCea93882](#)—Resolved in 12.2(17a)SX

Symptoms: If Cisco Express Forwarding (CEF) is disabled, a router may reload with the following error message upon the receipt of a malformed generic routing encapsulation (GRE) packet:

%ALIGN-1-FATAL: Illegal access to a low address addr=0xA30, pc=0x40992D3C, ra=0x405E64B8, sp=0x43562838

Conditions: This symptom is observed on a Cisco router that has CEF disabled. The symptom even occurs without a tunnel configuration on the router.

Workaround: Enable CEF on the router by entering the **ip cef** global configuration command.

Resolved Voice Caveats

- [CSCdz44138](#)—Resolved in 12.2(17a)SX

Symptoms: After a Session Initiation Protocol (SIP) message is received, a memory leak may occur in the CCSIP_SPI_CONTROL process on a Cisco MC3810 and the following errors are reported:

- Method Not Allowed
- Invalid CallId -
- Internal Server Error

Conditions: This symptom is observed on a Cisco MC3810 that is running Cisco IOS Release 12.2(12).

Workaround: There is no workaround.

Other Resolved Caveats in Release 12.2(17a)SX

Identifier	Technology	Description
CSCdx07849	AAA	Unable to save configuration due to startup-config file open failed
CSCds19651	Access	cablelength short 133 is not displayed on running config
CSCdt48893	Access	output stuck on PA-CE1
CSCdx33931	Access	dialer behavior is inconsistent with VJHC enabled and MPMP
CSCdy61602	Access	NRT: RSP-3-RESTART after changing encapsulation to lapb
CSCdy67459	Access	dialer interface does not work properly after reconfiguring
CSCdz00415	Access	%SCHED-2-EDISMSCRIT for Process= Compute load avgs
CSCdz31561	Access	Callback fails if dialer string different than calling number
CSCdz48147	Access	Incoming call rejected, exceeded max calls with x25 configuration
CSCdz50451	Access	spurious memory access ct3sw_show_controllers
CSCdz55396	Access	CRC errors dont show up on MC-8E1 interfaces
CSCdz71171	Access	CT3 reports LOS and FEAC when ports are up
CSCdz72292	Access	Output queue stuck on PA-MC-8E1 after some interface flapping
CSCdz75118	Access	Interface input / output rate not decreasing to zero after shutdown
CSCea21643	Access	Dialer Watch stalls
CSCea42252	Access	PA-MC-E3 bad index in DS1-MIB
CSCea42298	Access	PA-MC-E3: E3 controller is missing from MIBs
CSCea58283	Access	%RSP-3-NOIDB: bad vc 3840 error with CT3IP-50
CSCea63532	Access	c7200:ifEntry object disappears after OIR of PA-MC-T3
CSCea87183	Access	show interface serial 4/0/0/3:0 giving %invalid input detected
CSCeb24875	Access	Const2:FW MC-8T1 pkts > 1650 bytes are dropped on t1 interfaces
CSCeb45429	Access	Line protocol goes down on CT3 interface
CSCeb47812	Access	clear counter will cause CE3/cT3 PA invalid mem action(malloc)
CSCin23422	Access	In Flexwan with PA-MC-2T3+, unprovisioning T1 is not clean
CSCin24364	Access	Boot tftp <image> command gets skipped while reloading
CSCin26892	Access	Input counters zero for PA-MC-8TE1+ and PA-CE3

Identifier	Technology	Description
CSCin28487	Access	Traceback at clear_idb_subblocks while unconfiguring PA-MCTE1
CSCin34068	Access	Unable to create channel-group on PA-MC-8TE1+
CSCin35837	Access	PA-E3 Needs shut/no shut to come up after fault
CSCin39446	Access	Incorporating changes for FREEDM errata
CSCds30121	ATM	Incorrect ATM MAP entry cause SVC connectivity
CSCdv38344	ATM	ATM PA does not work when TokenRing PA-4R-FDX in lower slot
CSCdw68278	ATM	Z-CDS: allowed to configured vbr-rt for spvp connection
CSCdw87766	ATM	CEF drops counted as InPktDrop under atm PVC on PA-A3-OC12
CSCdy18923	ATM	LANE: Non-control traffic may get enqueued to control path
CSCdy31278	ATM	SNMP:SONET section/line/path alarms issue
CSCdy74214	ATM	PA-A2: VC output stuck
CSCdz37332	ATM	Removing PVC from pvc range clears vc-class bbinded to this PVC
CSCdz37449	ATM	multicast: RP announce not forwarded out OIL, S,G bouncing
CSCdz43056	ATM	debug atm oam vc x.yy enables the debug for all VCs configured.
CSCdz45785	ATM	protocol ppp unavailable under pvc/svc after CSCdz25164
CSCdz53151	ATM	CSCdj74418 fix for cisco 3600 (NM-1A-OC3MM)trlane
CSCdz59562	ATM	PA-A3-T3/PA-A3-E3: Frammer facility statistics counters with sh cntlr
CSCdz62055	ATM	Bandwidth does not recover after link flap in IMA
CSCdz63708	ATM	AToM configurations disappear after the router reloaded.
CSCdz65823	ATM	Wrong UNI version on NRP-NSP when no atm autoconfig
CSCdz67483	ATM	Encapsulation aal0 option missing for CRoMPLS
CSCdz76166	ATM	Router reloads when show atm vc <vcd#> is issued for an SVC
CSCdz76961	ATM	sh int atm shows incorrect 5 minute output rate in congested vc
CSCdz79023	ATM	ATM Sub-int goes down after clearing last SVC. Needs Int flapping.
CSCdz80585	ATM	NSP Memory Leak with SoftVC Establishment
CSCea11344	ATM	SLT:can not config abr rate-factors properly on RPM-PR/MGX8850-PXM1
CSCea11453	ATM	C7200-NP400 router crash due to SAR crash pas-atm
CSCea19552	ATM	Some ATM PVC in inactive state, when loading this code
CSCea29435	ATM	Const2:FW Jumbo frames greater than 4470 bytes are dropped on atm pa
CSCea34340	ATM	console locks up with decnet atm flexwan int config change
CSCea38882	ATM	Modular packet cleanup for ATM PAs in 7200
CSCea39282	ATM	LE-arp getting responded on blocked ports
CSCea39354	ATM	SLB causes crash when virtual ip pinged across atm.
CSCea50251	ATM	PA-A3-OC12 does not handle OAM/routing updates with priority
CSCea51113	ATM	Const2:flxw traceback @atm_encap_common() when enabling half-bdg
CSCea51200	ATM	ATM sub-interface counter update slow
CSCea61178	ATM	Unable to configure PCR/SCR to max cell bandwidth of IMA int

Identifier	Technology	Description
CSCin17264	ATM	PA-A3/A6:Packet count shown incorrectly on pvc
CSCin26592	ATM	ATM: Multiple users configuring crashes router
CSCin26599	ATM	ATM_VPoL2TPv3:Connectivity issues aft continuous low b/w traffic
CSCin28792	ATM	Can not attach policy on ATMima Subinterface
CSCin30349	ATM	bay 1 crash while doing shut no shut
CSCin32872	ATM	back to back ping fails after bay reload due to INAC VC
CSCin33339	ATM	unnecessary trace back in debug atm event output
CSCin33561	ATM	MSFC crash when an ATM uni link is configured
CSCin33673	ATM	loki_state_change: Sending config failed - IMA interface down
CSCin33887	ATM	Bad refcount in retparticle at atmdx_buf_done_interrupt
CSCin33927	ATM	pcr is sometimes less than scr in IMA using dynamic b/w feature
CSCin34322	ATM	Flexwan crash while MSFC is booting
CSCin38132	ATM	when traffic rate > police cir ATM ima crashing
CSCin40163	ATM	ATM-PA-A3 not coming up on NPE400 and NSE-1
CSCin42584	ATM	PA-A3 not coming up on 7200 with NPE150
CSCin42799	ATM	Increase rx buffers for PA-A3/A6 on NPE-G1
CSCdz41584	CableBroadband	Downstream sync loss causes Output Stuck on uBR905
CSCdz37602	Connectivity	crash when deleting a translate x25 pvc command with login keyword
CSCdz36099	Content	CAT6K: Problems with bypass auth-traffic: GRE padding
CSCdz79996	Content	Enabling WCCP causes client TCP retransmissions
CSCuk41908	Content	WCCP redirect in may be applied to an interface incorrectly
CSCdu57101	Infrastructure	Incorrect information displayed in the ifStackTable
CSCdv20075	Infrastructure	%SYS-3-CPUHOG process = IP SNMP
CSCdv46906	Infrastructure	Incorrect LocIfReason in linkUp/Down Traps
CSCdw46392	Infrastructure	modemcap not applying on lines configured with modem DTR-active
CSCdx01536	Infrastructure	Caching not implemented correctly in entityextmib
CSCdy56342	Infrastructure	service config error messages only go to console
CSCdy87341	Infrastructure	Faulty Behaviour in Config Man Mib
CSCdz16090	Infrastructure	parser will not accept more than 256 chars in a line
CSCdz32940	Infrastructure	Crash in service Compression
CSCdz36877	Infrastructure	no echo of characters on vty exec
CSCdz40472	Infrastructure	TTY2: timer_create_bg error when telneting to router
CSCdz51138	Infrastructure	ifOperStatus shows incorrect value for PPP encap interfaces
CSCdz54372	Infrastructure	compress predictor accepted for HDLC if configured before for lapb
CSCdz54387	Infrastructure	sector read error while trying to boot/read corrupted file off disk0
CSCdz55986	Infrastructure	traceback found when reload RR router
CSCdz59591	Infrastructure	appending to files on ATA flash devies does not work

Identifier	Technology	Description
CSCdz59873	Infrastructure	ATA filesystem creates multiple identical xcpa directories
CSCdz60750	Infrastructure	Squeeze operation causes too much cpu utilization
CSCdz61503	Infrastructure	NE Crashed when trying to poll NOTIFICATION-LOG-MIB using getbulk
CSCdz72593	Infrastructure	ciscoFlashMIB loses ciscoFlashPartitionTable
CSCdz75810	Infrastructure	Should not have all traps appended to snmp-server host
CSCdz81035	Infrastructure	writing crashinfo to disk0 results in corrupted file
CSCdz85695	Infrastructure	RTR: Command rtr ping jitter unconfigures rtr key-chain
CSCdz89000	Infrastructure	3660 crash on parser code while manipulating CSB-PID DB
CSCea06647	Infrastructure	format of ATA flash card fails
CSCea15879	Infrastructure	SAA: Memory leak with rtr responder (Engine1)
CSCea17144	Infrastructure	RSP software forced crash with VIP crashes
CSCea19913	Infrastructure	Memory Protection Violation error
CSCea25697	Infrastructure	Memory leak found with default interface XYZ command
CSCea28333	Infrastructure	%IPC-2-PRECLOSE tracebacks
CSCea33897	Infrastructure	Bad Requeue leads to fragmentation crash
CSCea38774	Infrastructure	show parser cache causes crash
CSCea44786	Infrastructure	privilege command does not work correctly for named access-lists
CSCea62212	Infrastructure	ATA_status timeout errors
CSCea87766	Infrastructure	<interface> is a static pool and cannot be tuned message displayed
CSCeb64604	Infrastructure	SAA 2.1.1 Latest Oper Sense: httpError for HTTP status code 200
CSCin28606	Infrastructure	Invalid interface counters after loading the image
CSCin37630	Infrastructure	Sync Problems because of router_action attempting sync
CSCin41414	Infrastructure	Router crashes at fslib_ifs_ioctl when verify command issued
CSCuk44685	Infrastructure	SSO: RRP disabled (IPC failure) after OIR on another slot
CSCdt95129	IPServices	NAT: translation fails after manual table clearing
CSCdv34346	IPServices	IDS audit breaks policy routing on a NATd interface
CSCdv54170	IPServices	AsyncQ manager failure to adjust queued calls on remote disconnect
CSCdx46319	IPServices	CMF doesnt seem to work correctly
CSCdy57048	IPServices	MPLS/Tag switching results in invalid TCP packet
CSCdz18109	IPServices	NAT router receives self generate translated packet by itself
CSCdz36526	IPServices	NAT: missing changes in CSCdx40232 umbralla commit
CSCdz38681	IPServices	add-route wont create static route unless old entry removed first
CSCdz38987	IPServices	DD keeps checking server after it is removed
CSCdz44155	IPServices	Some NAT entries have no expiration timer set and never expire
CSCdz44758	IPServices	%STANDBY-3-DIFFVIP1 syslog message gets sent out as 3 messages
CSCdz46435	IPServices	Traceback at frame_relay_extract_addr after igmp_get_mac_or_ip_sread
CSCdz51270	IPServices	Software forced crash due to NAT

