Caveats in Release 12.2(33)SXI and Rebuilds

Caveats Open in Release 12.2(33)SXI and Rebuilds

Identifier	Component	Description
CSCue59987	cat6000-energywise	Input queue size becomes negative with energywise enabled.
CSCsu68054	cat6000-firmware	Cat6k Platform changes required for BGP 4-bytes AS Numbering
CSCsv53086	cat6000-firmware	ipv6 traffic route-cache switched at ipv6ip tunnel (over mpls)c tail end
CSCsw50021	cat6000-firmware	After SSO, FIBIDBINCONS1: An internal software error occurred
CSCsw70162	cat6000-firmware	C2W21: Span port capture duplicated port-channel packets after SSO
CSCsx08647	cat6000-firmware	Traceback at bitlist_validbit within vs_ltl_mgr_proc
CSCsx31739	cat6000-firmware	Outbound policy changes does not reflect by itself in MTR Code base
CSCsx76244	cat6000-firmware	Sup720-Standby continuously reboots on psec mac-move violation with prot
CSCsy24099	cat6000-firmware	get platform-provided x-matrix table on RP
CSCsy27228	cat6000-firmware	Eagle_cnh: Match statement fail to match prefixes
CSCsy47965	cat6000-firmware	FID:for non existent fid ACL on the switch, authz is success
CSCta03464	cat6000-firmware	VPLS VC hardware entry lost upon reroute and TE FRR tunnel shutdown
CSCtb95854	cat6000-firmware	%IDBINDEX_SYNC-4-RESERVE: Failed to lookup existing ifindex, on LV & RV
CSCte71854	cat6000-firmware	ACE 30 and ACE 20 reboots in SSO redundency
CSCtj52310	cat6000-firmware	C2wa1: VSS coming up in RPR after switchover w/ dual-active fast-hello

Identifier	Component	Description
CSCtj66981	cat6000-firmware	MET2 is not programmed for new SR translation rules added in ISSU RV
CSCtn12371	cat6000-firmware	SPA-IPSEC-2GE: XDR-6-XDRLCDISABLEREQUEST / Traceback
CSCtn76064	cat6000-firmware	ACE 30 and ACE 20 reboots in SSO redundency
CSCue53095	cat6000-firmware	ISSU fails between SXJ & SXI on sup32/s720-10G for certain versions.

Caveats Resolved in Release 12.2(33)SXI12

Resolved gsr-boot Caveats

- CSCsv74508—Resolved in 12.2(33)SXI12

  Symptom: If a linecard is reset (either due to an error or a command such as hw-module slot reload) at the precise time an SNMP query is trying to communicate with that linecard, the RP could reset due to a CPU vector 400 error.

  Conditions: This symptom occurs when the linecard is reset (either due to error or a command such as hw-module slot reload) at the precise time an SNMP query is received.

  Workaround: There is no workaround.

Resolved ospf Caveats

- CSCug34485—Resolved in 12.2(33)SXI12

  Summary: Multiple Cisco products are affected by a vulnerability involving the Open Shortest Path First (OSPF) Routing Protocol Link State Advertisement (LSA) database. This vulnerability could allow an unauthenticated attacker to take full control of the OSPF Autonomous System (AS) domain routing table, blackhole traffic, and intercept traffic.

  The attacker could trigger this vulnerability by injecting crafted OSPF packets. Successful exploitation could cause flushing of the routing table on a targeted router, as well as propagation of the crafted OSPF LSA type 1 update throughout the OSPF AS domain.

  To exploit this vulnerability, an attacker must accurately determine certain parameters within the LSA database on the target router. This vulnerability can only be triggered by sending crafted unicast or multicast LSA type 1 packets. No other LSA type packets can trigger this vulnerability.

  OSPFv3 is not affected by this vulnerability. Fabric Shortest Path First (FSPF) protocol is not affected by this vulnerability.

  Cisco has released free software updates that address this vulnerability.

  Workaround: Workarounds that mitigate this vulnerability are available. This advisory is available at the following link:
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130801-lsaospf.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5.8/5.8:
  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:P/A:P/E:H/RL:U/RC:C CVE ID CVE-2013-0149 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL:
  http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

Identifier	Component	Description
CSCsw43080	rsr-bridging	Traceback seen @ data_inconsistency_error_with_original_ra

Caveats Resolved in Release 12.2(33)SXI11

Resolved nat Caveats

- CSCtg47129—Resolved in 12.2(33)SXI11

  The Cisco IOS Software implementation of the virtual routing and forwarding (VRF) aware network address translation (NAT) feature contains a vulnerability when translating IP packets that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are not available.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-nat

  Note: The March 27, 2013, Cisco IOS Software Security Advisory bundled publication includes seven Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the March 2013 bundled publication.

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

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar13.html

Resolved Cisco IOS Caveats

- CSCua63614—Resolved in 12.2(33)SXI11

  Symptom: When Energywise is enabled on Cat6500 switch, input queue drops can be seen on the interfaces connected to other Energywise neighbors

  Conditions: EnergyWise is enabled on Cat6500 and on connected device

  Workaround: None

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 3.3/2.4: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:A/AC:L/Au:N/C:N/I:N/A:P/E:U/RL:OF/RC:C No CVE ID has been assigned to this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

Other Resolved Caveats in Release 12.2(33)SXI11

Identifier	Technology	Description
CSCth74527	—	Cat6K: Timing issue with diagnostics corrupt data-forwarding registers
CSCub94186	—	MPLS TE FRR with auto-bandwidth causes hw adj leak/glean on recalc
CSCud08574	—	Vlan Interface over Serial - IPCP nego and Vlan link-up race condition
CSCud95251	IPServices	static nat with vrf looses vrf name after nat translations expire

Identifier	Technology	Description
CSCue21223	IPServices	Intermitant HSRP hellos not sent w/ IP NAT redundancy configured on SVI

Caveats Resolved in Release 12.2(33)SXI10

- CSCty25257—Resolved in 12.2(33)SXI10

  Symptom: Packets sent in clear on encrypted link

  Condition: Cisco Software in Cisco VPN Services Port Adaptor for Catalyst 6500 contains a vulnerability that could allow an unauthenticated, remote attacker to gain access to sensitive information on a targeted system.

  The vulnerability resides in the encryption library used by the vulnerable software. This library allows a portion of an encrypted packet to be sent unencrypted in the following packet. The vulnerability is specific only when Internet Protocol Security (IPSec) is used, as in the case with Virtual Private Network (VPN) environments. If an unauthenticated, remote attacker could access an encrypted session, the attacker could obtain unencrypted packets that would contain information. This attacker could possibly benefit from this information and possibly launch further attacks.

  Workaround: None.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4.3/3.6:

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

  CVE ID CVE-2011-4667 has been assigned to document this issue.

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

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

Other Resolved Caveats in Release 12.2(33)SXI10

Identifier	Technology	Description
CSCsz53034	—	no ingress flows on tunnel interface if nat done before reaching tunnel
CSCtg11421	—	All egress traffic dropped by SIP-400 + BusConnectivityTest failure
CSCtj99724	—	SXI1: Memory leak in "mls-msc Process"
CSCto73878	—	Intermittent PAT Order-of-Operations problem
CSCtq38041	—	InterAS OptAB ASBR crash upon reloading peer
CSCtr67722	—	SP CPUHOG on VSS setup with span session
CSCtr92285	—	MPLS L2VC down as no SSM ID allocated to VC
CSCts27161	—	VSS:standby reloads due to parser return error command: duplex full
CSCts90103	—	Buffer leak on the RP due to IPC messages resulting in a crash
CSCts98176	—	RRI routes missing while IPsec SA is up
CSCtt96152	—	VSS: corrupted Portchannel: LTL missing VSL-link
CSCtu22335	—	On a 6500 after a sup switchover arp inspection fails to forward arp
CSCtw61876	—	IGMPv3 leave results in MCAST packet loss for other receivers
CSCtw89269	—	Ports in 2X1GE-V2 SPA is not coming UP with configured speed

Identifier	Technology	Description
CSCtx12231	—	Config Sync: Bulk-sync failure due to PRC mismatch in ACL
CSCtx50235	—	SP and RP mutually resetting each other hides the actual crash reason
CSCty00274	—	TLB exception with WAN cards
CSCty07538	—	Incorrect static NAT translation leads to TCP reset
CSCty15494	—	Memory leak in cfib_fibsb_chunk
CSCty20876	—	Show stack does not show correct Information of Last System Crash - SP
CSCty20953	—	Dot1x Re-AuthZl failure with PC connects to AVAYA IP phone
CSCty61152	—	Back out fix for CSCtt66441
CSCty97492	—	Not all ARP queries going out when port-channel (DEC) is brought back up
CSCtz12050	—	Not possible to disable hol-blocking for X6148
CSCtz45931	—	MVPN traffic drops when a Port-Channel member module is OIRed
CSCtz72735	—	Mcast traffic on vrf is dropped on shutting one of the paths to the host
CSCtz91260	—	bootup traceback @ %REGISTRY-SPSTBY-3-STUB_CHK_OVERWRITE:
CSCua02641	—	Multicast traffic has second drop during SSO/NSF
CSCua08028	—	Multicast traffic drops under the VRF with IPv6 Family after MVRF upgrad
CSCua31268	—	VRF-lite : ipv4 multicast traffic loss after "no address-family ipv6"
CSCua43298	—	Port loopback mode may not be cleared in corner case
CSCtf84248	AAA	AAA Failover not happening for a directed request
CSCti24577	Infrastructure	Loading a config with banner command creates config sync issues
CSCtk36938	Infrastructure	%SYS-SP-3-CPUHOG @preemption_forced_suspend
CSCty04899	Infrastructure	6500 - Smart Call Home ignores custom http port configuration
CSCtz74540	Infrastructure	2 Sup VSS - Mistral interrupt on SP : old active remains in RP Rommon
CSCsx28822	IPServices	Memory leak in the Redundancy inter-device feature (rf task)
CSCtq41121	IPServices	IOS NAT: unable to reconfigure static nat ports after removal
CSCtz85702	IPServices	NAT TCP pptp-control timing-out use_count 1 - entry not removed
CSCua43193	IPServices	Dynamic NAT'g of TCP traffic fails when redudancy VIP is used for NAT
CSCua70136	IPServices	NAT VRF with PAT - PPTP translation failure with dynamic pool
CSCub18395	IPServices	PAT not working when shut/no shut nat+hrsp config interface
CSCtc42278	ISDN	%DATACORRUPTION-1-DATAINCONSISTENCY - ISDN incoming call
CSCtd54694	Management	Switch crashes on Show cdp neighbor detail in some conditions
CSCsq83006	Routing	Port-channel down makes EIGRP SIA
CSCtf54561	Routing	Crash in 'show ip cef vrf' with large number of entries
CSCtn02656	Routing	BGP filtering is incomplete after prefix-list reconfiguration
CSCto02448	Routing	Lost of BGP as-path when clearing BGP soft- all become Local routes
CSCtx01476	Routing	Config Sync: Bulk-sync failure due to PRC mismatch in ACL
CSCtz84714	Routing	IPv6 : snmpwalk on cIpAddressPfxOrigin does not return /64 subnets
CSCty26147	Security	CIPSO pkt. not getting ignored on tunnel interface running 12.2(33)SXI6

Caveats Resolved in Release 12.2(33)SXI9

Resolved Infrastructure Caveats

- CSCtr91106—Resolved in 12.2(33)SXI9

  Summary: A vulnerability exists in the Cisco IOS software that may allow a remote application or device to exceed its authorization level when authentication, authorization, and accounting (AAA) authorization is used. This vulnerability requires that the HTTP or HTTPS server is enabled on the Cisco IOS device.

  Products that are not running Cisco IOS software are not vulnerable.

  Cisco has released free software updates that address these vulnerabilities.

  The HTTP server may be disabled as a workaround for the vulnerability described in this advisory.

  This advisory is available at the following link:
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 8.5/7:
  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:S/C:C/I:C/A:C/E:F/RL:OF/RC:C CVE ID CVE-2012-0384 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL:
  http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

Resolved IPServices Caveats

- CSCtr28857—Resolved in 12.2(33)SXI9

  Summary: A vulnerability in the Multicast Source Discovery Protocol (MSDP) implementation of Cisco IOS Software and Cisco IOS XE Software could allow a remote, unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available. This advisory is available at the following link:
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-msdp

  Note: The March 28, 2012, Cisco IOS Software Security Advisory bundled publication includes nine Cisco Security Advisories. Each advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all vulnerabilities in the March 2012 bundled publication.

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

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar12.html

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 7.1/5.9:
  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C CVE ID CVE-2012-0382 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL:
  http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

- CSCts12366—Resolved in 12.2(33)SXI9

  Symptoms: Memory may not properly be freed when malformed SIP packets are received on the NAT interface.

  Conditions: None

  Workaround: None

  Further Problem Description: None.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5/4.8: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:N/C:N/I:N/A:P/E:F/RL:U/RC:C CVE ID CVE-2011-2578 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

Resolved Cisco IOS Caveats

- CSCts38429—Resolved in 12.2(33)SXI9

  The Cisco IOS Software Internet Key Exchange (IKE) feature contains a denial of service (DoS) vulnerability.

  Cisco has released free software updates that address this vulnerability. This advisory is available at the following link: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-ike

  Note: The March 28, 2012, Cisco IOS Software Security Advisory bundled publication includes nine Cisco Security Advisories. Each advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all vulnerabilities in the March 2012 bundled publication.

  Individual publication links are in "Cisco Event Response: Semi-Annual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar12.html

Other Resolved Caveats in Release 12.2(33)SXI9

Identifier	Technology	Description
CSCsb02158	—	RSA-SIG without CA not working with usage-keys on 2811
CSCte44826	—	memory leak in cfib_alloc_sb running SXH3a
CSCth01912	—	Tbs @VSL manager on SSO
CSCtj46927	—	MF:Access Vlan is removed when 802.1x is enabled on port
CSCtq35225	—	Any new SVIs -> NOT coming up due to RP process SW VLAN RP getting stuck
CSCtr73095	—	LAG data-ports going into Suspended with extend Vlan
CSCts26267	—	Standby VSS switch reloads due to parser return error
CSCtt00490	—	snmpwalk for a N/A DOM-value is returning a bogus value
CSCtt17210	—	On setting crcSrcERSpanLoVlanMask to zero, device goes for a reset.
CSCtt18651	—	cat6000-qos and Traceback after a no shut of a port system crash
CSCtt23872	—	QoS queueing commands are rejected after manual OIR of module

Identifier	Technology	Description
CSCtt26784	—	SUP32 crashes on power cycle "registration timer event"at 12.2(33)SXI6
CSCtu38265	—	MA2 : Crash seen with http auth-proxy
CSCtu75030	—	FTP of exception core dump after crash times out
CSCtw44733	—	command "default interface" break the cos map on other interfaces
CSCtw85000	—	On 7600, 'snmp trap link-status' out of sync on WAN GiGE interface.
CSCtx15569	—	SPA-IPSEC-2G crash packet size above 1800
CSCtx99818	—	ISSU from SXI6 to SXI9 failed
CSCth64138	AAA	CPU high@'AAA ACCT Proc' session remains after user disconnects
CSCts80209	AAA	Cat6k switch crash on "no login block-for" with login quiet-mode
CSCto06915	Infrastructure	Sup720 remains in ROMMON after SP crash
CSCto70125	Infrastructure	High CPU due to IPSLA tcpConnect probess due to multiple start attempts
CSCts71958	Infrastructure	Last Reload reason in the show version scenario
CSCtx68100	Infrastructure	Reload reason not displayed correctly on some platforms
CSCtt70568	IPServices	PPTP timeout entries are never removed from NAT table.
CSCtq73473	Management	MF: Crash when entering the 'show cdp interface' command
CSCtv97307	MPLS	MLPS LDP flaps with high Tag Control and IPRM CPU utilization
CSCtf21128	Multicast	(S, G) fwd int is NULL while (*, G) is correct
CSCtr22007	QoS	Bus Error crash in MPLS TE LM Process on 7600
CSCtw48209	QoS	RSVP trap sent when MPLS-TE RSVP session state change may cause crash
CSCtf27303	Routing	6PE interop: Cisco router sends MP_UNREACH_NLRI in not negotiated SAFI
CSCtg79258	Routing	33SB7 PE does not send withdraw to CE for 0/0
CSCtr58203	Routing	Upgrade from 12.2(33)SXH5 to 12.2(33)SXI6 ip local policy w/ VRF
CSCto60047	Security	Chunk corruption crash on trying to abort "show tech" over SSH

Caveats Resolved in Release 12.2(33)SXI8a

Identifier	Technology	Description
CSCtt26784	—	SUP32 crashes on power cycle "registration timer event"at 12.2(33)SXI6

Caveats Resolved in Release 12.2(33)SXI8

Resolved Cisco IOS Caveats

- CSCto72927—Resolved in 12.2(33)SXI8

  Symptoms: Configuring an event manager policy may cause a cat4k to hang.

  Conditions: Configuring a TCL policy and copying that policy to the device.