Identifier	Technology	Description
CSCdz63000	IPServices	ICMP port unreachable creates NAT half entry
CSCdz76824	IPServices	Arp alias not set correctly after reload with static NAT configured
CSCdz78549	IPServices	7401 crashed at ip_nat_command after issuing wr t
CSCea07035	IPServices	alignment errors in IP NAT
CSCea10787	IPServices	Static inside network NAT does not work for multicast
CSCea17268	IPServices	HA: can not clear vty line
CSCea36425	IPServices	telnet source-interface affects session command
CSCea55449	IPServices	bus error while trying to age nat entry in 12.1(13)E04
CSCea60379	IPServices	Memory leak in LDP process
CSCdu15973	ISDN	ISDN should reject V110 calls based on LLC octet 5a
CSCdz61369	ISDN	ss7 gateway missing isdn service command after reload
CSCdz61729	ISDN	Need to disable Redirecting number IE for NTT
CSCdz86750	ISDN	need CLI to enable/disable fix for CSCdx12421
CSCdt55540	LAN	PA-2FE-TX does not support auto-neg so remove auto config commands
CSCdw00953	LAN	TX-ISL 1 port FE PA wont go DOWN immdly when carrier is lost
CSCdx63927	LAN	7200: reload due to memory corruption in PA-1FE
CSCdx80675	LAN	Spurious access at dec21140_rx_interrupt, possibly regression bug
CSCdy89749	LAN	lot of spurious access at fx1000_dtq_consumer_isl and vip crashes
CSCdz06957	LAN	Snasw virtual tokenring port drops null xid sent as SRE
CSCdz38604	LAN	Counter of collision is different between RSP and VIP
CSCdz45509	LAN	MPLS packets coming into GEIP dot1q sub. are dropped as ignore
CSCdz73287	LAN	VSEC: Gigabit Ethernet is in half duplex mode
CSCdz77618	LAN	PA GE show UP/UP when re-seated with Gbics with No cables connected
CSCdz84025	LAN	CWTLC PXF crash:Internal Error (0x00210001): Col0 CRASH_CODE_CMD_ID
CSCdz90090	LAN	VIP ignores unicast packets received from PA-2FE
CSCea22898	LAN	LLC2 does not follow N2 value
CSCea37647	LAN	Unable to maintain Full-Duplex setting when doing FEC
CSCea44850	LAN	SNA Host PU dropping when configured on Virtual-TokenRing interface
CSCea66198	LAN	Bus error when applying crypto map to fddi interface
CSCea82238	LAN	bus error when using % in vtp password
CSCec18181	LAN	sh pas i82543 interface giga1/0 MTA - crashes router
CSCin27090	LAN	Router crashes in update_dot1q_vlan_rp_out_counters()
CSCin31870	LAN	PA GE show UP/UP when re-seated with Gbics with No cables connected
CSCin43613	LAN	c7200 FE Data-plane performance degradation on flo_isp
CSCdu78087	LegacyProtocols	show x25 hunt-group status incorrect
CSCdx77062	LegacyProtocols	Snasw PUs (and LUs underneath) in Reset state after mainframe IPL
CSCdx79523	LegacyProtocols	X.25 DDR stops after first ISDN failure

Identifier	Technology	Description
CSCdy59779	LegacyProtocols	DLSw+: LLC session stuck in ADM state
CSCdz18119	LegacyProtocols	3640 router crashes at __doprnt while configuring ipx routing
CSCdz21952	LegacyProtocols	upstream cp-cp sessions flapping with sense 0x08890100
CSCdz22127	LegacyProtocols	DLSw+: CLS return code ignored on Confirm primitives
CSCdz24438	LegacyProtocols	HPR pathswitch time values should be configurable
CSCdz25898	LegacyProtocols	snaswitch dlur must report uplinks to ENs in TDU to DLUS
CSCdz25931	LegacyProtocols	allow snasw location with wildcard on just owning-cp
CSCdz40029	LegacyProtocols	DLSW ER: Buffer leak in the small buffer pool
CSCdz40331	LegacyProtocols	SNASw router rejecting CP-cap in Error-Capture.cap
CSCdz60566	LegacyProtocols	QLLC needs second call to establish DLSw circuit
CSCdz60694	LegacyProtocols	SNASW uses the same FQPCID when the second REQDACTPU is sent to VTAM
CSCdz62958	LegacyProtocols	Remove Inactive entries in snasw topology table as the TGs go inacti
CSCdz83029	LegacyProtocols	DlsW ER with GigE PA Wiseman FX1000 chipset doesnt work
CSCdz88297	LegacyProtocols	Actlu req from dspu causes snasw to queue bind requests indefinitely
CSCdz88396	LegacyProtocols	IPX-3-TOOMANYNETS displayed early when using IPXWAN interfaces
CSCea09001	LegacyProtocols	SNASw new sessions fail 0855000F Route Setup Reply sent ISR not HPR
CSCea10024	LegacyProtocols	Snasw router crash in nss_queue_handler after host IPL (99% cpu)
CSCea21073	LegacyProtocols	SNASW is causing VTAM ABEND
CSCea24708	LegacyProtocols	Ping fails while testing x25 HIC and LOC
CSCea29740	LegacyProtocols	DLSw ER broken with 7200 FE drivers in isl and dot1q encapsulation
CSCea36624	LegacyProtocols	SNASw router reloads in nba_send_ips
CSCea58092	LegacyProtocols	SYS-2-INTSCHED after unshut of a FE from portchannel with SNASw conf
CSCea60815	LegacyProtocols	SNASw PU hung in PendActPu state after host IPL
CSCea62116	LegacyProtocols	Snasw hang/crash after show snasw link, show snasw ips command
CSCea66127	LegacyProtocols	ipx eigrp packets wedge the input q on 3725
CSCea71681	LegacyProtocols	Snasw does not send REQACTPU, PU stuck Pend Actpu
CSCdz32837	Management	RM: Resource Manager Spurious access in VSNPRINTF __DOPRNT
CSCdz49271	Management	CDP broken -not receiving incoming packets
CSCea34230	Management	Router crashes while doing config change and show of CAR same time
CSCdu70170	MPLS	More than 1 vrf can assign on 1 interface and lose all vrf
CSCdv44316	MPLS	tag-switching ip propogate-ttl not recognized by parser after reload
CSCdw06558	MPLS	E4P: GRP crashes immediately after disabling mpls te tunnels
CSCdw33267	MPLS	ip_force_resolve_path not called for all parallel paths
CSCdw88145	MPLS	BGP soft reconfig make tag as explicit-null
CSCdx31291	MPLS	internet access via global keyword broken if multiple paths to NH
CSCdy09335	MPLS	MPLS: BGP updates do not occur if static route is removed
CSCdy52958	MPLS	Can not ping HSRP address from different VRF

Identifier	Technology	Description
CSCdy71876	MPLS	13E/MPLS: Spurious memory access with alignment traceback with traff
CSCdz37137	MPLS	PE to PE connectivity lost due to xtag cross-connect in DOWN state
CSCdz37794	MPLS	After SSO cutover w LC-ATM, pings not passing through
CSCdz43747	MPLS	Local label does not bind after route flapping
CSCdz51987	MPLS	concurrent mpls cos-map config overwrites current class-map var
CSCdz54206	MPLS	Debug mpls packet breaks packet forwarding in HDLC encap
CSCdz57007	MPLS	vip/rp/7200/any alignment errors or crash, mpls feature path
CSCdz61780	MPLS	Unwanted route_tag_change causes TFIB entry del and 1 sec pack loss
CSCdz66770	MPLS	LDP: Label change is not propagated/conveyed to LDP peer
CSCdz69177	MPLS	spurious access at tfib_fib_scanner_walk
CSCdz69414	MPLS	mpls ldp neighbor command garbled after ip vrf removal
CSCdz72673	MPLS	C2Sup2: system crashed on tfib_check_fib_rewrite
CSCdz75075	MPLS	Inter-AS fails with LC-ATM on ASBR and IPV4 BGP+Label exchange
CSCdz75507	MPLS	CLI should prevent config of bridge-group on an mpls interface
CSCdz81619	MPLS	MPLS packets dropped as ignored with DCEF
CSCdz85866	MPLS	MPLS/VPN: PE might fail to import some VPN prefixes
CSCdz89449	MPLS	Const2: CSC PE RP crashed when removing VRF from int tdp_get_dhcb
CSCea00530	MPLS	MPLS LDP: Label Withdraw with no label not handled properly
CSCea05061	MPLS	BOOTREPLY sourced from wrong interface in RBE MPLS/VPN setup
CSCea07570	MPLS	RSP crash at rsp_fastsend, dmlppp & mpls
CSCea09270	MPLS	CSCdt32774 reintroduced in 12.2S
CSCea25707	MPLS	LDP-MIB crashes, watchdog forced crash, where v8 upgrade not present
CSCea25789	MPLS	LDP MIB, router crash, mib walk, where v8 upgrade not present
CSCea28100	MPLS	TDP does not use configured Hello holdtime and interval
CSCea28656	MPLS	Align-3-Spurious at tagsw_tx_pak in the router of CSC-PE/ASBR/PE
CSCea35117	MPLS	Spurious memory access at bgp_bestpath_compare_pair
CSCea37722	MPLS	All rip interface showed in show ip protocol vrf xxx
CSCea56819	MPLS	crash with link failover and EoMPLS&MPLS VPN traffic
CSCea58795	MPLS	Label leaking: after VPN routes removed vpn not release local label
CSCea72654	MPLS	MPLS VPN CSC PE RP crashed after booting 410 with 1k vpn
CSCea75235	MPLS	LSC switchover - second outage found during test
CSCea80474	MPLS	Const2:FW RP crash at @ ldp_pdu_group_msgs_for_xmit during shut/nosh
CSCea84736	MPLS	CONST2: Cannot ping after shut/no-shut on POS interface with MPLS en
CSCea86724	MPLS	MVPN: P router RP crash, when the LC with VRF on PE router, CPU hog
CSCeb28065	MPLS	CONST2/MPLS: RP crash at rn_walktree_timed with overnight traffic te
CSCuk36841	MPLS	PAKSTICK Traceback @ip_fastswitch_wrapper
CSCdt82560	Multicast	mroute-cache disabled upon reload or line flap with hw compression