  Workaround: None.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 3.7/3.1: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:L/AC:H/Au:M/C:N/I:N/A:C/E:F/RL:OF/RC:C No CVE ID has been assigned to this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

Other Resolved Caveats in Release 12.2(33)SXI8

Identifier	Technology	Description
CSCsm43012	—	Speed value changed during the upgrade automatically from 10M to 100M
CSCtg96982	—	Memleak @ bitlist_chunk_alloc on VSS on standby switch
CSCth22344	—	ACE30 sub-module cefcModuleOperStatus returns missing
CSCth48435	—	Tracebacks seen on reduncdancy force with BFD
CSCti01971	—	Active router crashes @ bfd_ipv6_get_local for scaled bfd ipv6 configs
CSCtj44456	—	CSM redundancy sync via CLI causes Standby SUP crash if ANM used
CSCtj84234	—	Packets drop is there when configuring VRF
CSCtl77057	—	TestErrorCounterMonitor can generate false positive on 67XX cards
CSCtn68317	—	Cat6500/SXI: DHCP snooping removed from vlan on module OIR
CSCtn81945	—	MVPN extranet corrupted linkage
CSCto90846	—	Tunnel I/F and Vlan I/F stucked on output and dropped packets on Cat6k.
CSCto99774	—	Crash in vtp mib
CSCtq24526	—	Memory corruption crash in crypto code
CSCtq48027	—	MVRP: Traffic is NOT flowing in the netwok with MVRP enabled
CSCtq54944	—	Minor Error and port down on Failover from SXH2a to SXJ in RPR mode
CSCtq61884	—	DHCP snooping for unicast not working to HSRP DMAC
CSCtq80394	—	mroute entry not create for sparse default-MDT group
CSCtq86628	—	Traceback at SSO SCHED-SW2_SP-7-WATCH uninitialized boolean "rf task"
CSCtq94581	—	voice domain cannot authc when port-security is enabled (MDA mode)
CSCtr03012	—	On SSO, Mcast RPF-MFD fails only with static join @ RPF i/f
CSCtr26476	—	cat6k not always putting the link going to VS sup to FWD via uplinkfast
CSCtr46076	—	crash due to: terminated due to signal SIGBUS, Bus error: MF
CSCtr47317	—	Span replication loop after switchover on Service Module
CSCtr50629	—	Entity Display MIB shows incorrect ACTIVE & POWER MGMT LED status in VSS
CSCtr51180	—	IPSEC-2G in CC on subif reprograms badly icpu vlan map on change
CSCtr51517	—	SSH UNEXPECTED_MSG debugs do not display IP address
CSCtr52081	—	packet storm with external loop on dot1x/mab ports in singlehost mode
CSCtr61390	—	Standby SUP crash @ when its booting with SXI and SXJ image
CSCtr67276	—	PBR within a VRF with object tracking not working on Cat6k
CSCtr68112	—	SW installed NF entry does not get updated when next-hop sends garp

Identifier	Technology	Description
CSCtr84253	—	cat6k rapidly exhausts system buffers
CSCts15934	—	VSS: MALLOC failure reported by diag_display_fpoe_entries
CSCts57516	—	EzVPN server disconnects all PATed clients
CSCts66142	—	Reconfiguring "mls ip multicast stub" config does not program tcam
CSCts91215	—	after Sup OIR the SPA cards show as online diagnostic state unknown
CSCtt21565	—	QoS: bandwidth remaining percent of non-LLQ policy is not reflected
CSCtb89424	Infrastructure	Crash at saaEventProcessor
CSCsb70368	IPServices	Bus error at ipnat_delete_entry with PPTP-TCP entry deletion
CSCtn07696	IPServices	6506-E/Sup720 crash related to SYS-3-URLWRITEFAIL: and TCP-2-INVALIDTCB
CSCtq14817	IPServices	Traceback seen @ ipnat_pptp_client_inside
CSCtr16396	IPServices	TAC+ Code Incorrectly Implements timeout for tacacs-server timeout
CSCts00341	IPServices	CLI requiring DNS lookup cannot be configured when in SSO mode
CSCtg48785	LegacyProtocols	sh x25 hunt-group causes %DATACORRUPTION-1-DATAINCONSISTENCY: copy error
CSCtr88242	Multicast	PIM-SM doesn't trigger Join message when RPF is changed
CSCsg83966	Routing	Import MAP:sh ip bgp vpnv4 vrf does not show all entities
CSCtn78663	Routing	Cat6k No ICMP Mask Reply
CSCtq62273	Routing	Configuring IPV6 crashes the router.
CSCts16133	Routing	Sup720 may crash after rebuilding object-group configuration
CSCts43881	Routing	Unexpected RIP route leak/redistribution
CSCsr96084	Security	%SYS-6-STACKLOW: Stack for process NHRP running low, 0/6000

Caveats Resolved in Release 12.2(33)SXI7

Resolved Cisco IOS Caveats

- CSCtj22354—Resolved in 12.2(33)SXI7

  Symptom: System may crash when receiving LLDPDUs.

  Conditions: Incoming LLDPDUs with more than 10 LLDP MA(Management Address) TLVs

  Workaround: Disable LLDP MA TLV sending on the peers.

  Further Problem Description: Currently LLDP supports 10 MA TLVs per LLDP neighbor entry, however, it is not processed properly when more than 10 MA TLVs are received.

- CSCtn76183—Resolved in 12.2(33)SXI7

  The Cisco IOS Software Network Address Translation (NAT) feature contains two denial of service (DoS) vulnerabilities in the translation of IP packets.

  The vulnerabilities are caused when packets in transit on the vulnerable device require translation.

  Cisco has released free software updates that address these vulnerabilities. This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-nat

  Note: The September 26, 2012, Cisco IOS Software Security Advisory bundled publication includes 9 Cisco Security Advisories. Eight of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses a vulnerability in Cisco Unified Communications Manager. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the September 2012 bundled publication.

  Individual publication links are in the "Cisco Event Response: Semi-Annual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep12.html

- CSCtq36327—Resolved in 12.2(33)SXI7

  Symptom: A loop between a dot1x enabled port and another a)dot1x enabled port configured with open authentication or b) non-dot1x port, will create a spanning-tree bpdu storm in the network.

  Workaround: Avoid creating a loop.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.1/5.8: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:A/AC:L/Au:N/C:N/I:N/A:C/E:F/RL:U/RC:C CVE ID CVE-2011-2057 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

- CSCtq36336—Resolved in 12.2(33)SXI7

  Symptom: An external loop between 2 dot1x enabled ports can cause a storm of unicast EAPoL pdus in the network.

  Workaround: Avoid creating a loop.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.1/5.8: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:A/AC:L/Au:N/C:N/I:N/A:C/E:F/RL:U/RC:C CVE ID CVE-2011-2058 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

Other Resolved Caveats in Release 12.2(33)SXI7

Identifier	Technology	Description
CSCsd46369	AAA	IP source address on packets to TACACS server is wrong
CSCsi83685	AAA	AAA fallback to radius causes GET_PASSWORD debug message
CSCsl45701	AAA	TACACS+ per VRF authen failing: Address already in use

Identifier	Technology	Description
CSCtl54415	AAA	win11(FIT) - dut crashed after trying to ssh to the dut with no key
CSCtl77241	AAA	MF: webauth login triggers switch crash
CSCsk94501	—	AUTHPROXY: info timestamp array size not the same as max-login-attempts
CSCsm36855	—	%MCT1E1-3-TIMEOUT: TB@ cte1_wait_for_linkrec_ready while unconfig chn gr
CSCsr95189	—	VSS standby switch reset parser error in IDSM config command
CSCsu06967	—	auth-proxy-banner must not be displayed on result page
CSCsu65095	—	switch crash w traceback after applying "eou rev all"
CSCtb05389	—	Alignment errors seen when IKE phase1 failed due to malformed ike packet
CSCtc99947	—	Switch drops DHCP INFORM packets from DHCP client
CSCtd58259	—	sw voice vlan - port removed from STP if snmpset commands are executed
CSCtg09619	—	Web Auth host gets dropped after DHCP renewal with DHCP snooping enabled
CSCtg17979	—	vs_ltl_set_ucast_source_indices slot 19 num_ports 8 fail msgs on bootup
CSCtg32797	—	c6k long failover issue with multicast MVPN
CSCtg47088	—	Sticky mac-address entry not removed from running-config
CSCth31231	—	dACL for MAB still applied for dot1x users
CSCti28450	—	Show auth session port...and oid returns different results
CSCti30359	—	Client in guest-vlan sending EAPOL start cause security violation on int
CSCtj84500	—	Cat6500 - Locked semaphore after config change for CSM WS-X6066-SLB
CSCtk63049	—	Bulk-sync failure due to PRC mismatch due to mls sampling interface
CSCtl42871	—	Show Transceiver Detail Should Show N/A for all fields Instead of 0.00
CSCtl58831	—	small buffer leak on WS-X6708-10GE
CSCtl71282	—	Traffic of Promiscous port is not sent when sec VLAN mode is changed
CSCtl75972	—	CPUHOG for "Virtual Exec" seen when removing/adding ACL on VSS
CSCtl83800	—	Erspan traffic flows after shut/no shut of src port even if session down
CSCtn12198	—	Watchdog timeout after enabling NetFlow
CSCtn15098	—	MF:IDH:Local session timer does not kick in if AAA timer is disabled.
CSCtn27420	—	MF: device tracking causes duplicate address warning on Windows
CSCtn60147	—	6500 SXI - L2 traffic is policed when CoPP is enabled
CSCtn74068	—	CSCtl71282 Traffic from Promiscous port isn't switched on mode change
CSCto34230	—	RRI: C6K not remove routes when SAs removed by DPD.
CSCto53223	—	VSPA\>WS-IPSEC-3 : Failure in VRF Mode acting as EzVPN Server
CSCto98855	—	Supervisor crashes in VS mode when VSL LC crashes
CSCtq06964	—	Old Phase ID is used when EzVPN client connect with different ID
CSCtq26766	—	SUP720-3B crash due to large number of IGMP reports received
CSCtq26863	—	Authentication session information sticks when port shut down
CSCtq48386	—	Authfail->Guest, show cmd is incorrect
CSCtq64820	—	6500 SP crash at cmfi_frr_process_stats_counters

Identifier	Technology	Description
CSCtq65338	—	CDP Bypass allows cisco ip phone to bypass aaa in all host-modes.MUSTFIX
CSCtq72873	—	MF: Crash @ eap_auth_fail
CSCtr10155	—	Crash following defaulting an interface configuration in a port-channel
CSCee38838	Infrastructure	kadis timer abort reloads router
CSCta78502	Infrastructure	Banner: %r raw data support instead of %s output
CSCtn78758	Infrastructure	Crash on Modular IOS on cat6k
CSCtq46758	Infrastructure	process_reschedule_test should not reschedule with mempool_locks_held
CSCtq68778	Infrastructure	After ISSU complete, the reload reason line in "sh version" is missing
CSCtg16573	—	"%DOT1X_SWITCH-SPSTBY-5-ERR_VLAN_NOT_FOUND" on defaulting MDA port
CSCtl24871	—	GLBP virtual mac not programmed in tunnel internal vlan
CSCtl88070	—	IPv6 VRF configuration causes software punt for global uRPF
CSCtn11825	—	MVRP error disables L3 interface part of 6148A LC when match registerN/A
CSCto56118	—	ACL: Adding a duplicate ACE via an object-group is not rejected
CSCtr13929	—	Primary member link changing with addition of new member to bundle
CSCtk47601	IPServices	SSO failure for cmd ipv6 dhcp test relay forward add 2147483647 cisco123
CSCtl21288	IPServices	NAT: "%Port xx is being used by system" even after the CSCtd16493 fix
CSCtl74114	IPServices	NAT: static PAT breaks dynamic PAT if they both use the same IP address
CSCtn21561	IPServices	NAT crash while trying to translate DNS reply from an egress interface
CSCtl52345	LegacyProtocols	C3825 bounces back packets with non-owned MAC strangely
CSCto68456	Management	odr incorrectly installs default route out of an L2 interface.
CSCsd39315	PPP	distributed multilink bundle should never show no frags rcvd
CSCsv04412	PPP	%MCT1E1-3-TIMEOUT while deleting bundle with CHT1E1 SPA
CSCej87096	Routing	Redistribute OSPF command messed up
CSCek39299	Routing	BGP-NSR:stby keep reset after bulk sync for bgp dampening CLI
CSCsz56498	Routing	IPv6 route config is not taken into ipv6 routing table
CSCtg74011	Routing	BGP -IPv6 and IPv4 Capability
CSCtj88224	Routing	Effect of CSCsu96698's improvement "no bgp aggregate-timer" at SRD4
CSCtn96521	Routing	When the Spoke (dynamic) peer-group is configured before the iBGP (stati
CSCto00796	Routing	BGP stops advertising RT extended community to peers in a peer-group
CSCto31265	Routing	OSPFv3:ABR does not translate Type7 when primary Type7 is deleted
CSCto46716	Routing	TE tunnel is not added into RIB even its found in forwarding-ad and OSPF
CSCtq43285	Routing	Routing churn BGP-EIGRP in VRF-Lite
CSCsi67268	Security	Memory leak in Crypto IKMP process when using certificate authentication
CSCtk10401	WAN	Local log archive shows 'ntp authentication-key 1 md5 pwd' in clear text

Caveats Resolved in Release 12.2(33)SXI6

Resolved AAA Caveats

- CSCth25634—Resolved in 15.0(1)SY

  Symptoms: Password is prompted for twice for authentication.

  Conditions: This issue occurs when login authentication has the line password as fallback and RADIUS as primary. For example:

  ```
  aaa authentication login default group radius line
  ```

  Workaround: Change the login authentication to fall back to the enable password that is configured on the UUT. For example:

  ```
  enable password <keyword>
  aaa authentication login default group radius enable
  ```

  Further Information: The fix for this bug also fixes an unrelated problem that may allow unauthorized users access to EXEC mode if the "line" authentication method is configured with fallback to the "none" authentication method. In other words, if the following is configured:

  ```
  aaa new-model
  aaa authentication login MYMETHOD line none

  line con 0
    login authentication MYMETHOD
    password <some password>
  ```

  then users providing the wrong password at the password prompt will be granted access.

  This issue was originally introduced by Cisco Bug ID CSCee85053, and fixed in some Cisco IOS releases via Cisco Bug IDs CSCsb26389 ("Failover for aaa authentication method LINE is broken") and CSCsv06823 ("Authentication request doesnt failover to any method after enable"). However, the fix for this problem was not integrated into some Cisco IOS releases and this bug (CSCth25634) takes care of that.

  Note that Cisco Bug ID CSCti82605 ("AAA line password failed and access to switch still passed") is a recent bug that was filed once it was determined that the fix for CSCee85053 was still missing from some Cisco IOS releases. CSCti82605 was then made a duplicate of this bug (CSCth25634) since the fix for this bug also fixes CSCti82605.

Resolved Infrastructure Caveats

- CSCte01606—Resolved in 12.2(33)SXI6

  Symptoms: When Bidirectional Forward Detection (BFD) is enabled, issuing certain CLI commands that are not premption safe may cause the device to restart. This condition has been seen when issuing commands such as "show mem" or"show mem frag detail".

  Conditions: The issue may occur if BFD is enabled on a device that utilizes Pseudo Preemption to implement this feature. The device must be running an affected software build.

  Workaround: Disable BFD

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4.4/3.8:

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

  CVE ID CVE-2010-3049 has been assigned to document this issue.

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

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

- CSCti25339—Resolved in 12.2(33)SXI6

  Symptoms: Cisco IOS device may experience a device reload.

  Conditions: This issue occurs when the Cisco IOS device is configured for SNMP and receives certain SNMP packets from an authenticated user. Successful exploitation causes the affected device to reload. This vulnerability could be exploited repeatedly to cause an extended DoS condition.

  Workaround: There is no workaround.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.8/5.6:

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

  CVE ID CVE-2010-3050 has been assigned to document this issue.

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

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

Resolved LegacyProtocols Caveats

- CSCth69364—Resolved in 12.2(33)SXI6

  Cisco IOS Software contains a memory leak vulnerability in the Data-Link Switching (DLSw) feature that could result in a device reload when processing crafted IP Protocol 91 packets.

  Cisco has released free software updates that address this vulnerability.

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-dlsw.