Identifier	Technology	Description
CSCdw75696	Multicast	Watchdog timed out during freeing of large linecard FCB queues
CSCdy60995	Multicast	Router crash in PIM RP ager after show ip pim rp mapping
CSCdz16276	Multicast	DR does not register if it already has a (S,G) with Null Olist
CSCdz37639	Multicast	Const2: Hangup or crash because of invalid radix_node chain
CSCdz39544	Multicast	MSDP: encaped data pkt with more than 1 SA entry can cause problem
CSCdz48132	Multicast	UDLR should not require a static mroute to prevent RPF failure
CSCdz52552	Multicast	PIM: Router reload, traceback at free/pim_show_interface
CSCdz59039	Multicast	Const2: Proxy join timer not reset properly, prune is not sent
CSCdz62860	Multicast	Traceback at process_send_message on cfging a frame-relay interface.
CSCdz71127	Multicast	unexpected packet can cause input queue wedge - reg to CSCdx02283
CSCea01892	Multicast	multicast fast switching not used with NAT configured
CSCea13379	Multicast	Router sends (*,G) joins instead of (*,G) join with (S,G)R prune
CSCea26993	Multicast	Dense-mode Incorrectly Sets T-flag on (s,g) if Pkt Arrives on OIF
CSCea26995	Multicast	7400:LINK-3-BADMACREG: Interface Gig0/1.251, non-existent MACADDR
CSCea29313	Multicast	CLI typo : ip multicast longest-match
CSCea46477	Multicast	Packets punted on (S,G)R entry
CSCea53049	Multicast	PIM Bidir does not have correct mroute table after oir
CSCea79487	Multicast	Bus Error crash in pim_jp_build_packet - CSCea24630 not fixed
CSCeb29878	Multicast	Need no mls ip multicast for ATM subinterfaces in FlexWAN
CSCeb76929	Multicast	CE3-NATIVE: Removing mcast boundary will not resume restricted traff
CSCec06466	Multicast	Const2: Crash in midb_re_queue_sorted+38 during the complex test
CSCin31057	Multicast	Mcast code crashes when delete an sub-intf with HSRP&MCST configed.
CSCdy11785	platform-72xx	c7206VXR bus error in printf and c7100_platform_show_env_last.
CSCdy27264	platform-72xx	PXF: Div/0 risk with police in child policy
CSCdy35153	platform-72xx	OIR, slow insertion of PA causes Error Interrupt at pci_config_read
CSCdy46150	platform-72xx	7200VXR/NPE400 malloc failures with 16mb IO and 256mb memory
CSCdy68922	platform-72xx	software forced crashed by block overrun
CSCdz23373	platform-72xx	PXF External memory exception with huge ACL
CSCdz47058	platform-72xx	Channel interface link recovery
CSCdz54538	platform-72xx	PXF: inconsistent counts in show ip cache flow
CSCdz56072	platform-72xx	i82543 Port Adapters send ISL frame with 4 extra bytes
CSCea17870	platform-72xx	need to cleanup pak on the pxf punt path
CSCea25265	platform-72xx	PXF crash when receiving large amounts of video streaming
CSCea26010	platform-72xx	7206 crashes when two PA are inserted
CSCea32437	platform-72xx	QoS policing on the Cisco 7200 NSE1 does not work
CSCea35403	platform-72xx	Discarded packets by input ACLs counted as output drops
CSCeb06567	platform-72xx	catastrophic pxf netflow problems

Identifier	Technology	Description
CSCin34382	platform-72xx	LAc router crashes at bus error exception
CSCdw49053	platform-74xx	Router crashed while reloading PB image
CSCin19645	platform-74xx	Failed to establish 50 pppoea sessions even after 30 minutes
CSCdx51367	platform-75xx	After reload some Mueslix serial interfaces do not come UP/UP
CSCdz24676	platform-75xx	LQRs and RSP value not in sync
CSCdz46018	platform-75xx	30 second input/output rate does not match byte count
CSCdz52713	platform-75xx	CEF switched packets cannot reset Last input/output counters
CSCdz70112	platform-75xx	NRT:RSP8 and RSP4+ freeze while unconfig MTU in AToM testing
CSCdz72611	platform-75xx	usedelay function is not working correctly on 7500, 7200, c6k
CSCea21328	platform-75xx	VIP Crashinfo file left open
CSCin29078	platform-75xx	Need a mechanism to recover from QA errors
CSCuk38757	platform-75xx	Problem with the Agents impl of the cardIfIndexTable
CSCds76128	platform-76xx	CWTLC POS: aps deselect message keeps rolling
CSCdx08807	platform-76xx	OSM:GE: 64 bit main interface counters are not supported
CSCdz41189	platform-76xx	13E3/PWAN2:VTMS[1]: queue failed to become idle,quid 0x9
CSCdz54502	platform-76xx	13E3: SROC packet length mismatch errors seen on linecard console
CSCdz58878	platform-76xx	13E3/PWAN2: LC crash due to vtms periodic on switchfabric oir
CSCdz62725	platform-76xx	BT: Static SVC no connectivity on BT main interface
CSCdz62748	platform-76xx	output drops seen on Gig Ethernet connection in the OSM module
CSCdz74052	platform-76xx	C2SUP2/FLO_ISP: Cannot ping between PE-CE after reload
CSCdz74625	platform-76xx	FLO_ISP/GBIC:scp_idprom_msg: BAD EEPROM on module xx errcode=1
CSCdz88585	platform-76xx	13E5/GBIC/GE-WAN2: Interface down with 1000baseT gbics
CSCea02472	platform-76xx	CWTLC Sup2:Flexwan Sup3 cbus-cmd timeout and pwrcycles on relo
CSCea15044	platform-76xx	Cat6500 with OSM module is not replicating mcast packets
CSCea18690	platform-76xx	POS keeps sending RDI-P for 10sec. after AIS-P is stopped.
CSCea21791	platform-76xx	HSRP/VRF standby router forwards traffic going thru virtual addr
CSCea24413	platform-76xx	BB: Input drops not accounted for in show int output
CSCea34141	platform-76xx	CWTLC:PR(OC3): 16 ports active lower perf than 8 ports
CSCea41242	platform-76xx	UCODE:CWTLC: OSM crashed with null OPCODE in src_mac magic
CSCea45053	platform-76xx	packets to unknown MAC are routed back incorrectly by GE-WAN
CSCea59633	platform-76xx	HSRP and override MAC should be available on same intf
CSCea76234	platform-76xx	Output drops seen on Gig Ethernet connection in the OSM module
CSCea78519	platform-76xx	Const2:DB-stats not updated from toaster to linecard
CSCea79793	platform-76xx	VLAN ID greater than 1005 not configurable under GE-WAN dot1Q
CSCea79844	platform-76xx	Override MAC writes top 4 bytes of Router MAC to zeroes
CSCeb00632	platform-76xx	IP PIM multipoint signaling needs to be removed from ATM-OSM CLionly
CSCeb04954	platform-76xx	local bus congestion on G+ card causes LDP flaps over PWAN2 OSM

Identifier	Technology	Description
CSCeb13114	platform-76xx	OSM-POS card crashes on snmp stats clear
CSCeb16918	platform-76xx	disable Sculptor->Valllen flow control to protect control pkts
CSCeb18694	platform-76xx	CONST2/oc48:TxSOP crash with fatal management errors during traffic
CSCeb31997	platform-76xx	OAM VCs not created on the LC when PVP is configured
CSCin35353	platform-76xx	POS interfaces fails to come up with keepalive using FR encap
CSCin37112	platform-76xx	c2sup2:PWAN2: OSM LC unexpectedly power cycles when reset fabric Mod
CSCdy62423	PPP	Bridging lat/mop across a PPP link truncates 4 bytes
CSCdy76871	PPP	MPLS packets fail when one E1 of a multilink bundle of 2E1 fails
CSCdz51400	PPP	Per-user route not removed after diconnection
CSCdz56776	PPP	Outgoing PPP frames are stuck on MLPPP
CSCdz65797	PPP	AUTHOR/FSM: Internal state is invalid messages in log
CSCdz65899	PPP	SYS-3-CPUHOG Task Ran for 2480 msec Multilink
CSCdz76361	PPP	7200/VXR: MLPPP is not working with CEF (due to punt adj)
CSCea01472	PPP	VIP2-50 crash at ce3_exit
CSCea16664	PPP	Distributed multilink PPP results in a VIP buffer header leak
CSCea38803	PPP	Const2:FW RP crashed at ppp_send_packet on moving the member
CSCea38851	PPP	RP crashed at mlp_fastswitch_les on peer chassis reload.
CSCea39238	PPP	dLFIoATM never comes up on interface flap and VIP crash
CSCea53696	PPP	FW STM-1 MM PA crashed after applying CBWFQ on a mlppp bundle
CSCea60211	PPP	Const2:RP crashed @ mlp_fragment on adding a mem to a mlp bundle.
CSCea72496	PPP	Alignment error in PPPoE switching path.
CSCea73586	PPP	FW ATM E3 crashes cont with traff @ dlfi_atm_bundle_process
CSCec00268	PPP	Input drops and * throttles on PPP multilink interface
CSCin08082	PPP	IOS MLP crash @ mlp_clear_group while uncfg multilink-group
CSCin21688	PPP	Ingress counters for primary member link of multilink is double
CSCin36465	PPP	Router crashes when re-adding member in the multilink bundle
CSCin40374	PPP	C2Sup3 : dlfi related counters problems
CSCin44386	PPP	Multilink interface flaps after a router reload
CSCin46014	PPP	dLFIoATM QoS : VIP crash at dlfi_do_fragment and runs out o memory
CSCin50167	PPP	dLFI broken after CSCin46014
CSCin50541	PPP	7200 and 7500 Routers crash when ppp multilink is configured
CSCdy47547	QoS	dTS increases output rate too quickly if no BECN received
CSCdy63247	QoS	high latency for MQC bandwidth class when c default with many flows
CSCdy78032	QoS	Can not recognized properly queuing type in sh queuing int virtual
CSCdy82043	QoS	VIP2-50 with PA-MC-8E1 crashes when issueing MLPPP commands
CSCdy87453	QoS	ip fragments are not classified properly for output queueing feature
CSCdz04423	QoS	CPUHOG when activating NBAR

Identifier	Technology	Description
CSCdz10519	QoS	Delayed boot-up due to QoS and dcef
CSCdz25848	QoS	Corrupted WRED DSCP counters in show policy interface CLI
CSCdz33759	QoS	router crashes while setting frame-relay cir
CSCdz40273	QoS	Support for finer grained scheduling
CSCdz41092	QoS	Spurious memory accesses at custom_dequeue
CSCdz50199	QoS	Router crashes when service policy is configured.
CSCdz51865	QoS	Router may reload if policymap/class-map is accessed simultaneously
CSCdz53696	QoS	RSVP: ResvError crashes the router
CSCdz64355	QoS	7500:Crash Attempted to free memory at D0D0D0D, no part of buffer
CSCdz68710	QoS	cosmos_e : Qos: Watchdog timeout at hqf_reset_all_blts_recursive
CSCdz74130	QoS	RSVP: Memory corruption crash while processing incoming PATH
CSCdz78276	QoS	Input policing and input acl with log causes input packet loss
CSCdz88368	QoS	Attaching nonexistent policy map to ATM subinterface
CSCdz89370	QoS	No more than 14% bandwidth can be reserved on GigabitEthernet int
CSCea02713	QoS	Bus error in fair_queue_update_class after malloc fail
CSCea06507	QoS	cant attach input shaping class to multiple FR DLCIs
CSCea06563	QoS	TE LSP does not come up after changing encapsulation HDLC to PPP
CSCea07020	QoS	Memory leak when configuring frame-relay WRED
CSCea07778	QoS	router reload @add_to_hunt_group.
CSCea11008	QoS	VIP crash if virtual interface is down which has policy with priorit
CSCea12346	QoS	Incorrect BW Allocation for CBWFQ
CSCea24835	QoS	adding priority in attached policy stops traffic from other classes
CSCea33288	QoS	Router reloads at qos_set_mark_wrapper
CSCea37783	QoS	Interleaving not functional on Mx Serial PA, 8 ports
CSCea47462	QoS	CPHUHOG on show shape queue
CSCea50942	QoS	set qos-group not working on MPLS P-router for atm p2p vc
CSCea55600	QoS	Serial Interface goes down/down on bootup.
CSCea66323	QoS	MPLS-TE: midpoint router crash after changing bandwidth at ingress
CSCeb08388	QoS	Pagent traffic dies down when QoS policy is applied to the DUT int.
CSCec03896	QoS	HQF: large packets not fragmented by FRF.12 when policy is enabled
CSCec27278	QoS	Memory leak in hqf_rp_mlp_blt_setup
CSCin28688	QoS	No drop via random-detect in ATM(OC3) Subinterface
CSCin39504	QoS	BADMAGIC detected by validblock_diagnose while removing the policy
CSCdt45079	Routing	OSPF: forwarding address in LSAs might be not updated on cfg changes
CSCdu06914	Routing	%IP-3-DESTHOST logged intermittently
CSCdv36378	Routing	BGP outbound route-map with next-hop or update-source suppress update
CSCdw50797	Routing	GRP Bus Error crash in bgp_print_entry