Other Resolved Caveats in Release 12.2(33)SXI6

Identifier	Technology	Description
CSCsb46724	AAA	AAA server group doesnt failover with mismatched keys for login
CSCsc49958	AAA	aaa authentication fallback to enable caches previously typed password
CSCti00011	AAA	MF: NAD sending previous state attribute in EAP Identity request
CSCsw52498	—	Extended unsuccessfull dot1x authentication causes red Sup5 to core dump
CSCsz72735	—	VSS STP state change over port channel
CSCta15276	—	auth_mgr_get_authotization_feature_name returns incorrect value
CSCta86571	—	c4hd1: BIT-SW2_SP-4-OUTOFRANGE TB seen during SS0
CSCtd70009	—	IPphone second port notification not clearing session on 2k
CSCte01410	—	lost packests between FWSM and engine when switchover by SSO
CSCte75473	—	SPA-IPSEC-2G is dropping ISIS L2 packets
CSCtf25141	—	Mem leak seen msc_create_met_set, msc_update_met_set & hal_send_met_job
CSCtf78122	—	EAPOL "seen" flag is not set when MAB is pre-empted by 802.1x
CSCtf80540	—	VSS: Memory Leaks with EAP Framework with CTS dot1x/manual links.
CSCtf91665	—	CSCtf56694 creates auth fail retry anomaly
CSCtg09360	—	dot1x security violation with RSPAN configured

Identifier	Technology	Description
CSCtg45139	—	4sup: vs_ha_slc_sync_startup_config:Getting local startup config failed
CSCtg54691	—	Met2 is not programmed when p2p gre tunnel is IIF for service reflect gr
CSCtg94601	—	C4HD1: Continuous TBs @ EthChnl assert failure: on VSS
CSCth23534	—	2960: Crash when host is in auth fail vlan and ACS not reachable
CSCth29986	—	ip2tag fragmentation not working with TE tunnel
CSCth35011	—	memory leak in name_svr.proc on devices running modular IOS
CSCth41644	—	6716 in performance mode has incorrect input/output rate counters
CSCth45241	—	CE1-CE2 ping is not wroking with GRE tunnel
CSCth49187	—	Alloc-Proc *Dead* in VTPMIB EDIT BUFFER using vtpmib_download_config
CSCth61317	—	Message Severity for Noc Payload Crc Error should be 3
CSCth69504	—	7600 - Small buffer leak on SP due to IGMP snooping
CSCth74953	—	SPI Value shown incorrectly as zero for ipsec sa with crypto profiles
CSCth79661	—	MPLS packets missing in TE tunnel accounting
CSCth93066	—	IPV6 mcast traffic is SW forwded over standby uplink with DCEF-only mode
CSCti22519	—	%ILPOWER-7-DETECT doesnt display with 6500Sup720 wid IOS train 12.2SX
CSCti32358	—	linkup is detected earlier than that of the connected device
CSCti33299	—	RP crash due to TLB exception following crypto-map configuration
CSCti37172	—	Ingress SPAN on Sup duplicates packets to ACE module
CSCti47250	—	MVPN: S,G entry not created in mroute table for default-MDT group
CSCti48407	—	Incorrect TTL handling in MPLS traceroute if TTL=1
CSCti54470	—	Cat6K Mcast Packet loss with IGMP snooping and frequent join/leave
CSCti57096	—	6500 OIR causes crash w/ service policty on Distributed Etherchannel
CSCti60740	—	crash after disconnect command
CSCti65529	—	Gold diag will fail TestTrafficStress with the Wism installed .
CSCti68459	—	ISSU aborts at runversion due to BOOT var using sup-bootflash
CSCti72424	—	Memory leak in dot1x auth process
CSCti89368	—	polling xbar using bogus index causes VSAPI-SW1-3-VSAPI_ASSERT &TB
CSCti93310	—	With static IGMP outgoing port not programmed in hardware after reload
CSCtj01590	—	Unexpected Crypto-routes removals and wrong refcount on RRI routes
CSCtj04562	—	PBR with 'set interface null' causes incorrect tcam programming
CSCtj06411	—	crash on single bit parity error with ECC memory
CSCtj06432	—	Crash seen @ msc_destroy_met_set during SSO
CSCtj07133	—	Incorrect switchover to SPT with Multipath configured
CSCtj27523	—	On Standby Sup SP, Memory leak seen related to MET
CSCtj28482	—	Cat6k QoS: priority-queue cos-map cmd inserts also rcv-queue cos-map cmd
CSCtj38057	—	QOS ACEs with 'eq' for dst ports not programmed when LOUs/label exceeded
CSCtj45154	—	DUT crashes upon removing dot1x global cmd (auth_mgr_context.c:2375)

Identifier	Technology	Description
CSCtj58219	—	Standby switch crashes when repl mode is changed to egress in ISSU RV
CSCtj59721	—	%PM_SCP-2-LCP_FW_ERR_INFORM: module 8 is experiencing the following err
CSCtj60445	—	clear crypto sa vrf may be removing sa in the wrong vrf.
CSCtj61261	—	DFC has misprogrammed i2k_slvan for private vlan after reload
CSCtj69212	—	MAB Framework leaking memory
CSCtj72688	—	SNMP: need to disable snmp flowcontrol setting for VSL interfaces
CSCtj76591	—	WS-X6548-GE-TX:Outdiscards is counted on only SPAN dest port
CSCtj84789	—	Additional bridge asic registers need to be removed from TestErrorCounte
CSCtj84908	—	Options data following option82 lost with DHCP-Snooping option82 enabled
CSCtj91384	—	IPC Crash Seen In SXH
CSCtj91928	—	C6K PBR set ip nexthop verify-availability w/ tracking & nexthop tunnel
CSCtj91961	—	nvlog contents are cryptic. power_oper_type 62
CSCtj95068	—	SPAN session gets enabled by snmp set operation
CSCtj96421	—	Leak in SP Buffers. Seen when C6KPWR-SW1_SP-4-PSOUTPUTDROP is logged
CSCtj96837	—	Blank occurred on show run when the system switchover.
CSCtk00723	—	publish w2clix fw library
CSCtk05146	—	IPv6 Solicit dropped by RAguard
CSCtk05747	—	TCAM remerge seen on interface up/down, causing 100% CPU
CSCtk06057	—	Enable ESM for sup32 image in sierra
CSCtk10374	—	Crash @ cts_dot1x_authc_supp_info.
CSCtk10626	—	Cat6k - CLNS frames cropped by flexwan
CSCtk14496	—	WA1: system crash when issue {red reload peer} on VS setup
CSCtk16232	—	MVPN traffic software switched due to mtu failure
CSCtk18890	—	Protected tunnel went down after FRR kicked in
CSCtk31747	—	RRI route deletion is not proper if same peer ip is across differentFVRF
CSCtk31870	—	FPD upgrade hangs with 'Failed to configure the line card' error message
CSCtk31978	—	c2wa1: VSS Act (SW2) reloads after ISSU LV and AV if NAM card is in SW1
CSCtk32622	—	WS-X6748-GE-TX May Reset If All Ports Are Shutdown With Interface Range
CSCtk33826	—	C2WA1: ISSU cycle from sierra->SXI with 256PO not working
CSCtk36622	—	Ingress PE routers do not join data MDT of other with connected source
CSCtk48038	—	c2wa1:SP:macedon_b2b_is_failover: msg seen when shut/noshut crypto vlan
CSCtk54650	—	Modifying IPv6 ACL completely change the ACL configuration
CSCtk60169	—	config sync not happening after setting crcSpanDstPermitListEnabled obj
CSCtk64490	—	c2wa1: XDR ISSU is bypassed on WAN cards while not bypassed on SUP side
CSCtk76633	—	Wrong FPOE programing after replacing the chassis with different type
CSCtl03781	—	ISSU:ONLINE-SW1_SPSTBY-6-INITFAIL: Module 6: Failed to bring up DFC
CSCtl23494	—	Dot1x not functioning properly with 3rd party ip-phones

Identifier	Technology	Description
CSCtl45122	—	CSCsv76509 seen again in SXI4
CSCtl47635	—	KB lifetime incorrect in "show crypto session detail"
CSCtl50744	—	crash on 6k when dot1x accounting feature is turned on
CSCtl54046	—	Standby Sup crashes@dot1x_get_supp_sb with cts dot1x/manual
CSCtl56002	—	Traceback seen @ "SCP Write Process"
CSCtl70909	—	c2wa1: Type6 password encryption is not wrking in Aggressive Mode
CSCtl83517	—	C2WA1: ISSU cycle from sierra->SXI with 256PO not working - red_mode
CSCtl87979	—	Flexwan card crashes on single bit parity error
CSCtn00835	—	Traceroute via mpls cloud does not show egress PE in 3C mode
CSCtn03582	—	TTL Failure rate-limiter not working
CSCtn12243	—	T/b @ icc_send_mcast_request upon bootup
CSCtn14939	—	Crash and Mem Leak under L2 PIM Snooping config after ISSU LoadVer
CSCtn16303	—	The notification was generated incorrectly by ME-C6524GT-8S.
CSCtn27004	—	PS AC/DC input sensor is not detected
CSCtn27447	—	Existing option 82 not overwritten but additionally created
CSCtn43662	—	Slow memory leak at watcher_create_common (TCP, telnet, watched boolean)
CSCtn57039	—	Memory leak in RADIUS and EAP Framework processes with dot1x configs
CSCtn60798	—	SXI6: System Reload on SSO in met_ha_destroy_tmp_set
CSCtn96481	—	wrr-queue cos-map can't be configured
CSCta09049	Infrastructure	memory leak in encrypto proc or Pool Manager
CSCta15808	Infrastructure	Router Crashes on V6 sanity test:tcrashes in trace_caller()
CSCtb81702	Infrastructure	OS provisioned CPU Hog detection logic used by BFD/UDLD is not optimal
CSCtc51539	Infrastructure	Router restart due to Watch Dog Timeout when configured with BFD
CSCtf27594	Infrastructure	ME-C3750 CPU util. spike to 100% related to BFD
CSCtf96250	Infrastructure	IDBMAN-4-CONFIG_WRITE_FAIL and standby sup crash
CSCti60077	Infrastructure	Memory leak in IP SNMP Process on cat6k
CSCtn50281	Infrastructure	SNMPv3 uses wrong mac for snmp engine ID
CSCsv02395	IPServices	Telnet hostname /vrf <name> does not work
CSCtg52885	IPServices	HSRP on subinterfaces stay stuck in INIT after link flap
CSCti05663	IPServices	DHCPACK dropped on relay when Ether-Channel active member link shut down
CSCti28796	IPServices	removing group from class-map type multicast-flows does not change igmp
CSCti71843	IPServices	Ping to NAT outside neighboring interface fails
CSCtl21294	IPServices	NAT: Port numbers are lost from running cfg if route-map option is used
CSCtn27504	IPServices	track CLI removed after the reload
CSCtk95992	LegacyProtocols	DLSw fails to set up circuit using UDP with peer-on-demand
CSCtn12726	Management	'show cdp neighbor detail' causes phone outage in dot1x environment.
CSCtf90182	MPLS	Traffic drop of more than 80sec after multiple SSO with 1PW configured

Identifier	Technology	Description
CSCti53167	MPLS	ION: crash in hw_api_vrf_platform_capability from is_pervrfaggr_enabled
CSCsz82587	QoS	Active crashed on module reset[ES20] with LSM configs
CSCsk56788	Routing	High CPU Proces='BGP Router',when remote neighbor router bgp not active
CSCsw63003	Routing	Continous BGP activity may result in increasing amounts of memory held
CSCsx27496	Routing	Rtr Crash when imported path is selected as mpath & src route del in RIB
CSCta23373	Routing	Eigrp packet size more than ip mtu of gre tunnel
CSCtc25791	Routing	EIGRP crash when issuing relevant "show" cmd while removing EIGRP config
CSCtf33336	Routing	Offset-list access-list set to 0 in rip configuration.
CSCtf51640	Routing	corrupt debug ip packet detail # output
CSCth46888	Routing	VRRP master sends ARP request with non local MAC as Source
CSCth89352	Routing	redistributed static is deleted from rip db when interface down
CSCti30149	Routing	soft-reconfig route not removed from RIB
CSCti32742	Routing	DSGS4: Stand-by is reloading continuously with Virtual-TokenRing1 int
CSCti67102	Routing	Tunnel disables due to recursive routing; holddown timer expires
CSCtj34568	Routing	crash during vrf unconfig - bgp_vpn_impq_add_vrfs_cfg_changes
CSCtj46331	Routing	SNMP walk of atTable leads to high CPU utilization
CSCtj47736	Routing	C4/Mt. Rose:EIGRP/SAF UUT crash shut/no shut on nei interface
CSCtj82292	Routing	summary-address AD 255 should supress components not advertise summary
CSCtj99048	Routing	NSF: type-5 lsa remains even after type-7 becomes unroutable v3 and v2
CSCtk15123	Routing	BGP updates not sent out with update group
CSCtk64094	Routing	when MP-BGP is enabled remote-as statement put on all peers
CSCtl00127	Routing	'ip security ignore-cipso' not shown as working in 'show ip interface'
CSCtl12492	Routing	Config sync failure after SSO
CSCtn78957	Routing	High CPU seen with large IPv6 neighbor table

Caveats Resolved in Release 12.2(33)SXI5

Identifier	Technology	Description
CSCtg58029	AAA	MF:%UTIL-STBY-3-TREE: Data structure error--attempt to remove an unthr
CSCth09686	AAA	"radius-server retry method reorder" removes the server IP upon failover
CSCth52843	AAA	SSO takes 20 to 40 minutes with aaa system accounting
CSCti10891	ATM	6500 crash due to ATM following upgrade to SXI4
CSCek52883	—	without IC new peers are added to dyn map instance
CSCse29460	—	distribute-list route-map match source-protocol not working for ospf
CSCsg49757	—	Combining Gig-Sub-intf & crypto connect & vlan with crypto engine
CSCsg78501	—	IKE should not delete established tunnel upon RSA key regeneration
CSCsj19194	—	SP crashes after %PM-3-INTERNALERROR due to switchport flapping

Identifier	Technology	Description
CSCsq45161	—	High CPU usage on Virtual-Exec due to renewal of DHCP Snooping database
CSCsr39340	—	MPLS packets are not sent across tunnel
CSCsr62489	—	No mask on LC/SP for directly connected prefixes
CSCsu67919	—	SIP crashes - hqf_cwpa_pak_enqueue_local
CSCsw36363	—	SUP32 temperature sensor AUX-1 temperature: N/O
CSCsx96689	—	Bulk sync failed for stp with 802.1x/MDA
CSCsz96236	—	tcp.proc/udp.proc crash at dispatch_manager_pool_context_free
CSCta24271	—	6500 removes switchport access vlan after a dot1x authentication
CSCtc32207	—	Need better accuracy in RP crash reporting
CSCtc69463	—	Interface input rate is doubled the output when BFD is configured
CSCtd84111	—	IOS SLB doesn't add the CASA input features on an interface
CSCtd91871	—	EZVPN - memory leak after ungraceful disconnect of client behind PATl
CSCte64898	—	Vacl capture won't work in Ringar when on different Metro
CSCte99373	—	extranet: mrib S,G entry never removed after pim disabled on IIF
CSCtf21851	—	BFD session flap after interface get up status
CSCtf33948	—	PC behind phone authenticates twice.
CSCtf61757	—	4sup: Power to module in slot 7 set off (Module Failed SCP dnld)
CSCtf93876	—	"sh plat hardware capacity multicast" does not work after switchover
CSCtf98621	—	Recreating a deleted vlan comes up with "act/lshut" state
CSCtg08019	—	Several Malabar-RL under test being reset while perform Sup switch-over
CSCtg26870	—	Bridge Assurance broken on root port
CSCtg34169	—	VSS: cannot boot standby after 2nd switchover
CSCtg37826	—	Inter range command doesn't work
CSCtg41420	—	PIM/BGP takes 60-70 sec to establish on ip-tunnel on serial interface up
CSCtg50990	—	6500 DHCPv6 relay does not forward on layer 3 vlan interfaces.
CSCtg63240	—	cat6500/12.2(33)SXH6 - SNMP-WALK: slow memory leak (SNMP SMALL CHU)
CSCtg68012	—	%SCHED-3-THRASHING: Process thrashing on watched mssg event
CSCtg85476	—	CAT6K NTI ERR and stdby hangs with abortversion while stdby reloading
CSCtg85484	—	No RST packets send to client for an idle out connection with VRF LITE
CSCtg92327	—	MET entries are not deleted properly
CSCtg94220	—	BIT-SP-4-OUTOFRANGE:bit 50463232 is notin d expectd rangeof 1920 t 8191
CSCtg98525	—	ISSU MLS MSC Client(6036) incompatible while issu btn SXI2a->SXI4.FC2
CSCth02812	—	Unicast flood on ingress asymmetric L2 device after TCN event
CSCth04998	—	[VSS] DFC installs drop index for MAC-address
CSCth07233	—	SPA Crypto Connect SSO fails with SVI to Physical int
CSCth10626	—	C2W2C: Memory leak due to OIR of WiSM Module
CSCth12206	—	6500 with 12.2(33)SXI3 May Not Forward Multicast With SLB Configured

Identifier	Technology	Description
CSCth13500	—	SXH: Member entries missing for port-channel in ifStackTable for SUP32
CSCth13572	—	C2W2C: WS-X6716-10GE Failed TestMacNotification and reset after VSS SSO
CSCth15109	—	Flowmask conflict between "Intf full flow" and "full flow least"
CSCth18024	—	xconnect: not show pseudowire status syslog on remote PE
CSCth23794	—	Heathland & RR interfaces errdisable with "vlan inte all poli des" cfg
CSCth26739	—	Data structure traceback and IDC ERRORS seen in Carson IOS
CSCth26806	—	%EC-SP-5-CANNOT_BUNDLE2 is logged against the auto-gen EC for WiSM
CSCth29861	—	VSS: Crash at validate_memory/checkheaps after ISSU from SXI3 to SXI4
CSCth33985	—	LLDP-MED Network Policy TLV DSCP set to 45
CSCth37830	—	12.2(33)SXI3 - xconnect traffic stops when neighboring xconnect removed
CSCth40444	—	Tracebacks on inserting 6708 in 6500 with SXI3
CSCth48803	—	VS2 - Heathland fast-hello link faills after chg port-grp mode
CSCth55383	—	%EARL-DFC2-2-SWITCH_BUS_IDLE message after "show tech"
CSCth60232	—	SXH: Port-channel interface flap when changing vlan mask
CSCth61622	—	Crash seen on carson split Image
CSCth62957	—	IPv6 link local packet loops endlessly when L2VPN/RP SPAN configured
CSCth63715	—	VSS:VPLS TE traffic not forwarded after twice switchover
CSCth66667	—	S,G expiry timer is updated during about 2min more after stop S,G stream
CSCth70481	—	LC frame-relay context missing in advipservices SXI4 Image
CSCth73181	—	Connectivity issue on Cat6k due to index2dvlan table misprogrammed
CSCth73553	—	dot1x phone unregistered during SSO switch-over
CSCth76204	—	TestSPRPInbandPing - No swover/crash after failure threshold reached
CSCth76325	—	OSPFv2 not present in SXI4 base image
CSCth83634	—	RSTP: Shut/No shut on unrelated neighbour causes root flap
CSCth84848	—	IPv6 OID's not getting polled IPServices feature set
CSCth87458	—	SSH: Memory leak in ssh_buffer_get_string
CSCth87937	—	Crash after configuring 'ip multicast boundary'
CSCth92639	—	Extranet MVPN: the triggered pim join functionality is not working
CSCti01426	—	Switch crashes after configuring 'auto qos voip trust'
CSCti02581	—	MF:State attribute from previous EAP exchange included in Access Request
CSCti15684	—	PO member and mem count not synched
CSCti23872	—	traceroute double hop with set vrf due to double ttl decrement
CSCti36805	—	show facility-alarm status shows negative alarm counts
CSCti53769	—	Standby reloads continuously when DA exclude link is Lo2147483647
CSCti55894	—	Service Policy applied twice on multilink interface when bounced
CSCti64429	—	Bus Error Crash at fm_process_nf_dbase_clr_timer
CSCti67447	—	C2wa1-NSF/SSO:- Traffic loss for 8-12 sec with LDP GR enabled

Identifier	Technology	Description
CSCti72095	—	c2wa1: Switch crashed after ISSU runversion from latest sierra to SXI2a
CSCti83486	—	c2wa1:Crash @pm_is_rspan_vlan with 7600-SSC with spa-ipsec-2g while boot
CSCti84025	—	VRFs hardware re-mapping causing MLS/CEF inconsistencies
CSCti84718	—	CPUHOG @ ipnat_ipalias_check_waitlist+E8 after sh/nosh PBR po int
CSCti89747	—	VSS: L2 traffic on healthland gets punted to CPU causing high CPU utilz
CSCti94107	—	c2wa1:BOOTUP_TEST_FAIL: Switch 2 Module 1: TestQos failed
CSCti99869	—	IOMEM memleak: DHCP snooping in relay agent environments - Middle buffer
CSCtj05198	—	With 2 EIGRP AS, PfR fails to control the route
CSCtj15088	—	c2w2:MDEBUG tracebacks @ qm process while applying service policy.
CSCtj22529	—	some mcast shortcut are process switched in ISSU RV.
CSCsi25430	Infrastructure	JQL: VS2: ActiveVS crash@show_one_proc_one_event_list
CSCsr18177	Infrastructure	Traceback after denied "do" command - 12.2SRB
CSCtf45681	Infrastructure	%SCHED-3-SEMLOCKED:SNMP ENGINE after warmstart SNMP ENGINE
CSCtg19572	Infrastructure	Memory leak in two dfs processes
CSCtg64468	Infrastructure	indefinit loops in get_bufferpool_info() & get_buffercachepool_info()
CSCth01674	Infrastructure	*Dead* memory increasing in (coalesced)
CSCti54695	Infrastructure	cannot remove snmp-server engineID from running-config
CSCsa94774	IPServices	NAT default breaks Traceroute response
CSCsv87146	IPServices	NAT: router crashes at ipnat_addrpool_find
CSCsz05783	IPServices	NAT translation fails with certain ALG traffic
CSCtd73578	IPServices	Multicast fragments dropped with NAT enabled
CSCtd80546	IPServices	HSRP Virtual mac-addr not flushed after VSS active failover
CSCte68677	Management	PC behind C7941G does not get IP address when connected to 6500 switch
CSCsy00657	Multicast	Bus error crash after PIM neighbor DR change
CSCtf74238	Multicast	crash with ip multicast ip multicast boundary command
CSCth02725	Multicast	Sending PruneEcho message incorrectly, without changing source IP addr
CSCth38699	Multicast	Auto-RP for multicast triggers RP-Discovery with 0 RPs
CSCsy98768	PPP	Ping unsuccessful through LAC
CSCth36280	QoS	Drop rate for parent hierarchical shaping policy is incorrect
CSCek71050	Routing	CPU Utilization at 100% in BGP Router process in 12.2(33)SRB1
CSCsg18933	Routing	ATM DSL: RIP default route in Routing Table eventhough not in database
CSCsx22124	Routing	CnH: static ip route does not take effect until reconfigured again
CSCtb98722	Routing	Memory leak on eigrp_timer_init
CSCtd81664	Routing	Not possible to "set ip next-hop" in vrf with import-map
CSCtf25357	Routing	Increased CPU usage in IP-EIGRP: PDM when reflexive ACL configured
CSCtf28793	Routing	bgp aggregate-address suppress-map does not suppress specific prefixes
CSCtf64231	Routing	Inbound route-map change shouldn't be effective immediately

Identifier	Technology	Description
CSCtg01873	Routing	EIGRP summary inherits manually set AD from more specific summary
CSCtg37404	Routing	RPPREFIXINCONST error comes up continuously due to checksum error
CSCth05272	Routing	ISIS/LB removes one route after TE FRR failover and recovery
CSCth74576	Routing	NSF for EIGRP is not configurable in the IPBASE images for SXI4
CSCti10518	Routing	Potential memory leak in ipigrp2_redist_process
CSCti20690	Routing	Request for show running config without displaying ACL configs
CSCtj00039	Routing	EIGRP:some prefixes are not being passed from PE to CE router
CSCtj32574	Routing	Deleting redistribute command into eigrp doesn't get synced to stdby
CSCed66047	Security	CRYPTO sems inadequately documented
CSCsb40163	Security	TCP SYN packet from an async interface may fail encapsulation with CBAC
CSCsz05583	Security	crypto pki config nvgened before ip config on which it depends - slow
CSCtg11808	Security	VSS: Standby supervisor reloads when crypto pki trustpoint removed
CSCtg84011	Security	mac-address on SVI does not work for EIGRP hello packets
CSCti26768	Security	Bus error while re-configuring a trustpoint
CSCtf03928	WAN	NTP packets received but ignored by the NTP process

Caveats Resolved in Release 12.2(33)SXI4a

Identifier	Technology	Description
CSCta24271	—	6500 removes switchport access vlan after a dot1x authentication
CSCth43783	—	No hardware entries for EoMPLS pseudowire

Caveats Resolved in Release 12.2(33)SXI4

Resolved AAA Caveats

- CSCsg21398—Resolved in 12.2(33)SXI4

  Symptoms: The Cisco IOS software image may unexpectedly restart when a crafted “msg-auth-response-get-user” TACACS+ packet is received.

  Conditions: This symptom is observed after the Cisco platform had send an initial “recv-auth-start” TACACS+ packet.

  Workaround: There is no workaround.

Resolved Infrastructure Caveats

- CSCtd72456—Resolved in 12.2(33)SXI4

  Symptoms: Entering the **show snmp pending** command may cause a Cisco switch to crash.

  Conditions: This symptom is observed on a Cisco 3750 switch running Cisco IOS Release 12.2(50)SE3 configured to send v3 informs, but may affect other platforms.

  Workaround: Do not enter the **show snmp pending** command if you have configured informs in the “snmp-server host” statement.

Resolved Multicast Caveats

- CSCtc68037—Resolved in 12.2(33)SXI4

  Symptom: A Cisco IOS device may experience an unexpected reload as a result of mtrace packet processing.

  Conditions:

  Workaround: None other than avoiding the use of mtrace functionality.

Resolved Security Caveats

- CSCsg65318—Resolved in 12.2(33)SXI4

  Symptoms: Malformed SSH version 2 packets may cause a memory leak.

  Conditions: This symptom is observed on a Cisco platform configured for SSH version 2 after it has received malformed SSHv2 packets. The impact of this flaw is that the affected platform may operate in a degraded condition. Under rare circumstances it may reload to recover itself.

  Workarounds: Options consist of using SSH version 1 in the interim until the affected platform can be upgraded to a fixed release or permitting only known trusted hosts/networks that can connect to the router by using a VTY access list.

  Following are examples of the workarounds:

  Configure SSH version 1

```
Configure SSH version 1
+----------------------
 !-- configure from global config mode
 !
 config t
 !
 ip ssh version 1
 end

VTY access-list
+--------------
 !-- 10.1.1.0/24 is a trusted network that
 !-- is permitted access to the router, all
 !-- other access is denied
 !
 access-list 99 permit 10.1.1.0 0.0.0.255
 access-list 99 deny any
 !
 line vty 0 4
  access-class 99 in
 end
```

  More information about configuring VTY access lists is available in Cisco IOS Security Configuration Guide: Securing the Data Plane, Release 12.4T Controlling Access to a Virtual Terminal Line:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_data_acl/configuration/12-4t/sec-cntrl-acc-vtl.html

  More information about SSH on IOS is available in the Configuring Secure Shell on Routers and Switches Running Cisco IOS guide:

  http://www.cisco.com/en/US/tech/tk583/tk617/technologies_tech_note09186a00800949e2.shtml

Resolved Unknown Caveats

- CSCsy16092—Resolved in 12.2(33)SXI4

  Symptoms: A router running Cisco IOS or Cisco IOS XE may unexpectedly reload due to watchdog timeout when there is a negotiation problem between crypto peers. The following error will appear repeatedly in the log leading up to the crash:

  .Mar 1 02:59:58.119: ISAKMP: encryption... What? 0?

  Conditions: When a malformed payload (Transform payload with vpi length =0) is received and "debug crypto isakmp" is enabled, the error messages are repeatedly seen leading upto the crash.

  Workaround: Remove this debug command.

- CSCtc49782—Resolved in 12.2(33)SXI4

  Symptoms: Upgrade from 12.2(18)SXF6 to 12.2(33)SXH5 introduced additional vty lines to the running-configuration (vtp line 5 - 15). These new lines do not inherit the security ACL or transports configured by the customer on the old lines (0-4). Switch upgrade caused device to be non-compliant with network security policy defined by customer.

  Condition: Software upgrade from 12.2(18)SXF6 to 12.2(33)SXH5.

  Workaround: We have to manually configure the ACL for those newly introduced vty lines.

- CSCtc71597—Resolved in 12.2(33)SXI4

  Symptom: Currently in EARL7 system, For an IPv6 packet the 96 bytes cover DBUS header (22), Ether header (14), IPv6 harder (40), IPv6 extension headers, and L4 header. That means only 20 bytes (96 - 22 - 14 - 40) are for extension header(s) and L4 header. So even packet with small extension header(s) can use up to 20 bytes that would cause l4_hdr_vld = 0. When that happens, all L4 features cannot be applied and packet would be hardware forwarded based on L3 forwarding result.

  Conditions: This issue is present from day one but would cause threat only when ipv6 access-list is configured on any interface and that access-list is containing L4 options.

  Workaround: No Workaround

- CSCte83104—Resolved in 12.2(33)SXI4

  Conditions: When an ipv6 RACL is confiured on an interface. All packets containing ipv6 optional headers are punted to RP. But if any packets that are sent with no L4 header are also hitting this punt entry present at the top of tcam.

  Workaround: No Workaround:

Resolved WAN Caveats

- CSCtd75033—Resolved in 12.2(33)SXI4

  Symptom: Cisco IOS Software is affected by NTP mode 7 denial-of-service vulnerability. Note: The fix for this vulnerability has a behavior change affect on Cisco IOS Operations for Mode 7 packets. See the section **Further Description** of this release note enclosure.

  Conditions: Cisco IOS Software with support for Network Time Protocol (NTP) contains a vulnerability processing specific NTP Control Mode 7 packets. This results in increased CPU on the device and increased traffic on the network segments.

  This is the same as the vulnerability which is described in http://www.kb.cert.org/vuls/id/568372

  Cisco has release a public facing vulnerability alert at the following link:

  http://tools.cisco.com/security/center/viewAlert.x?alertId=19540

Cisco IOS Software that has support for NTPv4 is NOT affected. NTPv4 was introduced into Cisco IOS Software: 12.4(15)XZ, 12.4(20)MR, 12.4(20)T, 12.4(20)YA, 12.4(22)GC1, 12.4(22)MD, 12.4(22)YB, 12.4(22)YD, 12.4(22)YE and 15.0(1)M.

All other versions of Cisco IOS and Cisco IOS XE Software are affected.

To see if a device is configured with NTP, log into the device and issue the CLI command **show running-config | include ntp**. If the output returns either of the following commands listed then the device is vulnerable:

```
ntp master <any following commands>
ntp peer <any following commands>
ntp server <any following commands>
ntp broadcast client
ntp multicast client
```

The following example identifies a Cisco device that is configured with NTP:

```
router# show running-config | include ntp
ntp peer 192.168.0.12
router#
```

The following example identifies a Cisco device that is not configured with NTP:

```
router# show running-config | include ntp
router#
```

To determine the Cisco IOS Software release that is running on a Cisco product, administrators can log in to the device and issue the **show version** command to display the system banner. The system banner confirms that the device is running Cisco IOS Software by displaying text similar to "Cisco Internetwork Operating System Software" or "Cisco IOS Software." The image name displays in parentheses, followed by "Version" and the Cisco IOS Software release name. Other Cisco devices do not have the show version command or may provide different output.

The following example identifies a Cisco product that is running Cisco IOS Software Release 12.3(26) with an installed image name of C2500-IS-L:

```
Router# show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-IS-L), Version 12.3(26), RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright ) 1986-2008 by cisco Systems, Inc.
Compiled Mon 17-Mar-08 14:39 by dchih

<output truncated>
```

The following example shows a product that is running Cisco IOS Software release 12.4(20)T with an image name of C1841-ADVENTERPRISEK9-M:

```
Router# show version
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 12.4(20)T,
RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright ) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 20:25 by prod_rel_team

<output truncated>
```

Additional information about Cisco IOS Software release naming conventions is available in "White Paper: Cisco IOS Reference Guide" at the following link:

http://www.cisco.com/web/about/security/intelligence/ios-ref.html

Workaround: There are no workarounds other than disabling NTP on the device. The following mitigations have been identified for this vulnerability; only packets destined for any configured IP address on the device can exploit this vulnerability. Transit traffic will not exploit this vulnerability.

Note: NTP peer authentication is not a workaround and is still a vulnerable configuration.

– NTP Access Group

Warning: Because the feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender's IP address, which may defeat access control lists (ACLs) that permit communication to these ports from trusted IP addresses. Unicast Reverse Path Forwarding (Unicast RPF) should be considered to be used in conjunction to offer a better mitigation solution.

```
!--- Configure trusted peers for allowed access
access-list 1 permit 171.70.173.55
!--- Apply ACE to the NTP configuration
ntp access-group peer 1
```

For additional information on NTP access control groups, consult the document titled "Performing Basic System Management" at the following link:

http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_basic_sys_manage.html#wp1034942

– Infrastructure Access Control Lists

Warning: Because the feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender's IP address, which may defeat ACLs that permit communication to these ports from trusted IP addresses. Unicast RPF should be considered to be used in conjunction to offer a better mitigation solution.

Although it is often difficult to block traffic that transits a network, it is possible to identify traffic that should never be allowed to target infrastructure devices and block that traffic at the border of networks.

Infrastructure ACLs (iACLs) are a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for this specific vulnerability. The iACL example below should be included as part of the deployed infrastructure access-list, which will help protect all devices with IP addresses in the infrastructure IP address range:

```
!---
!--- Feature: Network Time Protocol (NTP)
!---

access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
   INFRASTRUCTURE_ADDRESSES WILDCARD eq 123

!--- Note: If the router is acting as a NTP broadcast client
!---   via the interface command "ntp broadcast client"
!---   then broadcast and directed broadcasts must be
!---   filtered as well.  The following example covers
!---   an infrastructure address space of 192.168.0.X

access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
   host 192.168.0.255 eq ntp
access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
   host 255.255.255.255 eq ntp

!--- Note: If the router is acting as a NTP multicast client
!---   via the interface command "ntp multicast client"
!---   then multicast IP packets to the mutlicast group must
```

```
!---   be filtered as well.  The following example covers
!---   a NTP multicast group of 239.0.0.1 (Default is
!---   224.0.1.1)

access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
   host 239.0.0.1 eq ntp

!--- Deny NTP traffic from all other sources destined
!--- to infrastructure addresses.

access-list 150 deny udp any
INFRASTRUCTURE_ADDRESSES WILDCARD eq 123

!--- Permit/deny all other Layer 3 and Layer 4 traffic in
!--- accordance with existing security policies and
!--- configurations.  Permit all other traffic to transit the
!--- device.

access-list 150 permit ip any any

!--- Apply access-list to all interfaces (only one example
!--- shown)

interface fastEthernet 2/0
   ip access-group 150 in
```

The white paper entitled “Protecting Your Core: Infrastructure Protection Access Control Lists” presents guidelines and recommended deployment techniques for infrastructure protection access lists and is available at the following link

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

- Control Plane Policing

  Provided under Control Plane Policing there are two examples. The first aims at preventing the injection of malicious traffic from untrusted sources, whilst the second looks at rate limiting NTP traffic to the box.

  —Filtering untrusted sources to the device.

  Warning: Because the feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender’s IP address, which may defeat ACLs that permit communication to these ports from trusted IP addresses. Unicast RPF should be considered to be used in conjunction to offer a better mitigation solution.

  Control Plane Policing (CoPP) can be used to block untrusted UDP traffic to the device. Cisco IOS software releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP can be configured on a device to help protect the management and control planes and minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic that is sent to infrastructure devices in accordance with existing security policies and configurations. The CoPP example below should be included as part of the deployed CoPP, which will help protect all devices with IP addresses in the infrastructure IP address range.

```
!--- Feature: Network Time Protocol (NTP)

access-list 150 deny udp TRUSTED_SOURCE_ADDRESSES WILDCARD
   any eq 123

!--- Deny NTP traffic from all other sources destined
!--- to the device control plane.

access-list 150 permit udp any any eq 123
```

```
!--- Permit (Police or Drop)/Deny (Allow) all other Layer3 and
!--- Layer4 traffic in accordance with existing security policies
!--- and configurations for traffic that is authorized to be sent
!--- to infrastructure devices
!--- Create a Class-Map for traffic to be policed by
!--- the CoPP feature

class-map match-all drop-udp-class
   match access-group 150

!--- Create a Policy-Map that will be applied to the
!--- Control-Plane of the device.

policy-map drop-udp-traffic
   class drop-udp-class
      drop

!--- Apply the Policy-Map to the
!--- Control-Plane of the device

control-plane
   service-policy input drop-udp-traffic
```

In the above CoPP example, the access control list entries (ACEs) that match the potential exploit packets with the “permit” action result in these packets being discarded by the policy-map “drop” function, while packets that match the “deny” action (not shown) are not affected by the policy-map drop function.