Identifier	Technology	Description
CSCdw84055	Routing	EIGRP MD5 Authentication Broken
CSCdx42845	Routing	%Address-family not configure Message Seen
CSCdx81633	Routing	MLS entries not updated when the route changes in the routing table
CSCdx95505	Routing	BGP: a redistribute with a route-map is not applied automatically
CSCdy04087	Routing	OSPF RT extended community has wrong value (negative or too high)
CSCdy24940	Routing	bus error at prune_ndb_idb
CSCdy40742	Routing	CPU high after BGP reset when default-metric is configured
CSCdy80496	Routing	Disappearing the route even existing on the topology table
CSCdz11578	Routing	connected routes might be missing from EIGRP topology
CSCdz20796	Routing	No passive-interface commands in config after sub-ints are created
CSCdz21986	Routing	Redistribution of newly added static routes fails
CSCdz25963	Routing	Unequal cost load sharing does not work properly on E2 and E3
CSCdz29788	Routing	Adjacencies does not come back after beginning new adj table epoch
CSCdz30390	Routing	static with next hop network not removed when component missing
CSCdz38203	Routing	Inter-AS: Asbr advertises wrong next-hop for some VPNV4 prefixes
CSCdz39896	Routing	Pri does not reconnect with ip verify unicast reverse-path
CSCdz41087	Routing	EIGRP:Connected interface not in topology table
CSCdz41310	Routing	Const2 - Memory fragmentation on RP after route flaps
CSCdz45760	Routing	OSPF LSA refresh should not cause partial SPF
CSCdz56772	Routing	CEFv6 crash when i/f state changes & connected prefix is deleted
CSCdz58047	Routing	BGP: match ip next-hop does not work for non-IPv4 prefixes
CSCdz58674	Routing	OSPF ABR generates illegal type 4 LSA
CSCdz61787	Routing	ISIS BACKUPOVFL loop : endless SPF (every SPF Interval)
CSCdz63695	Routing	Problem redistributing RIP routes into EIGRP using Route-map
CSCdz67496	Routing	OSPF thinks Tunnel interface is down after reload.
CSCdz69000	Routing	VIP4-80 running 12.2(8)T4 crashes with CYASIC Error Interrupt
CSCdz69295	Routing	ISIS IPv6 crash with multiple next-hops
CSCdz70283	Routing	crash seen at bgp_neighbor_change
CSCdz71295	Routing	Bad voice quality after several calls with CRTP
CSCdz74211	Routing	FLO_ISP: SP crashes after running L2 and L3 traffic
CSCdz76611	Routing	Router crash when remove static EIGRP neighbor statement
CSCdz77470	Routing	ipv6 address gets truncated in sh bgp ipv6 summary
CSCdz77777	Routing	software forced crash on a router after clear ip bgp
CSCdz82284	Routing	Partial flag set on db without partial spf happening
CSCdz84521	Routing	SPD broken in 7200 & rpm
CSCdz88636	Routing	bgp table inconsistent before and after clear ip bgp
CSCea00377	Routing	IPv6 CEF: Adjacency Incomplete on FDDI

Identifier	Technology	Description
CSCea01062	Routing	GSR crashed while issuing show clns interface
CSCea01840	Routing	High CPU BGP scanner
CSCea02355	Routing	rare ip packets may cause input queue wedge
CSCea03198	Routing	SYS-2-INPUTQ: no IDB traceback if netflow packet enqueued to process
CSCea03212	Routing	sh ipv6 traffic is not count up when 6pe uses
CSCea11704	Routing	crash seen at bgp_find_next_nbr()
CSCea13075	Routing	MED is not being send across confederation eBGP
CSCea14412	Routing	Crash after distribute-list command entered
CSCea17037	Routing	Queries sent to stub remotes even after CSCdy65263
CSCea19236	Routing	router reload at bgp_routemap_check_internal
CSCea22310	Routing	nhrp auth config causes crash if 8 character string is exceeded
CSCea24313	Routing	ipv6 floating default route leads route flapping
CSCea24421	Routing	ISIS not load balancing correctly
CSCea26842	Routing	IOS crashed when acl removed
CSCea28131	Routing	router crashes upon rcv invalid packet
CSCea28472	Routing	show extended channel command causes CIP Utilization of 95%
CSCea35193	Routing	ACK for duplicate DBD request not sent by SLAVE
CSCea39371	Routing	Bus error in turbo_extended_check with compiled ACLs
CSCea40722	Routing	Tarp resolve command doesnt work
CSCea42500	Routing	BGP: default route not being advertised by BGP under vrfs
CSCea43167	Routing	BGP enabled on reload can cause OSPF instability
CSCea44570	Routing	IS-IS passive-interface not work
CSCea48609	Routing	show ipv6 traffic counts forwarded packet as Received
CSCea59374	Routing	Spurious access when NetFlow exports needs to be fragmented
CSCea93577	Routing	C10720: chunk_refcount crash in 6PE InterAS during clean_up
CSCeb04048	Routing	Upgrading/reloading IOS may cause OSPF interfaces/neighbors down
CSCeb19857	Routing	router crash on reload at ip_def_metric_configured()
CSCeb24407	Routing	Link-local address configured not shows after reload/swtover
CSCeb65685	Routing	ip cef load-sharing algorithm tunnel command lost upon reset of rpm-
CSCeb80992	Routing	Crash when ACL counters are sent from the LC to the RP
CSCec03066	Routing	Const2:IPv6:static route not removed from routing table
CSCec27239	Routing	OSPFv3: RP crashed in DoToAllChildren remove use-bia feature and wr
CSCin11611	Routing	IPX EIGRP will not establish adjacencies using SAP incremental
CSCin29995	Routing	is_rtp_header failed msg observed during shut, no shut of ctrl
CSCin40371	Routing	With no ip cef, ping to 20 net failing with 60% success
CSCin52817	Routing	OSPF: Router may reload on manually reloading the router
CSCuk40771	Routing	dCEFv6: distributed switching ipv6 pkts can cause some VIPs to crash

Identifier	Technology	Description
CSCdx05703	Security	Communication brakes when WCCP+CBAC is ena together in some situatio
CSCdx22576	Security	VSEC: rsa-encr broken when VAM is active
CSCdx74855	Security	Cannot ping IP address of local GRE tunnel interface
CSCdx84417	Security	Peer crashes when clearing tcb for a STUN connection
CSCdy29077	Security	With fast switching, NAT and inspect final TCP ACK not forwarded
CSCdy79517	Security	VSEC:VPN-SM:RP crashed during hw stress test deconfig.
CSCdz54555	Security	Intermittent ISA card reset
CSCdz56722	Security	SegV exception, PC 0x8019C08C with Firewall Feature Set
CSCdz60229	Security	SSHredder SSH DoS Tool Reboots Router without Authentication
CSCdz74538	Security	VSEC:VAM anti-replay fw check needed on VAM
CSCdz78239	Security	ISA card reset trigger tunnel drops and router crash
CSCdz89852	Security	Preshared key with VAM limited to 64 byte size
CSCea00475	Security	GRE: frame-relay encapsulated frames get corrupted on decapsulation
CSCea17079	Security	VSEC:VAM2 Align Error and Spurious memory access
CSCea19444	Security	System crashed under stress with 500 tunnels
CSCea26901	Security	cbac inspection idle-timeout killing live sqlnet sessions
CSCea30449	Security	SSH Client source port shouldnt falls within 1-1023
CSCea31844	Security	TE tunnel has unexpected no route-cache config w/out configing it
CSCea32392	Security	Huge HTTP downloads fail when using auth-proxy and inspect
CSCea40426	Security	VAM encr/decr error:Other Error for some MTUs
CSCea56559	Security	1700 crash on boot in crypto_rng
CSCeb01608	Security	Inbound SSH sessions hang with debugs and term mon
CSCdw17400	Telephony	Transcoding: One way audio between 711A GW and 729/723 IP Phone
CSCdt30513	Unknown	radius password length is non-compliant with RFC 2865
CSCdw13108	Unknown	MOC: static arp does not work, ltl not updated correctly
CSCdw24379	Unknown	RADIUS attribute Framed-Filter attribute parsing incorrect
CSCdw36564	Unknown	CES: Unrecoverable Red Alarm (Loss of Signal) on 3600
CSCdw48796	Unknown	AutoInstall fails with the NM-4A/S
CSCdw59505	Unknown	need IOS CLI to make noise threshold a configurable option
CSCdw72560	Unknown	Customer cant configure differnt speed in s0 and S1 when doing CES.
CSCdx04081	Unknown	controller t1 reports line code violations
CSCdx22012	Unknown	Router crashes on moving bgp update-source int from global->any vrf
CSCdx23388	Unknown	Router crashes at rs8234_oam_receive_complete
CSCdx27398	Unknown	Hubble:all non dfc cards medusas are not sending mac notifications
CSCdx31265	Unknown	Dial FTP throughput on a downlink may degrade by 18 percent
CSCdx60079	Unknown	VIP crashes after configuring feature accel and netflow
CSCdx73043	Unknown	resource monitor not updating ds0 inuse channels for first isdn call