—Rate Limiting the traffic to the device The CoPP example below could be included as part of the deployed CoPP, which will help protect targeted devices from processing large amounts of NTP traffic.

Warning: If the rate-limits are exceeded valid NTP traffic may also be dropped.

```
!--- Feature: Network Time Protocol (NTP)

access-list 150 permit udp any any eq 123

!--- Create a Class-Map for traffic to be policed by
!--- the CoPP feature

class-map match-all rate-udp-class
   match access-group 150

!--- Create a Policy-Map that will be applied to the
!--- Control-Plane of the device.
!--- NOTE: See section "4. Tuning the CoPP Policy" of
!--- http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html#5
!--- for more information on choosing the most
!--- appropriate traffic rates

policy-map rate-udp-traffic
   class rate-udp-class
      police 10000 1500 1500 conform-action transmit
         exceed-action drop violate-action drop

!--- Apply the Policy-Map to the
!--- Control-Plane of the device

control-plane
   service-policy input drop-udp-traffic
```

Additional information on the configuration and use of the CoPP feature can be found in the documents, “Control Plane Policing Implementation Best Practices” and “Cisco IOS Software Releases 12.2 S - Control Plane Policing” at the following links:

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

Further Description: Cisco IOS Software releases that have the fix for this Cisco bug ID, have a behavior change for mode 7 private mode packets.

Cisco IOS Software release with the fix for this Cisco bug ID, will not process NTP mode 7 packets, and will display a message “NTP: Receive: dropping message: Received NTP private mode packet. 7” if debugs for NTP are enabled.

To have Cisco IOS Software process mode 7 packets, the CLI command **ntp allow mode private** should be configured. This is disabled by default.

Other Resolved Caveats in Release 12.2(33)SXI4

Identifier	Technology	Description
CSCin67182	AAA	Crash in aaa_sg_v2_get_next_server on trying unconfigured radius ser
CSCsb17623	AAA	ALIGN-3-SPURIOUS: Spurious memory access made at error on 3725 (TACACS+)
CSCsd82068	AAA	single-connection to private TACACS+ doesn't recover
CSCsf17907	AAA	LI: not needed attributes in COA are accepted.
CSCsi54201	AAA	IDMGR-3-INVALID_ID error message
CSCsq71492	AAA	IOS device crash or tracebacks at tplus_handle_req_timeout
CSCsv13914	AAA	%ALIGN-3-TRACE: at pppoa_aaa_acct_get_nas_port_details
CSCsw79561	AAA	DROPACCTFAIL: System Accounting fails with tacacs
CSCsx07352	AAA	Console stuck with "authentication failed" on save & reload for sys acco
CSCsx15897	AAA	Cisco 3800 shows symptoms of memory leak in AAA component
CSCsx95806	AAA	Incorrect timeout delay for non-exist radius server
CSCsx97093	AAA	AAA Fails to parse RADIUS callback string ending in =
CSCsy20392	AAA	change default behaviour of accoutning gurantee-first command
CSCsy55362	AAA	Unresponsive Console/VTYs
CSCsy61321	AAA	tac+ acct is not failing over to next server group
CSCsz09373	AAA	POD Reply sent with physical intf ip when req rcvd with loopback intf ip
CSCta11120	AAA	Tacacs single-connect not able to make connection to prev down server
CSCta16724	AAA	IOS release 12.4(24)T breaks partner SCP functionality
CSCtb95275	AAA	Autocommands "access-profile" on vty not executed
CSCtc72862	AAA	C2W2C: Standby router crashes at pagp_switch_mp_create_idb after SSO
CSCtc86306	AAA	Authorization requests not using VRF interface
CSCtc94806	AAA	tacacs-server dns-alias-lookup causes high CPU on TPLUS process
CSCtd16343	AAA	Radius server declared as dead for MAB if server-private in server group
CSCte12007	AAA	System accounting retries are not consistent as expected
CSCte69879	AAA	ip radius source-interface for Acct-on/off not work under aaa group
CSCtf23298	AAA	tacacs-server host " " single-connection causes high CPU utilization

Identifier	Technology	Description
CSCtg40901	AAA	TACACS single connection crashes @tplus_increase_sock_write_event_count
CSCse75697	ATM	LOKI: ima clock should default to LINE, backout CSCin90422, CSCsb68536 .
CSCej00344	—	Crash when opening new session from router
CSCek61184	—	Memory leak in create_cce_target_class_group
CSCsb60761	—	Spurious memory access with debug crypto ipsec enabled
CSCsb95192	—	RRI with HA doesnt populate the routes correctly - static keyword
CSCsd27617	—	Password encryption aes corruptskeys for Group names containing _
CSCsg47058	—	show crypto ipsec client command is not supported
CSCsh20336	—	DMVPN - crypto socket unexpectedly closed for nhrp static entry
CSCsj57384	—	HWIF-QOS-ERR and other types of QoS error messages are seen
CSCsk18794	—	speed and negotiation configuration issue on FE-TX-V2 SPA
CSCsk25046	—	Not all ifIndex'es are in cbQosServicePolicyTable
CSCsk49041	—	crypto_ikmp_utils.c: possible Invalid Pointer Read
CSCsk66851	—	*,G/m entry does not have OIF programmed in HW sometimes
CSCsk86410	—	Abnormal ISAKMP traffic caused an alignment error and traceback.
CSCsk88751	—	Kron CLI Process 'show tech-support password
CSCsl94488	—	Smartports CLI missing in sup32 ipbase image
CSCsm63524	—	SUP32 crashes due to SP hang when it recovers from errdisable
CSCsm89642	—	Bus error crash when executing 'show crypto sessions'
CSCso19511	—	ESM20: No route drops are getting accounted wrongly.
CSCso35876	—	SRB3:New active SP crash at label_entry_get_inlabel
CSCso36150	—	duplicate vlan names causing config-sync failures
CSCso79925	—	EC with enhanced hash method (PFC3C) has no knob to use old method (3B)
CSCso99283	—	Crash with kron configured and show ipc ports
CSCsq40205	—	INTERFACE_API-3-NODESTROYSUBBLOCK:The SWIDB subblock named FM was not re
CSCsq63621	—	SPD classifies OSPF IP Precedence 0 as priority
CSCsr13388	—	To make default debounce timer present at LC to be as configurable
CSCsr50134	—	Router or Linecard may reload at cv6_6pe_frr_stats
CSCsr54959	—	Switch crashes when route-map/policy is unconfigured
CSCsr74002	—	7600 - VPLS - QinQ- UDLD packet received on qinq flooded to vpls
CSCsr99518	—	Granikos should not init rekey after recieving new outbound SA at QM3
CSCsu31088	—	Not able to execute any commands under intf after running SPA FPGA bert
CSCsu39458	—	SIP400: LLQ Cndl Policer Always Kicked in for Large Pkts
CSCsu51095	—	OER stop forwarding internet traffic
CSCsu81976	—	IPSEC NAT traversal fails to correctly track SAs
CSCsv13243	—	BFD config causing BGP session to go down
CSCsv36976	—	IKE - Need recovery mechanism when IKE pkts are re-enqueued indefinitely

Identifier	Technology	Description
CSCsv61041	—	VSS: static mac-address-table entries missing in standby running-config
CSCsv82285	—	Cat6k: UDP port 10000 is opened by default
CSCsw28024	—	Router is getting crashed at crypto_ikmp_cfg_auto_update_parameters
CSCsw46893	—	C2HD1-SI - %CHKPT-4-GET_HUGE_BUF: Client (Event Manager) message seen
CSCsx24934	—	CPU Monitor not heard and ipc TBs on Active VSS switch on issuing Reload
CSCsx56011	—	Switch may crash when issuing "show mac-address-table"
CSCsx65088	—	WiSM on 5.2.157.0 causes %WiSM-5-STATE: Oper-up messages on supervisor
CSCsx74064	—	On modular IOS, SSH on VRF int is allowed irrespective of vrf-also key
CSCsx76168	—	ISSU : hqf ipc Tracebacks on ISSU runversion.
CSCsx79111	—	7600 MPLS mls cef entry for label imposition has programmed mtu 0
CSCsx81468	—	CWPA2: Drops CLNS Hello packets
CSCsx87562	—	%SYS-3-TIMERNEG error following configuration change
CSCsy04594	—	Vlan interfaces flap when a root guard port receive superior bpdu
CSCsy07709	—	C2W2: %COMMON_FIB-4-FIBNULLIDB: Missing idb for fibidb Port-channel5A
CSCsy27389	—	EW does not update time accordingly when Daylight Savings time changes
CSCsy30937	—	Modify dual-active fast-hello function for rapid detection and recovery.
CSCsy41470	—	cewEntTable not releasing memory
CSCsy49927	—	IOSd restart seen with RP2@PrepareProcFrameForExecution
CSCsy54365	—	frequent datapath recovery and traffic loss on WS-X6704 with DFC
CSCsy58886	—	NGN:Active crashes when standby booting up on SRC2->SRC3 ISSU
CSCsy66678	—	stp_helper_manipulate_queue: standby SP CPUHOG
CSCsy69914	—	Some lines are omitted when Copy and paste of TCL script in TCL shell
CSCsy89677	—	"% Ambiguous command" returned in the TCLSH for all commands
CSCsz01976	—	Need a cli to dump the rommon environment and unset rommon variable
CSCsz04557	—	When the "set probe frequency" is less than 15 we receive an IP SLA erro
CSCsz14273	—	EEM: CPUHOG and watchdog crash when TCl policy prints large output
CSCsz14369	—	MAB not attempted when RADIUS is available again.
CSCsz15989	—	Event manager applet does not trigger for "clock set" CLI
CSCsz23099	—	Memory leak due to CEF: loadinfos in Collection proc
CSCsz23445	—	%PORT_SECURITY-SP-6-INVALID_SESSION: Invalid Port-Security ISSU Session
CSCsz35605	—	LBL sync failure during removal/addition of cts dot1x from a trunk port
CSCsz42143	—	WS-X6148A-GE-TX module fails keepalives when excessive errors on port.
CSCsz42241	—	RRI route deletion broken for non-crypto-map RRI
CSCsz47489	—	Full solution towards the problem faced with service card internal PO as
CSCsz52926	—	Input counters stop after unidirectional receive config change on 6704
CSCsz53124	—	IPSEC VPN interoperability issue when IPCOMP compression enabled
CSCsz54543	—	%BFDFSM-3-INVTRANS: seen when bfd is unconfigured

Identifier	Technology	Description
CSCsz74212	—	incorrenct PS status display after switchover
CSCsz76015	—	C2W2: Need cli to set PF_BIAS to ensure lower slot# Sup boots as active
CSCsz90894	—	Spanning Tree block L2 promiscuous port Leak broadcast traffi
CSCta06428	—	VSS: Active Crash at iccp_test_get_first_mcast_resp_data
CSCta06451	—	PfR:BR Memory leak in export path on 7600
CSCta10075	—	"clear counters" triggers EEM policy to be run
CSCta10402	—	Tracebacks seen due to BFD PP Process
CSCta12382	—	Udld port config does not sync to standby in rpr-plus mode
CSCta13870	—	Traffic duplicated on Primary and Backup tunnel after FRR
CSCta21771	—	%CONST_DIAG-SP-3-HM_FCI_0_STUCK: Flow control stuck at 0 error on modul
CSCta28455	—	IntMacTx-Err (PI_PN_S_CRC_ERR_CNT) increasing on X6408A-GBIC
CSCta29818	—	Enhanced-Flexwan Module Power Down after Code Upgrade from SXF to SXH
CSCta34143	—	2nd prefix-list in route-map stanza may not being used
CSCta36939	—	c2w2b:Crash On ISSU Run Version
CSCta37465	—	MAB runs indefinitely, despite received traffic
CSCta42669	—	C2W1: segv exception after portchannel configuration
CSCta47293	—	Enhancement on CDP TLV IP Phone 2nd port status processing
CSCta48521	—	%DATACORRUPTION-1-DATAINCONSISTENCY: copy error
CSCta48968	—	Modular IOS kernel crashinfo has missing information
CSCta52689	—	cat6k crash in RP due to address error with wccp configuration
CSCta53157	—	SPA-4XT3/E3 int in SIP-200 admin-down on standby after fpd upgrade
CSCta53466	—	ISSU on Sup4 causes IPV6 mcast traffic loss to Rcv in Standby uplink
CSCta55574	—	Once in a while catalyst fails to apply to proxyACL with auto mac-check
CSCta56305	—	Detector data port operation status not OK after boot
CSCta56890	—	WiSM LAG and Data Ports flaps on SSO Switchover
CSCta57778	—	auth-mgr/eap:: %IDMGR-3-INVALID_ID: bad id in id_get (bad table id)
CSCta61568	—	Forwarding loop after adding vlan to MST instance
CSCta67007	—	c2hd1:VRF interfaces not shown and not pinging the CE's
CSCta68053	—	time-period does not take effect in configuration archive
CSCta71873	—	Mcast traffic stops flowing across fabric to required fpoes
CSCta72199	—	"aggregate-address advertise-map" not updated dynamically with ION image
CSCta74242	—	VSS: crash due to snmp get after standby chassis reloads
CSCta74315	—	WS-X6324-100FX-MM May Be Inoperable and Have Status "Other"
CSCta75226	—	Mago:ds_isr_cbif ds_num:0 msg on bootup with ip-base image
CSCta75882	—	VSS crashes at platform_reset_by_peer(0x422787e4)+0x6c during sso
CSCta76808	—	add CLI command for medium buffer pool
CSCta80024	—	string repeat crashes router

Identifier	Technology	Description
CSCta83331	—	APS active and ptrotect circuit show same input counters
CSCta84749	—	Etherchannel should not be allowed if auto qos is enable
CSCta94179	—	Recirculated MPLS packets becasue of egress service policy are dropped
CSCta95295	—	IOMEM depleted when PKI servers unavailable for CRL checking
CSCta97265	—	ip igmp snooping querier is removed from SVI after PC removed.
CSCta98108	—	With NAT, on Netflow database cleanup timer expiry, CPU spikes on 7600
CSCtb03003	—	MAC table on standby Supervisor not flushed on link change
CSCtb04231	—	Imprecise parity error crash due to mistral timeout
CSCtb08846	—	Address build breakage due to SR commit CSCsz28039
CSCtb09203	—	active probes partially show up when add new oer-map policy
CSCtb15569	—	VPN-SPA - traffic failed to decrypt due to SecInfo check failure
CSCtb16453	—	ERSPAN /w specific VRF may see traffic routing to default route
CSCtb23289	—	Major temperature alarm has to force system shutdown
CSCtb25132	—	SLB: VSERVER HSRP group name is truncated if any modifcation in VS confi
CSCtb27643	—	cat6000 Medium buffers leak on SP leading to crash
CSCtb28032	—	Changing module corrupts Flex Link
CSCtb28712	—	SPAN Reflector not enabled for WS-SVC-ADM-1-K9
CSCtb31400	—	BGP sends Route-Refresh request on entering route-map configuration
CSCtb34857	—	crashed seen in xdr_reference
CSCtb35917	—	CSM: HSRP tracking status is not changed from INIT to Standby
CSCtb38000	—	Port error disabled due to ingress pause frames,WS-X6148A-GE-TX
CSCtb38547	—	Incorrect CP0 values and empty kernel variable section in kernel crashin
CSCtb41832	—	C2W23: Port-Channel may not form using LACP across EoMPLS
CSCtb44299	—	Stby RP carsh @ m_requeue
CSCtb45475	—	sh plat hard capacity cpu report system memory usage incorrectly
CSCtb47692	—	VSS: Switch crashed due to EBUS_SEQ_ERROR
CSCtb50678	—	Crash @ registry_add_case with VSS when change from RPR to SSO
CSCtb51922	—	chunk leak fund during " no host-address ip address key-chain CISCO "
CSCtb52180	—	set vrf nvgened while vrf deletion in progress causes standby to reload
CSCtb55853	—	A route-map permits ALL IPv4 routes when "match ipv6" is applied
CSCtb55858	—	No qos rewrite on untrusted port in SXI2
CSCtb55994	—	EW: Free memory loss when EW is enabled
CSCtb58820	—	RR-B0: Vlan drops observed on Roadrunner at all corners in IOS only
CSCtb60330	—	VTI: Missed DPD ACK on phase 1 expiry causing phase 2 deletion.
CSCtb62031	—	cat6k: High cpu and high inband when reflexive ACL is used with WCCP
CSCtb62523	—	PfR - inside prefixes not learned on cat6k BR
CSCtb63352	—	VSS: With 6KW DC PS, no power to bringup VSL supervisor or linecard