Identifier	Technology	Description
CSCdx86585	Unknown	Support for CP tone in the Czech republic
CSCdy03042	Unknown	cefcFRURemoved/cefcFRUInserted are missing on removing/insertingGBIC
CSCdy10714	Unknown	A config of a removed LC is not reflected on other LCs
CSCdy11767	Unknown	Disabling dot1qtunnel tagged frame still go through the link
CSCdy13419	Unknown	vpn accel dropping 1500 byte packets with df bit clear
CSCdy15369	Unknown	CWAN-QOS:class-default shouldnt have CIR = LR when QoS is applied
CSCdy18970	Unknown	Bus error at csm_send_event
CSCdy20760	Unknown	Software Forced Crash due to watchdog timeout(mai_modem_autotest)
CSCdy21998	Unknown	12e/13e: TFIB scan not completing messages on RP Console
CSCdy24304	Unknown	NM-1A-T3/E3 may stop passing traffic
CSCdy28282	Unknown	CWAN-QOS: police w/ drop action doesnt work for router gen. packets
CSCdy31164	Unknown	FIB: CEF disabled on the VIP (CEF-IPC: Unable to get the port info)
CSCdy34419	Unknown	Getting %DS_MODEM-3-LOW_PARTICLES:Not enough particles messages
CSCdy45007	Unknown	E1/R2 GW sends Answer Line Signal before B6 Signal ends
CSCdy47266	Unknown	Vortex:second fan-tray & clock entry miss from entPhysicalTable
CSCdy47341	Unknown	no tag-switching ip propagate-ttl still copy MPLS ttls to IP pac
CSCdy47789	Unknown	Non-directed LDP neighbors showing up under targetted discovery list
CSCdy49957	Unknown	12.1(13E): modules get wrongly power denied when PS fails
CSCdy55352	Unknown	Initial punting due to T flag not being set on ssm mroute entry
CSCdy55543	Unknown	IOS - msfc/msfc2 delayed or not booting from sup-slot0, 13E5, etc.
CSCdy57025	Unknown	13e: mem leak-proc=RPC draco-oir;pcle_g2_fw_admin_status_down_notifi
CSCdy59007	Unknown	Crashinfo on AS5400 does not include dump of corrupt memory blocks
CSCdy70191	Unknown	c1751 running 12.2T doesnt generate Cold Start Traps on Power up
CSCdy72977	Unknown	EAP MD5 (802.1x) RADIUS authentication fail
CSCdy81201	Unknown	crash in caim_complete_packet
CSCdy84113	Unknown	With dual sups, broadcast supp command returns 0 value
CSCdy84560	Unknown	C-HYB+HA_SRM: two switchover in 1 min makes cat6k send no packet
CSCdy86668	Unknown	spurious memory access made at is_aim_handle during ISDN/MLP call
CSCdz01387	Unknown	Spurious memory accesses after questioning cbQos MIB
CSCdz08234	Unknown	PA-MC-STM1:LP-RFI alarm cannot be disabled
CSCdz09522	Unknown	MSFC2-3-MISTRAL_BAD_PAK
CSCdz09551	Unknown	Tracebacks at aaa_acct_attr_add -- same as bug CSCdx85827
CSCdz15598	Unknown	VTSP should not pass bogus codec_bytes to crash dsps.
CSCdz19404	Unknown	CWAN-QOS: OSM crashes when heirarchical policy applied to main i/f
CSCdz19517	Unknown	LLQ-BC not engaging & sh cry eng qos not showing QoS counters
CSCdz21419	Unknown	Incorrect OIR-SP-3-PWRCYCLE reason
CSCdz21534	Unknown	T1 remote line loopback fails on CT3 card

Identifier	Technology	Description
CSCdz21587	Unknown	no mls 0.0.0.0/0 entry when non-zero default wins over 0.0.0.0
CSCdz24904	Unknown	helper-map group-address is helping broadcast traffic also
CSCdz27636	Unknown	NDE: Add unique engine ID for PFC2 exported traffic
CSCdz28754	Unknown	No status change logs dont come up in MST environment
CSCdz28877	Unknown	dialin user remain conn/dead if tacacs acl not there
CSCdz29883	Unknown	Mac Notification: L3 traffic loss with a L2 etherchannel across DFCs
CSCdz30206	Unknown	12.1(13)E1: buffer leak middle pool due to Remote Console Process
CSCdz30644	Unknown	bus error in deref_pathadj in native ios
CSCdz30790	Unknown	T3 controller link up/down traps not sent for snmp
CSCdz31376	Unknown	VIP crashes on configuring feature acceleration and dcef and cef
CSCdz32064	Unknown	MSFC: loadprog: bad file magic number: 0x0
CSCdz34982	Unknown	gre/ipsec with hardware card intermittently stops passing traffic
CSCdz35884	Unknown	NPE-G1 drops packets > 1498 even with tag mtu 1508
CSCdz36181	Unknown	PBR set interface Null 0 doesnot work in HW for Earl6
CSCdz39487	Unknown	CE interface is up even when the remote end is down
CSCdz40050	Unknown	Wrong syslog message sent when PSU is removed
CSCdz40232	Unknown	DSP does not respond when scheduler command is enabled
CSCdz40248	Unknown	CWAN-QOS: BT Traffic shaping not work with flo11e image
CSCdz40483	Unknown	%SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = IP I
CSCdz40971	Unknown	Unable to SSH directly to real servers after configuring SLB
CSCdz41650	Unknown	Lack of ip connectivity during few sec/min not reported as Lost pkt
CSCdz42307	Unknown	Multicast packets being routed when multicast routing is not enabled
CSCdz42549	Unknown	%CLS-3-BOGUSOP: Unknown CLS verb for STATION context.....
CSCdz43519	Unknown	VOICE-IF-MIB not populated with ISDN BRI info
CSCdz45188	Unknown	V110 callin-failure disable other callin
CSCdz46370	Unknown	CE1-HYB: Spurious memory access at const_fib_proc_sp_req_ipx_reload
CSCdz49099	Unknown	Called number gets overwritten between CCAPI layer and ISDN stack
CSCdz49276	Unknown	AGM: Gig0/0 intf throttles when rtp traffic received on wrong port
CSCdz50453	Unknown	Failed to send RPC request mapping_sp:get_current_mappings
CSCdz51275	Unknown	Memory leak in Buffer pool process packet header
CSCdz51932	Unknown	Reload after delete ACL that is used for crypto
CSCdz52398	Unknown	vrf not cleared when chE1 is removed
CSCdz52963	Unknown	c2600:ifType of ATM25 port adapter is invalid
CSCdz53958	Unknown	Setting cdpInterfaceEnable port in a channel=false reset switch
CSCdz54333	Unknown	incorrect unicast flooding seen on switchports
CSCdz55608	Unknown	memory leak in Crypto ACL
CSCdz55647	Unknown	RPR plus redundancy can not work for inter-vlan L3 traffic with ACL

Identifier	Technology	Description
CSCdz56987	Unknown	Configure ACL on channel member int break ACL on the L3 channel int
CSCdz57158	Unknown	Incorrect supervisor model and s/n displayed for sup
CSCdz58142	Unknown	%BSC-3-BADLINESTATE: Line state Tx when receiving xxx on line Serial
CSCdz58247	Unknown	Extensive frame loss upon link rejoining GEC with PAGP
CSCdz59003	Unknown	DE bit mapping for FR-ATM internetworking is broken.
CSCdz59578	Unknown	IOS should give DSP more time for codec download
CSCdz59821	Unknown	TCP intercept connections are getting reset after 24 hrs
CSCdz60032	Unknown	SMTP reports unknown error message 554 when doing offramp with VXML
CSCdz60980	Unknown	Download through sup-slot0/sup-disk0 fails - checksum incorrect
CSCdz61466	Unknown	AIM VPN/MP not encrypting/decrypting packets
CSCdz62845	Unknown	Cronos:APS switchover causes RP to crash, high CPU util
CSCdz63050	Unknown	NPE-G1:Output drop and bad length count up
CSCdz65299	Unknown	Bus Error crash in ipmulticast-loopback, ipsendnet, ipwrite
CSCdz66347	Unknown	On reload, static multicast L2 entry not processed by igmp-snooping
CSCdz66927	Unknown	Voice-ports Hung and Digits not being pulsed out
CSCdz67182	Unknown	CWAN-QOS:PFC aggregate policing not work for cwtlc
CSCdz68529	Unknown	Got EARL-SP-5-EXCESSIVE_INTR:
CSCdz69161	Unknown	Reoccurrence of CSCdz21420
CSCdz69690	Unknown	PRI T1 voice ports are down. Incoming calls fail
CSCdz69965	Unknown	VSEC:VPN-SM:RP/SP crash after reloading with 800 tunnels
CSCdz70721	Unknown	No Mls-cef entry for dynamically learned default entry via EIGRP.
CSCdz71296	Unknown	Removing template while configured on another tty reloads router
CSCdz71663	Unknown	5300 DSPRM dsp boot-up double-load recovery alarms problems.
CSCdz73517	Unknown	Channelised STM1 SMI PA reports line type as Multimode
CSCdz74155	Unknown	NM-HDV: Router crashes during booting sequence after reload command.
CSCdz74603	Unknown	spurious memory access in qde_get_ctrs_from_cmap_list
CSCdz76292	Unknown	Crash configing fair-queue/no fair-queue during stress test
CSCdz76588	Unknown	13E: RPC call failure under stress condition
CSCdz76698	Unknown	flo_isp: Sending 1000 multicast traffic, sp get Seg violation
CSCdz79139	Unknown	BGP convergence fails with FIB Control Task taking 100% CPU
CSCdz81658	Unknown	NPE-G1: Increasing MTU may cause native GE port receive ring lockup
CSCdz83037	Unknown	flo_isp/BCP:Show mac-address-table static interface is not working
CSCdz84447	Unknown	show vlan leads to high interrupt driven CPU load
CSCdz85694	Unknown	SYS-2-INTSCHED: may_suspend when changing GigE config on NPE-G1
CSCdz85729	Unknown	PA-MC-STM1:E1s are not synchronized with STM1 frame
CSCdz86512	Unknown	CE1-HYB:OC12 POS card not recognised when changing from NDR to DR
CSCdz87238	Unknown	SLB: http probe GET requests not specific about file requested

Identifier	Technology	Description
CSCdz88518	Unknown	VRF-Lite not supported in Hybrid
CSCdz89162	Unknown	PWAN:Mcast packets are not hardware switched if changing ISL to .1Q
CSCdz89258	Unknown	Traffic stops after BGP prim to sec peer failover with large ACL
CSCdz90377	Unknown	spurious error at hal_tx_interrupt
CSCdz90594	Unknown	OC-48 DPT only sends multicast packets out side-A
CSCCea00720	Unknown	CPU of DR goes high when hit by high rate Non-RPF dense mode traffic
CSCCea01505	Unknown	Supervisor22 and DFC EOBC retry timer workaround (improved version)
CSCCea02291	Unknown	RSP crashes at tagsw_flow_get
CSCCea02680	Unknown	Output packet counter for SVI is incorrect
CSCCea02744	Unknown	Ignore-dcd does not function on 3620 serial WIC modules
CSCCea03617	Unknown	AIM-VPNII - disabled on boot up
CSCCea04706	Unknown	Dangling DSP on AS5300 - DSP resource recovery
CSCCea05105	Unknown	13E4:QoS:Sup2CR:cannot configure COS-MAP on uplink ports
CSCCea06319	Unknown	backup commands removed from serial interface after reload
CSCCea07370	Unknown	output drops when using PXF due to matches against ACL
CSCCea07557	Unknown	SPD does not work on AS5300 Fast Ethernet
CSCCea07643	Unknown	13E:CWAN_QOS:4Mb shaping granularity on PWAN2 is too limited
CSCCea07970	Unknown	Various Trap issues in RPR, RPR+, OIR Standby Sup, etc.
CSCCea09302	Unknown	RP crashes in pimv2_send_refresh when switch dense->bidir
CSCCea09674	Unknown	Busyout (slot) with CT3 DFC drops all calls
CSCCea11485	Unknown	Probe sends arp requests to remote real servers
CSCCea13771	Unknown	ubr7100 may crash upon reload
CSCCea14557	Unknown	Voice path is not cut through by SETUP_ACK
CSCCea15290	Unknown	Const2:allow-default in uRPF isnt preserved in RPR+ setup
CSCCea15655	Unknown	CDP neighbors for port-channels show same local interface for member
CSCCea15963	Unknown	MVPN: Redundant PE sends duplicate MDT-joins
CSCCea17364	Unknown	ODM breaks VACL capture
CSCCea18561	Unknown	Static Multicast CAM entry disappears from the mac-addr-table
CSCCea20948	Unknown	Bridging over PPP broken on rsp-pv-mz (and other images)
CSCCea21064	Unknown	IDMGR-3-INVALID_ID: bad id to id_to_ptr Traceback message is seen
CSCCea21781	Unknown	PBR not working in HW (hardware) with SUP2/MSFC2
CSCCea25622	Unknown	NPE-G1 - Reset by hardware watchdog timeout with no traceback
CSCCea26983	Unknown	GRE doesnt work with PXF
CSCCea27037	Unknown	Unknown CPU displayed on NPE-G1(CPU:SB-1)
CSCCea27138	Unknown	MVPN: MDT-data mappings on recv PE not deleted, bad refcount.
CSCCea27336	Unknown	ACL with deny port eq 0 block non-initial fragmented packets
CSCCea27431	Unknown	Sup1/Sup2 IOS cant ping CMM and vice versa