Identifier	Technology	Description
CSCtb65406	—	QoS ACL May Not Program L4 ports Correctly In TCAM
CSCtb66983	—	Nas-port-type is missing in Access-request
CSCtb68478	—	"Illegal nextSsIndex value" message should be removed
CSCtb70344	—	SH7615 MAC: ucast frames marked as mcast and dropped in offline mode
CSCtb70504	—	Traceback at reg_inv_internal_ha_cs_stdby_out_of_sync
CSCtb70578	—	L2PT incorrectly decapsulates STP PDU for RSPAN causing PVID mismatch
CSCtb72638	—	Ezvpn server not sending split tunneling access-list to client
CSCtb78973	—	PM-SP-3-INTERNALERROR: Port Manager Internal Software Error with dot1x
CSCtb83677	—	Power Deny for pre-standard power on SXI2 or Later
CSCtb83776	—	X6148A-GE-TX-Outdiscard incrementing if queue-limit of priority Q is 0
CSCtb84298	—	Shadow state of wism PO line protocol down on stdby After OIR of WiSM
CSCtb87454	—	DHCP Rogue Server Detection
CSCtb88222	—	C2W2C: %IDBINDEX_SYNC-4-RESERVE: on LV & RV
CSCtb95464	—	Unable to configure individual interfaces of WiSM on VSS Switch
CSCtc01912	—	EEM: syslog text trigger won't start script if text is in body of debug
CSCtc05449	—	rstp BPDUs are not tunneled over eompls for dfc facing interface
CSCtc09913	—	VTY Process/Telnet connection stuck
CSCtc11691	—	VSS: Switch crashes after loading the sierra 090920 image
CSCtc11754	—	Diags: TestNetflowTCAM intrusive diags test fails with specific configs
CSCtc11809	—	FWSM internal port-channel goes down after SSO forced switchover
CSCtc15386	—	IOS tags VLAN name configuration command as level 1
CSCtc16740	—	Global BPDUGuard does not work on MVAP ports
CSCtc17058	—	VC stops sending traffic due to duplicate vpn id in port based EoMPLS
CSCtc17083	—	Tunnel decap not programmed, hence traffic RP switched
CSCtc19148	—	CASA: Standby chassis get crashed when Vserver is taken outofservice.
CSCtc22217	—	SPA-8X1FE-TX-V2 negotiation auto and duplex mode issue
CSCtc22760	—	VSS ENH: Immediate reset LC after crash occurrs on stdby chassis LC
CSCtc24864	—	Enable cdp - removed on shut/ no shut dot1q-tunnel interface
CSCtc27745	—	LLDP packets go out tagged if native vlan (not Vlan1) is configured
CSCtc28953	—	Crash on cat6k running MPLS: see resolution note and CSCtc82349
CSCtc30691	—	Crash/Spurious memory access on privilege ipaddr-object-group/port-objec
CSCtc30868	—	Irregular CPU (peaks) on Cat6500 rtr responder
CSCtc30909	—	TestRwEngineOverSubscription always fails for ACE module
CSCtc32375	—	Crash occurs issuing 'show eigrp service-family external-client
CSCtc38716	—	ME6524 may reset due to single power supply failure
CSCtc38771	—	12.2SXH: Intermittent BPDU drop over Dot1Q tunnel.
CSCtc38905	—	Disabling IPv6 MLD Snooping breaks IPv4 IGMP and PIM Snooping

Identifier	Technology	Description
CSCtc39052	—	svclc module command adds firewall module command to configuration
CSCtc40420	—	Basic packet forwarding failed when GRE tunnel is configured
CSCtc40724	—	Multicast packets may get dropped on 6500 when member join mcast group
CSCtc49542	—	VSS: output drops on VS-720 port due to CoS mapping mismatch
CSCtc52807	—	C2HD1-SI: L3 Portchannel's FPOE mask incorrect after SSO
CSCtc53375	—	C2W2B : pagp_switch_sp2mp:idbman_update_mp_delete_agport
CSCtc53453	—	stack members lost energywise config after stack reloading
CSCtc53958	—	"sh run" on Cat6k results in tunnel flapping on non-modular IOS
CSCtc54233	—	Traffic stops between CEs after "clear xconnect all" and SSO in AToM L2L
CSCtc54248	—	CDP neighbors aren't seen on sub-intf when it is disabled on main intf
CSCtc54878	—	NDE direct export packets are checked by egress ACL
CSCtc57356	—	IOS SLB nat pool uses addresses outside range
CSCtc58817	—	[VSS] Incorrect pMASK fpoe on standby causes traffic black-holed
CSCtc61506	—	VSS:VPLS TE traffic dropped on changing data paths.
CSCtc63032	—	Memory allocation failure on 12.2(33)SXI2a using DIA/DHCP Snooping
CSCtc64355	—	Online removal of standby SUP does not reflect to 'show module' command
CSCtc65227	—	standby keeps on reloading when renaming to a profile name with "
CSCtc70462	—	port-security Line-by-Line sync verifying failure
CSCtc71996	—	SSO : Bulk-sync failure at "ip flow-export source"
CSCtc78951	—	C2W2C: port's not recovering from "s" state with non-default native vlan
CSCtc79335	—	Sup Crash on several locations with IP SEC config
CSCtc80800	—	Config sync failure when call-home profile ends with a empty string.
CSCtc81612	—	VSS: Service Module reload triggers corrupted SP program counter
CSCtc81772	—	High cpu utilization with IPv6 ACL
CSCtc90469	—	Supervisor module crashes just after boot up with ACL Deny Test Failure
CSCtc91312	—	Switches crashed when attempting to power on phones after time change
CSCtd00423	—	Spurious memory/crash at adj_from_oce_base after wccp redirect ACL mod
CSCtd01483	—	With fm platform debug on when private-host is config'd the switch crash
CSCtd09117	—	CSM config sync timing out
CSCtd11309	—	VS2 ENTITY-ALARM traps not sent from slave chassis modules
CSCtd13853	—	Linecard interfaces going into UDLD errdisable state on reload
CSCtd13970	—	'ip cef accounting per-prefix non-recursive' breaks hw-based PBR
CSCtd16863	—	6500 PoE issues with 1120 line of APs when using dot1x
CSCtd18573	—	EARL-SPSTBY-2-SWITCH_BUS_IDLE: & PF_ASIC dump with 'clear mls qos'
CSCtd18807	—	"set ip next-hop <>" should lookup next hop in VRF when used on VRF int
CSCtd21153	—	Packets are not netflow switched for wccp-L2-redirect(inbound)with hash
CSCtd21951	—	C2W2B: "parser config cache interface" does't work with PO correctly

Identifier	Technology	Description
CSCtd25133	—	APS K1K2 Bytes Transmission shows channel mismatch
CSCtd26829	—	VSS: Duplicate packets after VSL link change
CSCtd26868	—	RACL blocks L2 switched traffic when adjacency is recirc2.2
CSCtd27768	—	CISCO-ENTITY-FRU-CONTROL-MIB reports missing module 12.2.(33)SXI2a
CSCtd31143	—	SPA in CC mode with SSO breaks connectivity when other sup comes online
CSCtd33166	—	router crash @ parse_call_action_func
CSCtd35521	—	MVPN PIM neighborship is not formed within vrfs
CSCtd39596	—	OIR of the LC causes bootup diagnostic to fail on TestL3VlanMet
CSCtd43793	—	Web Authentication is triggered after removing fallback configuration
CSCtd45736	—	EOAM:LB functionality is broken from 11/17 due to CSCtb70578
CSCtd46920	—	Watchdog timeout crash after CPUHOGs in 'Switch IP Host Track Process'
CSCtd49505	—	VSS gets to be multicast traffic blackhole after DAD or switchover
CSCtd58314	—	memory corruption crash with sh ip arp inspect log
CSCtd59664	—	%ERROR: Standby doesn't support this on configuring speed on SIP-400 int
CSCtd60858	—	Spurious accesses while testing dot1x accounting
CSCtd63041	—	%CONST_DIAG-SP-3-HM_FCI_0_STUCK on Mago
CSCtd64261	—	LBL config sync failure for extended vlan name changes
CSCtd66689	—	sip400/ChOC3: Quick shut/no-shut on controller leaves T1s in down state
CSCtd69637	—	Remote end port stays up/up when local port is down/down
CSCtd72243	—	sh int <port> transceiver incorrectly shows Module x doesn't suppot DOM
CSCtd72437	—	Packets punted to software forwarding when route-map is used for NAT
CSCtd76204	—	FPOE_DB-SP-4-ENTRY_USAGE_FULL messages with large vlan config in SXI3
CSCtd78587	—	Crash when recovering a port which was err-disabled twice
CSCtd82666	—	[VSS] Incorrect pMASK fpoe on standby causes traffic black-holed
CSCtd92043	—	Ph2 rekey use wrong proxy-id's on cat6k ezvpn ipsec-spa-2g
CSCtd93384	—	Etherchannel on switch working but interfaces showing shutdown
CSCte00934	—	SLOTCACHE is not updated with "write mem".
CSCte03275	—	Configuring TE tunnels on a causes chunk corruption on the SP.
CSCte04768	—	TestErrorcounter is not counting interrupt on the WS-X67XX linecard
CSCte08785	—	mac notification change history log not seen for deleted mac entries.
CSCte15193	—	c2w2c:"no spanning-tree vlan 16" command is not removed from standby
CSCte17961	—	Web Authentication is triggered after 802.1x authentication
CSCte20914	—	SPAN Reflector not enabled for WS-SVC-ADM-1-K9 : 2nd Commit
CSCte21190	—	WS-X6148A-GE-TX ports 25-32 stop forwarding traffic
CSCte21958	—	Router crashed at l2tun_app_mgr_process when xconnect is configured
CSCte28703	—	cat6k/VSS: fast-hello packet not send to standby SP CPU
CSCte30224	—	Compiled Tcl script crashes when generating a random number

Identifier	Technology	Description
CSCte35598	—	Extra vlans get created from MVRP Packet recieved from 3rd party device
CSCte40044	—	SXI: Medium buffer failure followed by 6k crash
CSCte40472	—	FWSM: Private vlan association not syncing on VSS systems from switch
CSCte41199	—	[VSS] MEC port on standby SW appears "missing port in hw"
CSCte43407	—	No %LINK-3-UPDOWN log for SPAN destination port
CSCte48967	—	VSS : isolated pvlan not associated with VRF on DFCs
CSCte50279	—	Need to allow disabling power to empty slots
CSCte56366	—	DSCP values are not mapped to RX priority queue
CSCte56437	—	TCP connection loss due to NAT incorrect translation on cat6500
CSCte71999	—	Replace ISSU capability negotiation workaround for 4k
CSCte72214	—	ME6500 - Traffic may be dropped on applying cos-map.
CSCte76471	—	sup32 SP hangs on process watchdog
CSCte79217	—	ICCQ never decreases, flow stats affected, (S,G) expires
CSCte81230	—	IP Source Guard feature goes into an incorrect state
CSCte83052	—	Xauth is getting disabled when putting keyring into isakmp profile12.2
CSCte87347	—	FPGA upgrade of CHT1E1 to 2.8 is not successful
CSCte89428	—	SNMP tty traps not sent
CSCte89787	—	Segment Switch manager Error followed by crash at 'sw_mgr_sm_cm_send_msg
CSCte90108	—	VS:monitor traffic fabric wrong for sw1-2,mod3/ch1 and mod8/ch0 -> RPR
CSCte90261	—	6500 PoE issues with 1120 and 1230 line of APs when using dot1x
CSCte90801	—	SCP async queue of LC1/LC2 get closed when fan module removed
CSCte96453	—	Switch intermittently crashes bringing up port with energywise level 10
CSCtf02760	—	Kernel crash (cache error) without any crashinfo generated
CSCtf07907	—	Crash observed @ atom_mgr_activate_dataplane
CSCtf08607	—	%BIT-SW1_SP-4-OUTOFRANGE: bit 1797 is not in the expected range of 1920
CSCtf09903	—	line vty 5 15 can't be deleted on sup32
CSCtf12294	—	Memory leak in ceDiagBootUpFailedNotif trap
CSCtf15479	—	VSS: TestMatchCapture failure causing Sup Minor error after manual failo
CSCtf16330	—	DHCP Rogue Server Detection : Multiple DHCPDISCOVER's issue
CSCtf23313	—	C2W2C: Standby Crashes continuously after ISSU LV
CSCtf34183	—	Client can not register to SAFF after correcting wrong user ID
CSCtf36557	—	Cat6K platform side changes related to CSCsk65812
CSCtf37626	—	Ospf flaps with oversubscription on enhanced flexwan Multilink T1
CSCtf39183	—	OBFL Master may not be initialized after IOS upgrade from SXF to SXH
CSCtf51278	—	PIM snooping : Router port missing in multicast mac entry
CSCtf51541	—	Mistral reset due to TM_DATA_PARITY_ERROR error
CSCtf52407	—	Sup720 may reload when passing GRE traffic

Identifier	Technology	Description
CSCtf53433	—	Knob 'platform ipv6 acl punt extension-header' default should be false
CSCtf54617	—	Supervisor fails to come up due to bad compact flash.
CSCtf62507	—	Netflow s/w switched flow not entried if disable/enable ip flow ingress
CSCtf64296	—	SFP on sup720 port 2 show inventory display garbled characters
CSCtf71990	—	Call-home message not sent on reload if source-ip-addr is configured
CSCtf75608	—	No PIM neighbour on newly created SVI
CSCtf77734	—	wrong message is displayed even though cos-map for all ports are removed
CSCtf81843	—	Enh VSS: Fast-Hello interface Allowed commands
CSCtf83737	—	Standby Supervisor crashes on bootup @ fib_vrf_mgr_lookup_vrf
CSCtf83906	—	W2.Clix: after apply/remove/re-apply v6 ACL's, TCAM full
CSCtf83970	—	IO MALLOCFAIL SSO mode
CSCtf88089	—	VSS: TB's seen with SSO
CSCtf89494	—	QoS: bandwidth remaining percent of non-LLQ policy is not reflected
CSCtf91692	—	Insertion of 6708/6716 linecard into the chassis resets another linecard
CSCtf94697	—	failed SCP transfer can crash router
CSCtf96643	—	Supervisor crashing qm corruption (Block overrun)
CSCtf97963	—	VSS DFC card miss MN setting, 4Sup: ICS MN ORPOE error
CSCtg06121	—	W2.Clix:Active sup crashes on doing ICA reset of the standby vss switch
CSCtg08523	—	%CONST_DIAG-SP-3-HM_TEST_FAIL:TestIPSecEncrypDecrypPkt seen randomly
CSCtg29266	—	Increasing DHCP snooping database size
CSCtg41173	—	Checkout CSCte68072 (CoPP for VRRP,BFD,GLBP) from w2clix
CSCtg58235	—	Minor Error @ bootup on multiple 8xCHT1/E1 SPA cards.
CSCtg73213	—	c2w2c - Crash seen on Configuring ATMoMoGRE
CSCtg78883	—	Patch triggers EARL Recovery.
CSCtg79692	—	W2C: Multicast traffic duplicated when OIR card comes back up
CSCee55603	Infrastructure	SNMP ACL does not work for VRF interfaces
CSCee83031	Infrastructure	test crash, dumping log before command is displayed
CSCek77907	Infrastructure	show run partition does not work with vrf aware ospf process
CSCin66315	Infrastructure	Inconsistency with sysuptime and rttMonLatestRttOperTime
CSCin89580	Infrastructure	Incorrect entry returned by SNMP query in CAT6k platform
CSCsd55997	Infrastructure	archive tar /xtract prematurely stops unpacking files if target is LEFS
CSCse97095	Infrastructure	C2W1: int range po shows it can allow upto 445 ports against 256 max
CSCsh64390	Infrastructure	SNMP Proxy Get-Next fails when called with a single OID.
CSCsk85192	Infrastructure	copy command with : after attribute is not checked against ACS. .
CSCsl52962	Infrastructure	interface range Port-channel command causes RP crash
CSCsm95041	Infrastructure	Write command causes SBY RP to crash if 2nd user viewing startup config
CSCso40612	Infrastructure	7600 HA router crashed @ parser_syntax_cleanup on

Identifier	Technology	Description
CSCsv81952	Infrastructure	CLI Views: Standby Reloads after creating view or Superview
CSCsx10028	Infrastructure	Core dump may fail to write
CSCsx27136	Infrastructure	carson ION: crashinfo from Dome drops last character/line
CSCsy24505	Infrastructure	Process "sbin/dfs_disk0.proc" crashed while inserting CF @ dfs_id_delete
CSCsy46543	Infrastructure	HTTP command "default interface" reboots WS-X4503+ SUP in red. mode.
CSCsy94827	Infrastructure	Support for ":" Illegal character should be removed
CSCsz09775	Infrastructure	Routers may fail to create crashinfo due to mallocfail in mem corruption
CSCsz29272	Infrastructure	Crash issuing commands on SP after SCP transfer
CSCsz38328	Infrastructure	DDNS HTTP packet has ip address instead of FQDN in 'Host' field
CSCta18073	Infrastructure	Memory leak in "IP SLAs Event Pr"
CSCtb37662	Infrastructure	Deferencing a null ptr in syncNlmLogTableVarbind_callback leads to crash
CSCtb40985	Infrastructure	IP SLA memory leak with invalid source address
CSCtb47647	Infrastructure	Active RP crashed at pim_send_join_prune
CSCtb59930	Infrastructure	Tacacs+ rem_addr field not sent in HTTP authentications
CSCtc21712	Infrastructure	TE-RFC-MIB:mplsTunnelPerfHCPackets/Bytes show incorr value
CSCtc43231	Infrastructure	SNMP Informs Source Interface Command not working
CSCtc61794	Infrastructure	ISSU/SSO upgrade fails with "logging discriminator" commands
CSCtc86476	Infrastructure	Cannot set value for rttMonEchoAdminCodecPayload greater than 1500
CSCtc87480	Infrastructure	dir slavenvram and wr mem triggers slavenvram:/(Device or resource busy)
CSCtd62220	Infrastructure	%DATACORRUPTION-1-DATAINCONSISTENCY: copy error,
CSCte52416	Infrastructure	VSS member switch crash when power down active switch
CSCte79777	Infrastructure	Syslog with filter: Process hog by Logger and crash
CSCtf04954	Infrastructure	Depracate cns config notify diff on pre-component code
CSCec19891	IPServices	DHCP client needs automatic route to DHCP server via default gateway
CSCeg27235	IPServices	DHCP: BOOTP sends RENEW request which causes problems
CSCsa47672	IPServices	NAT refcount counter maximum value of 65536 (64K)
CSCsc35536	IPServices	memory leak when no serivce dhcp/service dhcp
CSCse01431	IPServices	NAT-CCE : NAT SBC : outside sip call not go through
CSCse59109	IPServices	high CPU usage when IP SLA is enabled
CSCse70141	IPServices	Tracebacks @ ipnat_nbss_is_special_packet
CSCse72665	IPServices	Mem leak at ipnat_remove_static_cfg and ipnat_add_static_cfg
CSCsg89055	IPServices	Traceback due to NBSS pak parsing during IMBlock PhaseII testing
CSCsi93916	IPServices	Alignment Error/ Traceback @ ipnat_nbss_is_special_packet/ latest SPUD
CSCsj19805	IPServices	ip igmp static-group broken after reload on int vlan on a 7600
CSCsl76411	IPServices	IOS FTP client does not support multi-line replies
CSCso06542	IPServices	NAT VRF command gets corrupted in running config
CSCsy24878	IPServices	DHCPv6 relay CLI allows any int for output causing severe problems

Identifier	Technology	Description
CSCsz51146	IPServices	TCP bad segment and sequence number in BGP raises CPU on SXI1 modular
CSCsz56393	IPServices	Modular IOS - SUP720 - Sends malformed syslog packet
CSCsz72591	IPServices	Router configured as a DHCP client crashes with crafted DHCP packet.
CSCsz91851	IPServices	NAT : ESP packets not translated with static NAT outside translation
CSCsz97239	IPServices	PmtuAger Expiration and MSS value
CSCta08194	IPServices	Router crashes when reprovisioning AToM tunnel
CSCta10764	IPServices	uSBC RLS4:SBC SIP no vrf aware when overlapping address
CSCta23301	IPServices	FTP: ctrl and data conn do not get terminated when cp'n 0 byte fileftp
CSCta55610	IPServices	ISSU(MCPDEV->RLS3X):Stby failed to come up after R1 reload
CSCta56667	IPServices	tcp.proc displays excessive cpu usage
CSCta77091	IPServices	"socket SO_UDPCHECKSUM option setting failed" when sla responder
CSCta83548	IPServices	NAT Platform: unable to clear an specific nat entry
CSCta89283	IPServices	Add support for NAT redundancy feature in SX releases
CSCta97782	IPServices	delay reload timer incorrectly start when standby changing to active 1st
CSCtb58282	IPServices	show tcp brief can cause crash
CSCtb72550	IPServices	Call Detail Record File not created in FTP Server
CSCtc17163	IPServices	rsh command does not honor enable setting
CSCtc18841	IPServices	arp entry becomes incomplete state with local-proxy-arp
CSCtc22729	IPServices	proxy-arp inconsistent with HSRP ipv4 and GLBP ipv6 in 122-33.SXI
CSCtc55616	IPServices	RSA key generation from SSH session disables SSH service in ION
CSCtc60424	IPServices	EBGP Neighbor send to another port for FIN packet
CSCtd13820	IPServices	Show Standby causes unexpected exception to CPU: crash at standby_show
CSCtd13999	IPServices	Bugs in the Path-mtu logic
CSCtd16493	IPServices	port xx in use by system error while configuring NAT
CSCtd21890	IPServices	Router crash at dhcp autoinstall
CSCtd32285	IPServices	No nat translation with PAT applied on VRF interfaces
CSCtd46206	IPServices	After Reload NAT does not create dynamic aliases and arp entry.
CSCtd60670	IPServices	Username not included in the SNMP trap when tacacs authentication used
CSCtf21937	IPServices	UDP Modular IOS sends out DHCP Packet with diff source-IP comp. to IOS
CSCtf34691	IPServices	HSRP group name tied to static NAT for redundancy is not saved to config
CSCsc62963	LAN	Have configurable MTU Range 1500 -1530 on PA-1FE and PA-2FE
CSCtd47338	LegacyProtocols	DLSw generates corrupted internal router UDP pakets
CSCte78230	LegacyProtocols	DLSw Ethernet Redundancy and IPV6 will not work together
CSCta48816	Management	CDP Protocol: %SYS-2-GETBUF: Bad getbuffer, bytes= 32717
CSCtc40711	Management	next-hop verify-availability still forwards traffic with no CDP neighbor
CSCtc45716	Management	SNMPWALK of ipRouteEntry.7 with a view configured triggers high CPU
CSCtd43540	Management	Memory leak at cdp_handle_version_info

Identifier	Technology	Description
CSCej82248	MPLS	%LFD-3-NOOCE: Traceback in lfd_fib_update_mpls_oces
CSCta32836	MPLS	Vrf is not getting deleted and stuck in this state (backout CSCsx74883)
CSCtb13472	MPLS	asr1:ldp:core session also flaps on flappping emulated ldp sessions.
CSCtb17388	MPLS	cmfi_vpnid_is_valid Invalid Vpn Id: messages while cfiging large# of vpn
CSCtc90579	MPLS	Block allocated by 'rsvp_hc_db_nbr_alloc' gets corrupted
CSCte56840	MPLS	Auto-bw collect timer maxed out
CSCsm13783	Multicast	No (*, G) join received from CE1 on PE1 MVPN
CSCsz47622	Multicast	Traceback seen at default_ip_raw_enqueue while testing gnat-vif
CSCta01025	Multicast	Inconsistent multicast MIB output compared to show ipmroute
CSCtb76828	Multicast	%SYS-2-BADSHARE: Bad refcount in datagram_done for MSDP process
CSCtc43521	Multicast	During soft link recovery, PIM flaps seen with other PIM neighbors
CSCtf11034	Multicast	PIM Join/Prune with RP-bit set is not NATed
CSCtf34720	Multicast	DR will not send periodic join for SSM group with "static-group" config
CSCdj40945	PPP	PPP multilink MRRU value is not configurable
CSCsi49953	QoS	sip1- tx cpu crashes @ blt_pak_holdq_peek with RCK070410
CSCsl70963	QoS	Priority and class default pkts drop-H/W MLP+fragment+llq on SIP400
CSCta26106	QoS	RSVP-3-CONSISTENCY error followed by an unexpected reboot.
CSCdp10763	Routing	EIGRP:(12.0S only)Once manual summary Admin Distance set, cannot chg
CSCdz75312	Routing	EIGRP does not work when seq number becomes negative
CSCek27981	Routing	NRT:dn6 script fails due to timing issue. .
CSCsa86801	Routing	Traceback messages seen at ipigrp2_route_map_inform.
CSCsd14873	Routing	Allow Multiple EIGRP Processes To Use the Same RID on One Router
CSCsd78551	Routing	EIGRP internal route tag is not carried across PE routers
CSCse25308	Routing	EIGRP Neighbor relationships are torn down after changing the MTU Size
CSCsi46522	Routing	During ciscoEigrpMIB access ,Spurious memory access made @ mib_get_intf
CSCsk47893	Routing	eigrp stub function doesn't work correctly
CSCsk92412	Routing	EIGRP:PE-CE:HopCnt/SoO attrs skipped when redist w/metric on route-map
CSCsl65407	Routing	EGIRP SOO: Routing loop occurs when modifying EIGRP metrics on CE-PE i/f
CSCsl76135	Routing	Tracebacks seen when eigrp neighbour goes down.
CSCsm14899	Routing	ip nhrp cache non-authoritative command should not be hidden
CSCsm25000	Routing	IPv6 Route not removed from routing table: metric == infinity
CSCsm62215	Routing	Bus error crash with NHRP
CSCsm79085	Routing	EIGRP routes flapping due to nexthop changed
CSCsm95129	Routing	"no ip next-hop-self eigrp" not working when redistribute from BGP
CSCso56038	Routing	%DUAL-3-INTERNAL traceback at igrp2_packet_community_add_item
CSCso98964	Routing	EIGRP authentication not working for long key-strings
CSCsr49376	Routing	Switch crash at eigrp_ipv4_rib_rdbupdate

Identifier	Technology	Description
CSCsr51164	Routing	distribute-list command conversion to use parser db
CSCsr82785	Routing	APS Failover of large # of interfaces takes a long time
CSCsu25206	Routing	EIGRP tag-based filtering broken if tag is changed on the fly
CSCsu78975	Routing	Crash seen @adj_switch_ipv4_generic_les on 38xx router
CSCsv56081	Routing	ACE sequence numbers changed after the 2nd switchover
CSCsv66694	Routing	EIGRP:tag not set correctly from BGP community info
CSCsv77932	Routing	Router crash while configuring serial int for insufficient mtu
CSCsw22106	Routing	Switch crash at eigrp_ipv4_rib_rdbupdate continuation of CSCsr49376
CSCsw42724	Routing	EIGRP: cant reach SSO terminal state with distribute-list in VRF context
CSCsw80640	Routing	%SYS-2-SHARED errors when forwarding UDP packets
CSCsw91250	Routing	IP-EIGRP(0) 100: Internal Error, -Traceback@dual_packetize_interface
CSCsx18270	Routing	EIGRP: tags from version 2 peers are not displayed in topology table
CSCsx20147	Routing	Incorrect metric calculation for EIGRP for IPv6
CSCsx42982	Routing	EIGRP query is sent to stub peers when MD5 authentication is enabled
CSCsx70561	Routing	IOS will retain the community-list name even after unconfig
CSCsx75866	Routing	EIGRP Stub-Site: routing loop when poison suppressed
CSCsy42615	Routing	Entries missing from OSPF router route table
CSCsy56736	Routing	SIP-200 crash with "ip rtp-header compression format ietf" in MLPPP
CSCsz36368	Routing	EIGRP extended community synchronisation issue
CSCsz43096	Routing	Getting mismatch pkts in show ip cache verbose flow,com. to expected one
CSCsz53614	Routing	Incorrect notification sent to OSPF when subinterface added
CSCsz76616	Routing	PPP negotiation does not happening
CSCta05516	Routing	EIGRP offset-list does not rescan when ACL is modified
CSCta07104	Routing	Config-Sync & Traffic failure in VPN SSO scripts
CSCta19718	Routing	%SCHED-3-STUCKTMR: Sleep with expired timer
CSCta46880	Routing	Directly connected IP adress is learnt via ISIS, "clear ip rou" fixes.
CSCta60119	Routing	non recursive accounting can cause prefixes linked to drop
CSCta79313	Routing	Traceback seen when modifying route-map associated with BGPredistributio
CSCta93223	Routing	Router crashed upon confuguring ip extcommunity and issuing show run
CSCta99162	Routing	Switch reloads when entering the command passive-interface default
CSCtb01505	Routing	Router crashes with ospf_build_net_lsa
CSCtb01934	Routing	sh ip bgp vpnv4 vrf <VRF> x.x.x.x longer/shorter commands do not work.
CSCtb35914	Routing	nsf command not available in non-modular IPBase image.
CSCtb36384	Routing	ipdatastart_iph() could cause problem when called from interrupt path
CSCtb37132	Routing	OSPF NSF processing fails on iprouting process restart
CSCtb38882	Routing	OSPF-MIB returns only one OSPF process 12.2SX
CSCtb43448	Routing	EIGRP:interf cmds not removed from Standby conf when deleted from Active

Identifier	Technology	Description
CSCtb70508	Routing	OSPF Summary route not advertised after convegence/flaps from CE to PE
CSCtb82674	Routing	IS-IS adjacency stays down after switchover
CSCtb91412	Routing	Ipv6/named-mode/Eigrp session goes down if one of ipv6 addr is deleted
CSCtb94723	Routing	31SB16:RR sending illegal pfx in withdraw to old style MDT PE
CSCtc01196	Routing	Carson: ISIS topology broken after 2-3 consecutive SSO
CSCtc31545	Routing	EIGRP - Active routes remain in topo table after link flap
CSCtc36727	Routing	ospfNbrIpAddr unnumbered interface entries don't include the neighbor IP
CSCtc39809	Routing	Memory leak @ dual_sia_active
CSCtc57092	Routing	Standby resets due to MCL issue with offset-list name inconsistency
CSCtc59162	Routing	EIGRP resync is not triggered when modifying inbound/outboun prefix-list
CSCtc70737	Routing	Static routes are not in EIGRP topo table after add/remove the static
CSCtc72772	Routing	Bulk sync failure and Standby reloads continuously @ "clns route"
CSCtc73440	Routing	Changing interface ip address/mask triggers a bad OSPF route
CSCtd00479	Routing	ISIS IETF NSF fails on LAN interface when restarting router is a DIS
CSCtd07257	Routing	OSPF does not remove unnecessary redistributed routes
CSCtd42462	Routing	Show CLNS traffic command output showing negative values.
CSCtd48455	Routing	Summary and components seen after 'clear ip route' w/ ip summary-address
CSCtd49246	Routing	round-trip average of ping MIB may show less value
CSCtd68197	Routing	mem leak in IPv6 RIB Redistribute with EIGRP Work Ent
CSCtd73256	Routing	a catalyst switch may reload unexpectedly during 'show ip ospf int'
CSCtd73951	Routing	OSPF discard-route(Null0) is deleted when area auth command is removed
CSCtd86572	Routing	DMVPN EIGRP next hop update not sent to spoke
CSCte10790	Routing	c6500: device crashing on removing ace entry or entire acl
CSCte29212	Routing	EIGRP summary leak-map is not independent of AD keyword
CSCte39250	Routing	Router crashes @ ipv6_show_interface
CSCte53365	Routing	Connected global address not in eigrp topo after 'no shut' v6 process
CSCte54840	Routing	Router crashed at ospfv3_routerid_command during simultanious operation
CSCte54852	Routing	Route of non-first interfaces on Secondary Module is added later
CSCte57710	Routing	Process replies to ping to I/F downed unlike cef handling.
CSCte58468	Routing	OSPF conditional default route not advertised after config removed
CSCte58962	Routing	Line-by-Line sync verifying failure after "no router ospf" command
CSCte69761	Routing	Default Route deleted when prefix marked as candidate default is deleted
CSCte73093	Routing	distribute-list with an explicit interface does not work.
CSCte91997	Routing	DHCP breaking when DHCP server and VRRP master are same.
CSCtf06436	Routing	high CPU due to HW backwalk continually walking the looped OCE chain
CSCtf16300	Routing	clear arp-cache is not working correctly
CSCtf45374	Routing	Eigrp route-tags not sent using distribute-list

Identifier	Technology	Description
CSCei66915	Security	Incorrect option for ip-address under crypto pki
CSCsb10291	Security	$$TS: Router forced crash on PKI Bind service failure (C_UnbindService)
CSCsd84640	Security	SSH2 Error message should adhere to Cisco Syslog Format
CSCsd98525	Security	SSH2 session closes prematurely
CSCse31829	Security	Memory leak in Crypto IKMP process
CSCsf17411	Security	trustpoint authentication fails if key usage is non standard
CSCsg75994	Security	Show login failure output does not display Username
CSCsk05015	Security	USERAUTH_SUCCESS not handled correctly for "none" auth method
CSCsl02104	Security	SSH Unexpected mesg type received should display in Cisco Syslog Format
CSCsl10459	Security	show crypto pki timers command causes a software forced crash
CSCso27236	Security	IOS CA client shows renew date 1 Jan 1970
CSCsu29044	Security	Inconsistencies attaching policies to Tunnel and physical interfaces
CSCsv54863	Security	IOS PKI: Not expired Certificate is deleted if autoenrollment fails
CSCsv92274	Security	SSH process might not handle some IPC messages
CSCsx17447	Security	IOS not including HOST header in HTTP CRL request
CSCsz83570	Security	SSH Sessions disconnect when viewing logs w/ pagers
CSCsz84055	Security	System crashed unexpected while open ssh2 session
CSCsz92328	Security	Some configs not synced with crypto certificate configured on active
CSCta77073	Security	Router Crash while unconfiguring crypto trustpoint
CSCtc12312	Security	PKI may get stuck after 32678 CRL fetches
CSCtc41114	Security	New SSH sessions with RSA key fails after changing hostname
CSCtd35586	Security	Tunnel on VRF bring down due to HSRP status change on Non VRF
CSCtd78270	Security	12.2 : ssh feature needed to allow selection of rsa keys to use
CSCtf47512	Security	SXH5: Memory leak in ACE HAPI and IPSec Key Engine
CSCsw31019	WAN	Router crashes while configuring the command "frame-relay be 1"
CSCtd22993	WAN	SNMP ifIndex for certain serial interfaces becomes inactive

Caveats Resolved in Release 12.2(33)SXI3

Resolved MPLS Caveats

- CSCsz45567—Resolved in 12.2(33)SXI3

  A device running Cisco IOS Software, Cisco IOS XE Software, or Cisco IOS XR Software is vulnerable to a remote denial of service condition if it is configured for Multiprotocol Label Switching (MPLS) and has support for Label Distribution Protocol (LDP).

  A crafted LDP UDP packet can cause an affected device running Cisco IOS Software or Cisco IOS XE Software to reload. On devices running affected versions of Cisco IOS XR Software, such packets can cause the device to restart the mpls_ldp process.

  A system is vulnerable if configured with either LDP or Tag Distribution Protocol (TDP).

  Cisco has released free software updates that address this vulnerability.

Workarounds that mitigate this vulnerability are available.

This advisory is posted at: http://www.cisco.com/warp/public/707/cisco-sa-20100324-ldp.shtml

Resolved Unknown Caveats

- CSCtc41760—Resolved in 12.2(33)SXI3

  Symptom: 6500 may experience redzone crash at UDLD process. Message may appear %SYS-SP-3-OVERRUN: Block overrun at 44456570 (red zone 6D000700) -Traceback= 40291448 402938DC 40D74570 40D763A0

  Traceback will vary from code to code.

  Conditions: UDLD configured

  Workaround: Disable UDLD.