Identifier	Technology	Description
CSCea28325	Unknown	Fix build breakage due to CSCdx33049
CSCea28471	Unknown	VIP crash in tagsw_flow_get, at bootup or steady-state
CSCea28575	Unknown	OSM-4GE-WAN-GBIC module returns incorrect portType
CSCea29849	Unknown	Cef receive breaks with decnet config changes
CSCea31842	Unknown	HA2: Active SP crashes in VTP code for stack memory running low
CSCea34259	Unknown	Mpls netflow egress on ATM sub-intf turns on ldp address-message
CSCea35846	Unknown	Const2: No PVID, type incon, root or loop inconsistency generated
CSCea37725	Unknown	MPLS:VPN:CHOCx:MLPPP:No connectivity over Proton int. in ce-pe link
CSCea37935	Unknown	SLB VIP not responding to pings with FWLB.
CSCea38189	Unknown	config from tftp broken service config missing from show run
CSCea38945	Unknown	NPEG1: PA-2FEISL-TX crashes upon bootup or noshut
CSCea39298	Unknown	7600: sub-int ifIndex disappears when modifying vlan encapsulation
CSCea39633	Unknown	MSFC2 experiences bus error exception - const_fib_enqueue_fib_req
CSCea40015	Unknown	Native: VTP Transparent switch passes update from diff domain
CSCea41123	Unknown	Loopback receive CEF entry not present in Sup2 CEF table.
CSCea41980	Unknown	Catalyst 6000 Native crashes with Failed to send RPC request msg
CSCea42188	Unknown	autostate interoperability with lb and sensors
CSCea42504	Unknown	ICMP fail across L3 EtherChannel
CSCea43709	Unknown	Const2:Show mac-address does not respond from RP
CSCea43871	Unknown	PA-MC-STM loop on sonetPathIntervalEs
CSCea44864	Unknown	Const2:locIfCollisions return negative value for l3 vlan.
CSCea45950	Unknown	VLAN-do-not-learn-bit set for active vlan --> unicast flooding
CSCea46236	Unknown	12.1(13E): excessive collisions on EOBC channel
CSCea47314	Unknown	not able to autoboot when all vlans are down
CSCea47607	Unknown	Delay in dispatching data received on asynch WIC-2A/S interface
CSCea48170	Unknown	IOS-SLB RLB casa replication causes memory corruption and reload.
CSCea50623	Unknown	C-NATIVE: Sup11: Crash in c7100_dma_pack_coalesce in send mcast pack
CSCea51320	Unknown	MSFC2 crashes with Illegal access to a low address with IP inspect
CSCea54148	Unknown	Need tag2tag load balancing on OSM and Flexwan .
CSCea54756	Unknown	HSRP preempt causes high cpu when slb inservice standby configured
CSCea56746	Unknown	DMFR unreliable under load - %SYS-2-INLIST: Buffer in list
CSCea59575	Unknown	L2 entries dont age out after disabling and then reenabling aging
CSCea59922	Unknown	Bcast and MultiCast 64 bit counters not working on GE-WAN main int.
CSCea60527	Unknown	FWSM: Vlan 1 not working with MP , so image download fails
CSCea61460	Unknown	C2:failed to assign rate limiter to multicast non-rpf, #3 was free
CSCea61966	Unknown	IOS-SLB: RLB backup with sticky radius username may reload.
CSCea62217	Unknown	Wedged queue if inbound CAR is configured

Identifier	Technology	Description
CSCea62335	Unknown	Clear ip route all causes CPUHOG & core dump
CSCea63521	Unknown	Catos mistp bpdu not tunneled thru switch running IOS
CSCea64751	Unknown	router reload when DSL interface uses s/w with CSCdz51275
CSCea65695	Unknown	FW STM-1 PA crashed @ vip_mlp_ip_fib on starting the traffic.
CSCea66858	Unknown	%SM-SP-4-BADEVENT: Event insert is invalid Standby gone
CSCea67226	Unknown	Cat6000:With large number of NAT overload flows recip paks FIB switc
CSCea68988	Unknown	BPDU with old root bridge priority sent after max age expiry
CSCea69116	Unknown	L2/L3 switched counters remain 0 in sh int vlan
CSCea69334	Unknown	C2: ifIndex does NOT persist after RPR+ switchover and reload
CSCea70621	Unknown	VELA-SP-4-ERR_INTRPT: Interrupt ST_OVL_ERR reoccurring log message
CSCea71481	Unknown	ISIS doesnt work over GRE tunnel
CSCea71694	Unknown	Native 6500 Nam2 Module causes Autostate not to work
CSCea72405	Unknown	multicast static L2 entries not processed correctly
CSCea72468	Unknown	EoMPLS vlan needs to allow output shaping policy on CLI
CSCea72525	Unknown	Const2: default send by FM breaks feat asso betw primary & sec pvlan
CSCea72771	Unknown	netflow stats are not accurate with low fast aging times
CSCea79633	Unknown	13E: Sup crash when GBIC module is removed and stp portfast is chang
CSCea80062	Unknown	Many esp_seq_fail with MLPPP and hardware locks IPSec tunnel up
CSCea80221	Unknown	19E : Multicast traffic process switched after OIR
CSCea82353	Unknown	PIM Register & Register stop messages are looped until TTL expires
CSCea82782	Unknown	CE2-HYB:Creating 1000 vlan on RP in srm mode, resets RP
CSCea83414	Unknown	stack-mib portname command gets erased upon reboot
CSCea83603	Unknown	NDE sends ARPs when NFC is on remote network
CSCea84940	Unknown	Cannot route between 1483 PVCs in different VLANs on ATM OSM
CSCea85251	Unknown	no mls ip cef arp-throttling not NVGENed and disappears from config
CSCea85883	Unknown	Multicast flows may become software switched after rapid OIF changes
CSCea86541	Unknown	flowmask changes not enforced on command line
CSCea87362	Unknown	DMFR does not work with fast switched traffic
CSCea87671	Unknown	MPLS-QoS marking problem on PE
CSCea88502	Unknown	Proton:NXDS0 flap with LC reload while unidir traffic is flowing
CSCea89099	Unknown	after WS-X6816 reset, L3 traffic to HSRP mac, into 6816 SW switched
CSCea89468	Unknown	Continuous link flaps on port on a WS-x6348 module
CSCea90470	Unknown	Native: WS-X6348-RJ-21 no link after dis/re-connect IBM FE OSA/E
CSCea91600	Unknown	19E/C2SUP2:clear mac-add dyn int stops packet switching
CSCea93328	Unknown	mrrouter configurations has no effect after reload and shut/no shut
CSCeb00126	Unknown	Default route learnt via routing protocol not updated on switch-side
CSCeb00351	Unknown	IOS-SLB: RLB - cisco msid-based access problems with HA Acct.

Identifier	Technology	Description
CSCeb00678	Unknown	sup crash while making csm config changes
CSCeb03367	Unknown	router reloads in bundle mode config at atm_getvc with SYS-3-CPUHOG
CSCeb03414	Unknown	const2: BPNfpoe index not cleared on receiving leave on port
CSCeb04343	Unknown	Fragmented Packets matching deny ACE with no L4 ports fwded in HW
CSCeb05093	Unknown	Switch may reload if insufficient initial memory for SLB.
CSCeb05464	Unknown	Some routed frames are dropped on the GEC/dot1q trunk over DFC modul
CSCeb05517	Unknown	boot variable is not added or overwritten
CSCeb05672	Unknown	SLB processed switch packets are dropped in router.
CSCeb05818	Unknown	19e: vlans ifIndex not synced to NAM
CSCeb06811	Unknown	Loop-inconsistent port has designated role
CSCeb09340	Unknown	RLB does not pass AcctStop pkts to correct SSG when maxclients excee
CSCeb11577	Unknown	Egress lookup disabled on DFC, causes flooding
CSCeb17471	Unknown	SP crashed in FATAL EXCEPTION: 0xF floating point exception
CSCeb17597	Unknown	Netflow entries installed for Non TCP/UDP flow in NAT
CSCeb18414	Unknown	ICC-SP-5-WATERMARK: pkts for class MCAST-HW-LC are waiting to proces
CSCeb18552	Unknown	Default route learnt via routing missing or incomplete in sp TCAM
CSCeb18618	Unknown	VPNSM: IKE Traffic needs to be marked as Precedence 6
CSCeb18943	Unknown	OSM-DPT: SRP Rate-limit high does not work correctly
CSCeb21202	Unknown	Undefined route-map cause intermittent loss of L3 connectivity
CSCeb21292	Unknown	MOC/SRP linecard crash with clear counter on the lc console
CSCeb22952	Unknown	SUPPORT FOR TOS BYTE PRESERVATION WITH GRE
CSCeb23191	Unknown	Const2:RPR:After switchover some C2 modules dont come online
CSCeb23201	Unknown	XCONNECT has different checks for VLAN @ provision and authorization
CSCeb27549	Unknown	19E:switch crash w/:SP: EthChnl assert failure:
CSCeb28084	Unknown	CSG: Cannot configure content defn with same IP, different VLAN.
CSCeb28275	Unknown	13E/19E: Policing doesnt work after switchover.
CSCeb29441	Unknown	CWAN-EoMPLS:Service-policy with multiple actions is broken
CSCeb32189	Unknown	sup720 crashes at process = UDLD
CSCeb33177	Unknown	Output of show mls ip non-static shows dynamic entries as well
CSCeb35612	Unknown	Module WS-X6348-RJ-45 is excessivly resetting
CSCeb36253	Unknown	Cat6K may reload with process watchdog at FIB Control Task.
CSCeb38062	Unknown	19E-renumber:no arp, adjacency is drop for static route after bootup
CSCeb38084	Unknown	Const2/BT:LC crashes on applying dss policy on atm multipoint subint
CSCeb38485	Unknown	Const2: sup720 crashes due to FM memory corruption
CSCeb40557	Unknown	CE2-NATIVE: Cannot write configs to NVRAM
CSCeb42402	Unknown	19(E1): RPR+ swover can cause cwan main interface datapath failure
CSCeb45403	Unknown	non-RPF traffic on SRP interface not HW dropped

Identifier	Technology	Description
CSCeb46918	Unknown	router crashed at ipaccess_checksum_on
CSCeb47047	Unknown	%SNMP-3-TRAPBLOCK message received with Traceback
CSCeb47151	Unknown	Uplink port config not synced upon RPR+ swover
CSCeb47607	Unknown	RPR mode fails to recognize flexwan modules at boot up
CSCeb47640	Unknown	CE2-HYB:T48:dest. router gets no tcp packets with cef route-cache
CSCeb47669	Unknown	19E:Tcp Intercept with empty ACL doesnt allow any traffic except TCP
CSCeb48670	Unknown	Cat6K : SP crashing with corrupted PC at sm_post_event
CSCeb48884	Unknown	CE2-HYB: Mcast out-of-sync between RP and SP during Anycast-RP test
CSCeb49134	Unknown	Native:HA SUP crashes due to bus error signal=10 using RPR
CSCeb49514	Unknown	Const2: Distributed port channel does not forward traffic
CSCeb49605	Unknown	CE2-NATIVE:SUP11 OIR causes mcast packet drop if OIF is L3 port
CSCeb49634	Unknown	slot/port not initialized for vlan interface in show policy-map
CSCeb50412	Unknown	Multicast packets switched by both software and hardware (FIB FULL)
CSCeb51698	Unknown	faulty fan causes SUP to crash.
CSCeb51785	Unknown	when SP is low in memory, no crashinfo is generated
CSCeb52142	Unknown	TTFIB inconsistent with TFIB on cwtlc
CSCeb52169	Unknown	Tag adjacencies point to incorrect local label on OSM
CSCeb53215	Unknown	Crash in pagp_switch_mp.c 287
CSCeb54698	Unknown	Interface rate counters do not increment on OSM-12CT3/T1
CSCeb54936	Unknown	IOS does not provide all 96 15 min intervals for T3 and T1 int
CSCeb55216	Unknown	CE2-NATIVE:All packets drop using VACL Capture and NAT with BDD
CSCeb55271	Unknown	Complementary fix to CSCdy15598 / QoS Default Bucket Policer Problem
CSCeb57796	Unknown	7603 with a 950W DC power-supply denies power to line modules
CSCeb60262	Unknown	Deleting/renaming vlans using vlan database may trigger VTP pruning
CSCeb60961	Unknown	GE OSM 64 bit SNMP counters wrap at 2^32
CSCeb62692	Unknown	CE2-NATIVE:Adding new OIF fills MET table,causing mcast packet drop
CSCeb63548	Unknown	R4: crash changing from R2 to R3/4 style configurations
CSCeb64392	Unknown	snmp-server host configuration fails
CSCeb65671	Unknown	Wrong local vc label is programmed for data plane
CSCeb67650	Unknown	WS-X6548-GE-TX & WS-X6148-GE-TX may drop frames on egress
CSCeb69582	Unknown	6500 Native IOS:in corner cases acls get applied on wrong interfaces
CSCeb72014	Unknown	Static MAC address turns dynamic on DFC card.
CSCeb72466	Unknown	IKE fsm crash on rx of bad notify
CSCeb75803	Unknown	RP crashes after CPU_MONITOR messages have not been sent for 150 sec
CSCeb76023	Unknown	TC counters not working with MST
CSCeb77077	Unknown	Spurious access occurred at dot1q_ether_vlan_demux
CSCeb78428	Unknown	sup720/dfc3a: vla stats not working for mcast w/ ingress replication

Identifier	Technology	Description
CSCeb80326	Unknown	13E10: config loss in NDR running config
CSCeb80453	Unknown	CE1-NATIVE:VACL,packets sent to the destination on vlan shutdown
CSCeb83558	Unknown	VRF communication problem after adding subinterface on PE
CSCeb87003	Unknown	CE1-HYB:CBAC:tcp sessions fail after rpr+ switchover
CSCec00232	Unknown	Cat6000 - PAUSE frame causes High CPU when FC disabled
CSCec00966	Unknown	13E10:Etherchannel port comes up as suspended after reload on Sup22
CSCec02275	Unknown	CSM: vserver sticky mask changed to 255.255.255.255 on cfg dnld
CSCec03005	Unknown	13E10:L3 traff not forwarded for 10min on 6816 on doing clear mac dy
CSCec04451	Unknown	HA/RPR+ %SYS-SP-2-BADSHARE:Bad refcount in datagram_done on LC OIR
CSCec07319	Unknown	13E10:mls ip directed broadcast rpr+ swover all pkts hit software
CSCec08966	Unknown	%SYS-STDBY-2-CFORKMEM:Process creation of RFSS_server_action failed
CSCec10112	Unknown	ROMMON variables are not cleared by write erase on Sup720
CSCec10363	Unknown	FM-2-TCAM_MEMORY: Request to make error message more meaningful
CSCec14288	Unknown	13E10:L3 Traffic not forwarded across DFC for 3 minutes or more
CSCec16666	Unknown	two channel group interfaces of PA-MC-STM1 have same ifindex
CSCec18681	Unknown	C2: Berytos: Janus --> SSA CRC errors on Rx datapath
CSCec18683	Unknown	19E1:crash in l2_ufp_limit_source_flood_update_history
CSCec20522	Unknown	mem leak - Master Running Configuration Sync proc; resetting NDR
CSCec21124	Unknown	20E:Sup22 comes up with minor diagnostic error
CSCec22581	Unknown	Incorrect value for ciscoEnvMon mib objects for some modules
CSCec24628	Unknown	Sampled Netflow Stalls Under Heavy Load
CSCec31276	Unknown	MPLS-tagged pkts sourced from the RP are not prioritized correctly
CSCec32816	Unknown	%C6KPWR-SP-4-PSREDUNDANTBOTHSUPPLY message missing upon PS recovery
CSCec48379	Unknown	Const2: pak expansion on rate limit index causes resets
CSCin27542	Unknown	After reload, RP stops receiving OAMs from LC for an ima sub-intf
CSCin33181	Unknown	a2a Et-VI: Imposition VIP crash when OIR core-facing VIP in traffic
CSCin33334	Unknown	7200: Calls failing for E1R2 non-compelled signaling
CSCin35198	Unknown	PA-MC-STM1:Sonet MIB data not getting updated
CSCin35854	Unknown	PA-MC-STM1:Controller shutdown after reload, if too many interfaces
CSCin37176	Unknown	PA-MC-STM1:RFI, RDI alarm may bring down E1 when in local loopback
CSCin37330	Unknown	Wrong return value of portType for GBIC ports in 4OC3 & 1OC48 cards
CSCin37567	Unknown	PA-MC-STM1: FIFO block 2047 never used.
CSCin37893	Unknown	PA-MC-STM1:some of the E1s remain down when Insufficient FIFOs
CSCin40363	Unknown	crash on executing no tag-switching mtu
CSCin50930	Unknown	Const2 : DC RTP command is not propagated to the flexwan with STM
CSCin51334	Unknown	SLB will be in a Loop when a GTPv0 req with destination port 2123 co
CSCin52105	Unknown	CWPA2:dmlfr:MFR bundle link flaps along with MFR bundle

Identifier	Technology	Description
CSCin56266	Unknown	Router crashes at sss_sip_info_free with FRoMPLS
CSCuk37312	Unknown	multicast static mac address entries removed on reload
CSCuk42146	Unknown	code corruption at 0x602A0244 to 0x3040000 on RRP only
CSCdu07504	Voice	sh voice dsp causes reload
CSCdw20927	Voice	Bus error when processing alert timer in CS_CutProgress
CSCdx17219	Voice	Caller ID need to support Bellcore variation in Canada
CSCdy61597	Voice	decodeAndPrintQ931IEs may cause memory corruption
CSCdz20801	Voice	Memory corruption on As5850 as Voice GW
CSCdz37574	Voice	VOFR keepalive are not restarted after it times out
CSCdz38268	Voice	Bus error at sipSPISendBye
CSCdz40015	Voice	ALIGN-1-FATAL: Illegal access to a low address
CSCdz48635	Voice	Reload @ cpm_enqueue_calls_list/cpm_dequeue_calls_list during calls
CSCdz49277	Voice	Disconnected calls show as refused calls
CSCdz53326	Voice	Channel is stuck on S_TSP_WAIT_RELEASE state
CSCdz54800	Voice	RAS GW registration fails at boot time if security password too long
CSCdz60807	Voice	Router crash few hours after adding use-proxy command
CSCea22981	Voice	Using reserve <dsp> command crashes 7200 with NPE G1 on reboot
CSCea32240	Voice	H323 crashes in strncpy when receiving invalid setup packet
CSCea33065	Voice	H323 Spurious memory access in h450ProcRcvdApdus
CSCea36231	Voice	Router hangs when receive in invalid h225 setup
CSCea46342	Voice	h.323 crashes in ACFnonStandardInfo DEC_ERR=13
CSCea51030	Voice	h323: proxy crashes when malformed h225 setup message received
CSCea51076	Voice	h323: proxy crashes when processing invalid h225 setup messafe
CSCea54851	Voice	h323 proxy: crash at pxy_proc_rcv_SETUP when invalid h225 setup rx
CSCea64747	Voice	VAD Agressive overrides VAD configuration after reload
CSCin28504	Voice	OIR removal of uninitialized PA-MCX-8TE1 crashes router
CSCdz25535	VPDN	NAS-Port attribute is getting corrupted on multihop router
CSCdz66576	VPDN	VPDN failure manager Traceback
CSCdz67847	VPDN	l2f/l2tp needs to drop invalid PPP packets
CSCea11967	VPDN	LNS not sending SLI when LCP is renegotiated
CSCea19848	VPDN	Packets dropped at client with CEF/MLP at LNS and dialer MTU<1500
CSCea46367	VPDN	L2TP tunnel not established if user logged without realm
CSCdu05871	WAN	PA-T3 will not come up in the flexwan even if looped
CSCdv13877	WAN	Boot time is 45 minutes to 1 hour with 2000 VCs on FlexWAN
CSCdw64588	WAN	Huge delay in fast switching from tunnel to FlexWAN port
CSCdx69085	WAN	L2TP:snmp trap problem when the Virtual-Access interface up/down
CSCdy30537	WAN	Serial subint goes down after reload with frame-relay de-group

Identifier	Technology	Description
CSCdy46026	WAN	CE-HYB: %ATMPA-3-CMDFAIL: ATM8/1/0 Command Failed at ../src-rsp/rsp_
CSCdz00624	WAN	After configure no ip cef router starting to drop packets
CSCdz09542	WAN	HSSI interface wedged
CSCdz16414	WAN	The NTP on ONS15104 does not stay synchronized
CSCdz16768	WAN	The RRs that Cisco 2610 send have delay times at diverse times
CSCdz33003	WAN	Traceback found for dconfig tests with POS interface
CSCdz38136	WAN	Flexwan Multi-channel-T1 : frame-relay pvc counters skewed
CSCdz38482	WAN	Router crashes with SegV exception
CSCdz40567	WAN	Counter overflow error occurs on ip protocol
CSCdz46845	WAN	HC counters remain at 0 for POS interfaces in FlexWAN module
CSCdz48092	WAN	PA-MC-STM-1SMI interface comes up, router crashes
CSCdz58282	WAN	VIP crash - FRF.11 Annex C fragmentation
CSCdz60567	WAN	Cannot switch back to H/w compression
CSCdz61586	WAN	ATM VC bundling precedence mapping does not work on Flexwan w Hybrid
CSCdz61962	WAN	Cat6k: MLS Enabled ATM Connection Problems
CSCdz70716	WAN	POS interface doesnt increment broadcast counters
CSCdz73574	WAN	PA-POS-OC3SMI hang and needs router reload
CSCdz78099	WAN	MFR: MFR interface can no longer be configured
CSCdz85565	WAN	IPHC regression failing on M4T interfaces
CSCea12025	WAN	MFR: memory leak on 2621XM in high traffic load
CSCea17496	WAN	Flexwan with ATM pa resets due to Deadman Timer.
CSCea27953	WAN	FW 1483 bridged PVCs remain in INAC status on reload.
CSCea34094	WAN	SDLC traps flooding for unknown SDLC link
CSCea38967	WAN	Make sure pkt cleanup is complete for Mx HSSI-B PA
CSCea40836	WAN	MFR: ADD_LINK_REJ message includes Cause IE with invalid Length
CSCea46073	WAN	Running configuration does not show changes in NTP password
CSCea56687	WAN	ATM VC bundling precedence mapping does not work on Flexwan
CSCea63940	WAN	Peer reset on FW oir:Failed to allocate IPC buffer loveletter
CSCea71196	WAN	FW:hardware NAT not working on ATM flexwan PA
CSCea71729	WAN	Command srp srr enable appears after reload in SRP interface
CSCea79535	WAN	Receipt of illegal range DLCI prevents LMI exchange
CSCeb37354	WAN	Flexwan double counts input packets on frame-relay PVCs
CSCeb72381	WAN	MLFR -New MFR intf with ospf config -OSPF-6-ZERO_BANDWIDTH Traceback
CSCin08621	WAN	%CBUS-3-CMDTIMEOUT seen on reload with multiple LCs
CSCin12517	WAN	VIPMLP:Traffic loss on scaling multilink on 2CT3+
CSCin27157	WAN	c2sup2:HalfBridging:Output packet counters are not updated
CSCin41295	WAN	ATM sub-interfaces remain down after OIR

Identifier	Technology	Description
CSCin45088	WAN	Flexwan with PA-MC-E3 crashing when OIR is done
CSCin50105	WAN	IMA link protocol status displayed incorrectly
CSCdz52774	Wireless	The GGSN reloads due to Illegal access to a low address
CSCea44554	Wireless	GGSN reload with BUS error while updating fast cache
CSCea62665	Wireless	Bus error at acct_cleanup
CSCin40563	Wireless	GGSN delete all PDP contexts for a particular SGSN during update con

Caveats in Release 12.2(14)SX and Rebuilds

- [Open Caveats in Release 12.2\(14\)SX and Rebuilds, page 446](#)
- [Resolved Caveats in Release 12.2\(14\)SX1, page 446](#)
- [Resolved Caveats in Release 12.2\(14\)SX, page 447](#)

Open Caveats in Release 12.2(14)SX and Rebuilds

Identifier	Technology	Description
CSCdy84624	QoS	Flexwan rebooting when NBAR is configured
CSCea67226	Unknown	Cat6000:With large number of NAT overload flows recip paks FIB switc
CSCea71219	Unknown	linecard resets due to invalid fib ipc packet
CSCea71196	WAN	FW:hardware NAT not working on ATM flexwan PA

Resolved Caveats in Release 12.2(14)SX1

Identifier	Technology	Description
CSCin32872	ATM	back to back ping fails after bay reload due to INAC VC
CSCin33561	ATM	MSFC crash when an ATM uni link is configured
CSCin33673	ATM	loki_state_change: Sending config failed - IMA interface down
CSCin34322	ATM	Flexwan crash while MSFC is booting
CSCdz71127	Multicast	unexpected packet can cause input queue wedge - reg to CSCdx02283
CSCea60211	PPP	Const2:RP crashed @ mlp_fragment on adding a mem to a mlp bundle.
CSCea73586	PPP	FW ATM E3 crashes cont with traff @ dlfi_atm_bundle_process
CSCdy11767	Unknown	Disabling dot1qtunnel tagged frame still go through the link
CSCea35846	Unknown	Const2: No PVID, type incon, root or loop inconsistency generated
CSCea61460	Unknown	C2:failed to assign rate limiter to multicast non-rpf, #3 was free
CSCea62335	Unknown	Clear ip route all causes CPUHOG & core dump
CSCea65695	Unknown	FW STM-1 PA crashed @ vip_mlp_ip_fib on starting the traffic.
CSCea66858	Unknown	%SM-SP-4-BADEVENT: Event insert is invalid Standby gone

Identifier	Technology	Description
CSCea69334	Unknown	C2: ifIndex does NOT persist after RPR+ switchover and reload
CSCea71481	Unknown	ISIS doesnt work over GRE tunnel
CSCea82353	Unknown	PIM Register & Register stop messages are looped until TTL expires
CSCeb00678	Unknown	sup crash while making csm config changes
CSCeb05818	Unknown	19e: vlans ifIndex not synced to NAM
CSCeb11932	Unknown	Port-channel interfaces will not come up after RPR+ sw/over
CSCeb17471	Unknown	SP crashed in FATAL EXCEPTION: 0xF floating point exception
CSCin35854	Unknown	PA-MC-STM1:Controller shutdown after reload, if too many interfaces
CSCin27157	WAN	c2sup2:HalfBridging:Output packet counters are not updated
CSCin41295	WAN	ATM sub-interfaces remain down after OIR

Resolved Caveats in Release 12.2(14)SX

Resolved PPP Caveats

- [CSCdz22366](#)—Resolved in 12.2(14)SX

In a Virtual Private Dial-up Network (VPDN) environment, if the LAC is not configured for authentication and the user does not provide any authentication information, the authentication on the LNS may be bypassed. This problem will not occur if the LAC is configured properly to authenticate the users.

In the case of client initiated tunnels

(http://www.cisco.com/en/US/tech/tk801/tk703/technologies_configuration_example09186a00800946f5.shtml), where there is no separate LAC, all authentication may be bypassed.

Only the IOS devices that are acting as LNS are affected. The IOS devices that are not acting as LNS are not affected.

An attacker may exploit this vulnerability to gain unauthorized access to network resources if authentication is not configured on the LAC.

The workaround is to configure “lcp renegotiation always” command in virtual private dialup network (VPDN) group configuration mode.

Other Resolved Caveats in Release 12.2(14)SX

Identifier	Technology	Description
CSCdy61602	Access	NRT: RSP-3-RESTART after changing encapsulation to lapb
CSCdz75118	Access	Interface input / output rate not decreasing to zero after shutdown
CSCin34068	Access	Unable to create channel-group on PA-MC-8TE1+
CSCdz67483	ATM	Encapsulation aal0 option missing for CRoMPLS
CSCin28792	ATM	Can not attach policy on ATMima Subinterface
CSCin38132	ATM	when traffic rate > police cir ATM ima crashing
CSCdz36877	Infrastructure	no echo of characters on vty exec
CSCdz40472	Infrastructure	TTY2: timer_create_bg error when telneting to router

Identifier	Technology	Description
CSCdz51138	Infrastructure	ifOperStatus shows incorrect value for PPP encaps interfaces
CSCdz81035	Infrastructure	writing crashinfo to disk0 results in corrupted file
CSCin28606	Infrastructure	Invalid interface counters after loading the image
CSCdy57048	IPServices	MPLS/Tag switching results in invalid TCP packet
CSCdz36526	IPServices	NAT: missing changes in CSCdx40232 umbrella commit
CSCdz46435	IPServices	Traceback at frame_relay_extract_addr after igmp_get_mac_or_ip_srcad
CSCdz76824	IPServices	Arp alias not set correctly after reload with static NAT configured
CSCdy89749	LAN	lot of spurious access at fx1000_dtq_consumer_isl and vip crashes
CSCdz90090	LAN	VIP ignores unicast packets received from PA-2FE
CSCdz43747	MPLS	Local label does not bind after route flapping
CSCdz57007	MPLS	vip/rp/7200/any alignment errors or crash, mpls feature path
CSCea09270	MPLS	CSCdt32774 reintroduced in 12.2S
CSCea17870	platform-72xx	need to cleanup pak on the pxf punt path
CSCdz74858	platform-75xx	RSP16 crash in rsp_input_raw_prefetch and rsp_mip_fs
CSCdz41189	platform-76xx	13E3/PWAN2:VTMS[1]: queue failed to become idle,quid 0x9
CSCdz58878	platform-76xx	13E3/PWAN2: LC crash due to vtms periodic on switchfabric oir
CSCdz74625	platform-76xx	FLO_ISP/GBIC:scp_idprom_msg: BAD EEPROM on module xx errcode=1
CSCdz76361	PPP	7200/VXR: MLPPP is not working with CEF (due to punt adj)
CSCea38851	PPP	RP crashed at mlp_fastswitch_les on peer chassis reload.
CSCdz53696	QoS	RSVP: ResvError crashes the router
CSCdz74130	QoS	RSVP: Memory corruption crash while processing incoming PATH
CSCea02713	QoS	Bus error in fair_queue_update_class after malloc fail
CSCea06563	QoS	TE LSP does not come up after changing encapsulation HDLC to PPP
CSCea07020	QoS	Memory leak when configuring frame-relay WRED
CSCin28688	QoS	No drop via random-detect in ATM(OC3) Subinterface
CSCdz41310	Routing	Const2 - Memory fragmentation on RP after route flaps
CSCdz45760	Routing	OSPF LSA refresh should not cause partial SPF
CSCdz76611	Routing	Router crash when remove static EIGRP neighbor statement
CSCdz77777	Routing	software forced crash on a router after clear ip bgp
CSCea02355	Routing	rare ip packets may cause input queue wedge
CSCea03212	Routing	sh ipv6 traffic is not count up when 6pe uses
CSCea24313	Routing	ipv6 floating default route leads route flapping
CSCdz74538	Security	VSEC:VAM anti-replay fw check needed on VAM
CSCdy84560	Unknown	C-HYB+HA_SRM: two switchover in 1 min makes cat6k send no packet
CSCdz21419	Unknown	Incorrect OIR-SP-3-PWRCYCLE reason
CSCdz29883	Unknown	Mac Notification: L3 traffic loss with a L2 etherchannel across DFCs
CSCdz51932	Unknown	Reload after delete ACL that is used for crypto

Identifier	Technology	Description
CSCdz53958	Unknown	Setting cdpInterfaceEnable port in a channel=false reset switch
CSCdz57158	Unknown	Incorrect supervisor model and s/n displayed for sup
CSCdz59821	Unknown	TCP intercept connections are getting reset after 24 hrs
CSCdz65299	Unknown	Bus Error crash in ipmulticast-loopback, ipsendnet, ipwrite
CSCdz66347	Unknown	On reload, static multicast L2 entry not processed by igmp-snooping
CSCdz67182	Unknown	CWAN-QOS:PFC aggregate policing not work for cwtlc
CSCdz69161	Unknown	Reoccurrence of CSCdz21420
CSCdz69965	Unknown	VSEC:VPN-SM:RP/SP crash after reloading with 800 tunnels
CSCdz76698	Unknown	flo_isp: Sending 1000 multicast traffic, sp get Seg violation
CSCdz87238	Unknown	SLB: http probe GET requests not specific about file requested
CSCdz89258	Unknown	Traffic stops after BGP prim to sec peer failover with large ACL
CSCea07970	Unknown	Various Trap issues in RPR, RPR+, OIR Standby Sup, etc.
CSCea13771	Unknown	ubr7100 may crash upon reload
CSCea15655	Unknown	CDP neighbors for port-channels show same local interface for member
CSCea18561	Unknown	Static Multicast CAM entry disappears from the mac-addr-table
CSCea35846	Unknown	Const2: No PVID, type incon, root or loop inconsistency generated
CSCea39633	Unknown	MSFC2 experiences bus error exception - const_fib_enqueue_fib_req
CSCea41980	Unknown	Catalyst 6000 Native crashes with Failed to send RPC request msg
CSCea43709	Unknown	Const2:Show mac-address does not respond from RP
CSCea45950	Unknown	VLAN-do-not-learn-bit set for active vlan --> unicast flooding
CSCea59575	Unknown	L2 entries dont age out after disabling and then reenabling aging
CSCea63521	Unknown	Catos mistp bpdu not tunneled thru switch running IOS
CSCin37567	Unknown	PA-MC-STM1: FIFO block 2047 never used.
CSCdz16414	WAN	The NTP on ONS15104 does not stay synchronized
CSCdz38482	WAN	Router crashes with SegV exception
CSCdz61586	WAN	ATM VC bundling precedence mapping does not work on Flexwan w Hybrid
CSCdz73574	WAN	PA-POS-OC3SMI hang and needs router reload
CSCea27953	WAN	FW 1483 bridged PVCs remain in INAC status on reload.