- CSCsh61458—Resolved in 12.2(33)SXI3

  Symptoms: A Cat4k switch may reload after receiving a malformed packet on one specific specific port.

  Conditions: This symptom may be observed on a Cat4k switch that enables DNSIX audit trail and recieves crafted IP packets on a specific port.

  Workaround: Do not enable the DNSIX audit trail.

Other Resolved Caveats in Release 12.2(33)SXI3

Identifier	Technology	Description
CSCei37916	AAA	Incorrect AAA behavior when both wait-accnt & broadcast accnt is con
CSCsc97727	AAA	Access Point Crashes When Removing TACACS Server
CSCsq71492	AAA	IOS device crash or tracebacks at tplus_handle_req_timeout
CSCsy55362	AAA	Unresponsive Console/VTYs
CSCse75697	ATM	LOKI: ima clock should default to LINE, backout CSCin90422, CSCsb68536 .
CSCej00344	—	Crash when opening new session from router
CSCek53099	—	SIP200+4xT3/E3:Fail to load cRTP CFG from startup file
CSCsb88996	—	slb traceback spurious memory access after slb statefull switchover
CSCsk88751	—	Kron CLI Process 'show tech-support password
CSCso35876	—	SRB3:New active SP crash at label_entry_get_inlabel
CSCso36150	—	duplicate vlan names causing config-sync failures
CSCso79135	—	Wism controller ports 1 state is down after mod shut/unshut
CSCso79925	—	EC with enhanced hash method (PFC3C) has no knob to use old method (3B)
CSCsr04916	—	PBR dropped the packets after add set vrf vpn1 back to the route-map
CSCsr99518	—	Granikos should not init rekey after recieving new outbound SA at QM3
CSCsu29301	—	C2W21: Ingress SPAN on Sup - ACE module duplicates packets
CSCsu67413	—	RRI - Route disappears after ipsec rekey with multi int scenario
CSCsu81976	—	IPSEC NAT traversal fails to correctly track SAs
CSCsu84213	—	RPF-MFD hardware entry is missed after doing SSO.

Identifier	Technology	Description
CSCsv27372	—	telnet to a real(directed mode) via GRE tunnel crates SUP crash on SRC2
CSCsw28024	—	Router is getting crashed at crypto_ikmp_cfg_auto_update_parameters
CSCsx13442	—	After shut no shut hub tunnel, spoke cannot trigger isakmp SA
CSCsx81468	—	CWPA2: Drops CLNS Hello packets
CSCsy03587	—	c2w2b: SYS-2-MALLOCFAIL: Memory allocation failed seen with tracebacks
CSCsy07709	—	C2W2: %COMMON_FIB-4-FIBNULLIDB: Missing idb for fibidb Port-channel5A
CSCsy30937	—	Modify dual-active fast-hello function for rapid detection and recovery.
CSCsy34566	—	Disable VLAN mapping on ME6524, 6148A-GE-TX
CSCsy69740	—	SXH: Traffic drop on L2 PO after cleared psecurity on rcving L2 ports
CSCsz01976	—	Need a cli to dump the rommon environment and unset rommon variable
CSCsz04297	—	Cat6k: False Dynamic MAC entry is installed with format 0000.<LTL>.0000
CSCsz23445	—	%PORT_SECURITY-SP-6-INVALID_SESSION: Invalid Port-Security ISSU Session
CSCsz36826	—	6509E fan-tray failed to restore back to HP mode after OIR
CSCsz50968	—	ace interface and vlans up but has no ip connectivity to CAT 6K
CSCsz74896	—	VSS redundancy reload shelf X causes UDLD err-disable
CSCsz76015	—	C2W2: Need cli to set PF_BIAS to ensure lower slot# Sup boots as active
CSCsz81520	—	MRIB_PROXY-2-MRIB_RP_FAILED_GET_IPC: RP failed allocating IPC buffer
CSCsz81627	—	spurious memory accesses due to snmp
CSCsz83701	—	W2B: SFP-UTP entPhysicalVendorType cevSFP1000BaseSx to zeroDotZero
CSCsz84544	—	output drops increment on not-connected interface of 6548GE-TX module
CSCsz86787	—	IPV6 mcast and IPV4 EMVPN VRF Lite traffic are not forwarded after SSO
CSCsz87648	—	SP/RP and redundant system handshake broken when the kernel crashes.
CSCsz92137	—	Crash in crypto_destroy_sadb_root() upon unconfiguring tunnel protection
CSCsz92508	—	SPA module reloads when no response to keep-alive polling
CSCsz96469	—	Tracebacks seen @chunk_free_with_pc while unconfiguring
CSCta06175	—	Cat6500/SXH: Deleted configs re-appear on IDSM reset
CSCta06689	—	Rapid PVST:mac address table not flushed after topology change
CSCta10402	—	Tracebacks seen due to BFD PP Process
CSCta10870	—	FPOE takes long time to be programmed on active vss switch
CSCta14457	—	A Cisco device may report alignment errors
CSCta15415	—	DHCP Snooping functionality is not working fine with private vlan
CSCta15851	—	Changing allowed vlan mask causes WiSM LAG member ports to reset
CSCta17587	—	VRF + RHI combination does not work on FWSM
CSCta21771	—	%CONST_DIAG-SP-3-HM_FCI_0_STUCK: Flow control stuck at 0 error on modul
CSCta22749	—	C2W2b: %CONST_DIAG-SW1_SP-3-BOOTUP_TEST_FAIL:LC powercyled during Multip
CSCta27279	—	WCCP s/w switching with Ingress redirection & interface ACL
CSCta30298	—	CHKPT-SP-3-NOMEM: Memory leak seen and later the box crashed

Identifier	Technology	Description
CSCta32922	—	SP crash due to heartbeat failure.
CSCta36799	—	Router Crases @ ppcp_ppm_add_class_to_stored_policy_internal
CSCta36939	—	c2w2b:Crash On ISSU Run Version
CSCta42989	—	"%CSM parser state" configuring CLI when configuring via XML also
CSCta44166	—	Memory leak seen with dynamic crypto map
CSCta48968	—	Modular IOS kernel crashinfo has missing information
CSCta52689	—	cat6k crash in RP due to address error with wccp configuration
CSCta55498	—	[Modular IOS] MIPS CP0 registers save algorthim needs a few improvements
CSCta56676	—	IPsec SA liftime can go to negative values
CSCta57705	—	C2W2b: reg_invoke_vs_ltl_src_index_changed() needs to be added on stdby.
CSCta57778	—	auth-mgr/eap:: %IDMGR-3-INVALID_ID: bad id in id_get (bad table id)
CSCta60531	—	VSS Preemption causes CAM table updation fails in FWSM env
CSCta67007	—	c2hd1:VRF interfaces not shown and not pinging the CE's
CSCta68053	—	time-period does not take effect in configuration archive
CSCta74242	—	VSS: crash due to snmp get after standby chassis reloads
CSCta74315	—	WS-X6324-100FX-MM May Be Inoperable and Have Status "Other"
CSCta84749	—	Etherchannel should not be allowed if auto qos is enable
CSCta94179	—	Recirculated MPLS packets becasue of egress service policy are dropped
CSCtb03003	—	MAC table on standby Supervisor not flushed on link change
CSCtb15569	—	VPN-SPA - traffic failed to decrypt due to SecInfo check failure
CSCtb23289	—	Major temperature alarm has to force system shutdown
CSCtb27643	—	cat6000 Medium buffers leak on SP leading to crash
CSCtb38547	—	Incorrect CP0 values and empty kernel variable section in kernel crashin
CSCtb62523	—	PfR - inside prefixes not learned on cat6k BR
CSCtb63352	—	VSS: With 6KW DC PS, no power to bringup VSL supervisor or linecard
CSCtb66983	—	Nas-port-type is missing in Access-request
CSCtb68478	—	"Illegal nextSsIndex value" message should be removed
CSCtb83677	—	Power Deny for pre-standard power on SXI2 or Later
CSCtb87454	—	DHCP Rogue Server Detection
CSCee83031	Infrastructure	test crash, dumping log before command is displayed
CSCsd99763	Infrastructure	Cisco 7200 series reload unexpectedly while configuring BGP acces list
CSCsu65967	Infrastructure	Modular IOS crash at free_lite_internal
CSCsv30540	Infrastructure	Memory corruption in remove_ws when NULL string is passed
CSCsx10028	Infrastructure	Core dump may fail to write
CSCsy24505	Infrastructure	Process "sbin/dfs_disk0.proc" crashed while inserting CF @ dfs_id_delete
CSCsy31159	Infrastructure	ASR1k 'show history all' is NOT updated properly
CSCsy88640	Infrastructure	nested crash in crashinfo collection.

Identifier	Technology	Description
CSCsz29272	Infrastructure	Crash issuing commands on SP after SCP transfer
CSCta02715	Infrastructure	SXH5: RP crash on each booting time if <logging count> enabled
CSCtb37662	Infrastructure	Deferencing a null ptr in syncNlmLogTableVarbind_callback leads to crash
CSCsi99841	IPServices	vrf-aware trustpoint authentication/enrollment doesn't work
CSCsj19805	IPServices	ip igmp static-group broken after reload on int vlan on a 7600
CSCso06542	IPServices	NAT VRF command gets corrupted in running config
CSCsw65614	IPServices	NAT with route maps doesn't work for TCP application
CSCsz51146	IPServices	TCP bad segment and sequence number in BGP raises CPU on SXI1 modular
CSCsz89107	IPServices	high cpu due to ip_input process during SNMP trap
CSCta24043	IPServices	"%IPNAT-4-ADDR_ALLOC_FAIL" message seen when all ports are not allocated
CSCta27331	IPServices	HSRP authentication applied to secondary addresses fails
CSCta77091	IPServices	"socket SO_UDPCHECKSUM option setting failed" when sla responder
CSCta83548	IPServices	NAT Platform: unable to clear an specific nat entry
CSCta89283	IPServices	Add support for NAT redundancy feature in SX releases
CSCtb58282	IPServices	show tcp brief can cause crash
CSCsz05918	Management	CDP neighbors do not come up on vlan interface
CSCsz75221	Management	A local variable in cdp takes up 2k process stack space-prompting crash
CSCej82248	MPLS	%LFD-3-NOOCE: Traceback in lfd_fib_update_mpls_oces
CSCsx82365	MPLS	LDP does not immediately send all IP addresses on new session
CSCsz75180	MPLS	Crash due to mpls subintf being removed
CSCsz92368	MPLS	MDEBUG-2-ACCESSFREED: @tc_handle_dead_peers Enabling/disabling "mpls ip"
CSCta32836	MPLS	Vrf is not getting deleted and stuck in this state (backout CSCsx74883)
CSCsm13783	Multicast	No (*, G) join received from CE1 on PE1 MVPN
CSCsz63723	Multicast	[UNI] MLD entry denied by mCAC isn't deleted.
CSCsz88850	Multicast	Rework CSCsz16580 fix
CSCta26106	QoS	RSVP-3-CONSISTENCY error followed by an unexpected reboot.
CSCsm57831	Routing	EIGRP: admin tags do not propagate between eigrp peers
CSCsm79085	Routing	EIGRP routes flapping due to nexthop changed
CSCsq83006	Routing	Port-channel down makes EIGRP SIA
CSCsu78975	Routing	Crash seen @adj_switch_ipv4_generic_les on 38xx router
CSCsw16157	Routing	Crash following OSPF and MPLS-TE tunnel changes
CSCsw42724	Routing	EIGRP: cant reach SSO terminal state with distribute-list in VRF context
CSCsz31770	Routing	Per-user static route is not installed on LNS after session established
CSCsz43096	Routing	Getting mismatch pkts in show ip cache verbose flow,com. to expected one
CSCsz76701	Routing	Supervisor crash with decodeds pointing to ISIS
CSCsz84906	Routing	isis redistributed route is not removed when interface shutsdown
CSCta08632	Routing	ISIS topology broken after Sup force-switchover with ispf

Identifier	Technology	Description
CSCta60119	Routing	non recursive accounting can cause prefixes linked to drop
CSCta93223	Routing	Router crashed upon confuguring ip extcommunity and issuing show run
CSCta99162	Routing	Switch reloads when entering the command passive-interface default
CSCtb01505	Routing	Router crashes with ospf_build_net_lsa
CSCtb35914	Routing	nsf command not available in non-modular IPBase image.
CSCtb43448	Routing	EIGRP:interf cmds not removed from Standby conf when deleted from Active
CSCsc49862	Security	IPaddress in Subject Alternative Name is not parsed correctly.
CSCso27236	Security	IOS CA client shows renew date 1 Jan 1970
CSCsv54863	Security	IOS PKI: Not expired Certificate is deleted if autoenrollment fails
CSCsy74318	Security	aaa authentication fail-message not displayed over SSH
CSCsz84055	Security	System crashed unexpected while open ssh2 session

Caveats Resolved in Release 12.2(33)SXI2a

Identifier	Technology	Description
CSCsu65967	Infrastructure	Modular IOS crash at free_lite_internal
CSCtb15569	—	VPN-SPA - traffic failed to decrypt due to SecInfo check failure
CSCtb27643	—	cat6000 Medium buffers leak on SP leading to crash

Caveats Resolved in Release 12.2(33)SXI2

Resolved Infrastructure Caveats

- CSCsx49573—Resolved in 12.2(33)SXI2

  Symptom: Three separate Cisco IOS Hypertext Transfer Protocol (HTTP) cross-site scripting (XSS) vulnerabilities and a cross-site request forgery (CSRF) vulnerability have been reported to Cisco by three independent researchers.

  The Cisco Security Response is posted at the following link: http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20090114-http

  Conditions: See “Additional Information” section in the posted response for further details.

  Workarounds: See “Workaround” section in the posted response for further details.

Resolved IPServices Caveats

- CSCsv87997—Resolved in 12.2(33)SXI2

  Symptom: DHCPv6 relay process crash on Actice RP.

  Conditions: Unknown at this time.

  Workaround: Unknown at this time.

- CSCsw18636—Resolved in 12.2(33)SXI2

  Symptoms: High CPU utilization occurs after device receives a ARP packet with protocol type as 0x1000.

Conditions: This problem occurs on Supervisor 32 running Cisco IOS Release 12.2(33)SXI. This problem may also occur on Supervisor 720. The problem is only seen when you have bridge-group CLI being used, which leads to ARP packets with protocol types as 0x1000 being bridged. The problem does not apply for IP ARP packets.

Workaround: Filter the ARP packet. The device configuration should have bridge-group creation first, followed by interface-specific bridge-group options.

- CSCsx16152—Resolved in 12.2(33)SXI2

  Symptom: Under unique circumstances erroneous routing prefixes may be added to the routing table.

  Conditions: When the DHCPv6 relay feature is enabled and a router receives a normal DHCPv6 relay reply packet, this may lead to an erroneous route being added to the routing table.

  Workaround: No workaround except turning off DHCPv6 relay.

Resolved MPLS Caveats

- CSCsz45567—Resolved in 12.2(33)SXI2

  A device running Cisco IOS Software, Cisco IOS XE Software, or Cisco IOS XR Software is vulnerable to a remote denial of service condition if it is configured for Multiprotocol Label Switching (MPLS) and has support for Label Distribution Protocol (LDP).

  A crafted LDP UDP packet can cause an affected device running Cisco IOS Software or Cisco IOS XE Software to reload. On devices running affected versions of Cisco IOS XR Software, such packets can cause the device to restart the mpls_ldp process.

  A system is vulnerable if configured with either LDP or Tag Distribution Protocol (TDP).

  Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are available.

  This advisory is posted at: http://www.cisco.com/warp/public/707/cisco-sa-20100324-ldp.shtml

Resolved Multicast Caveats

- CSCsm64082—Resolved in 12.2(33)SXI2

  Symptom: The router may report AUTORP-4-PAK_ERR.

  Conditions: PIM Auto-RP is configured and ip multicast boundary is enabled with filter-autorp option.

  Workaround: Configure ip multicast boundary without filter-autorp option.

Resolved Routing Caveats

- CSCsx73770—Resolved in 12.2(33)SXI2

  Symptom: A Cisco IOS device that receives a BGP update message and as a result of AS prepending needs to send an update downstream that would have over 255 AS hops will send an invalid formatted update. This update when received by a downstream BGP speaker triggers a NOTIFICATION back to the sender which results in the BGP session being reset.

  Conditions: This problem is seen when a Cisco IOS device receives a BGP update and due to a combination of either inbound, outbound, or both AS prepending it needs to send an update downstream that has more than 255 AS hops.

Workaround: The workaround is to implement **bgp maxas-limit X** on the device that after prepending would need to send an update with over 255 AS hops. Since IOS limits the route-map prepending value to 10 the most that could be added is 21 AS hops (10 on ingress, 10 on egress, and 1 for normal eBGP AS hop addition). Therefore, a conservative value to configure would be 200 to prevent this condition.

- CSCsy86021—Resolved in 12.2(33)SXI2

  Recent versions of Cisco IOS Software support RFC4893 (“BGP Support for Four-octet AS Number Space”) and contain two remote denial of service (DoS) vulnerabilities when handling specific Border Gateway Protocol (BGP) updates.

  These vulnerabilities affect only devices running Cisco IOS Software with support for four-octet AS number space (here after referred to as 4-byte AS number) and BGP routing configured.

  The first vulnerability could cause an affected device to reload when processing a BGP update that contains autonomous system (AS) path segments made up of more than one thousand autonomous systems.

  The second vulnerability could cause an affected device to reload when the affected device processes a malformed BGP update that has been crafted to trigger the issue.

  Cisco has released free software updates to address these vulnerabilities.

  No workarounds are available for the first vulnerability.

  A workaround is available for the second vulnerability.

  This advisory is posted at the following link:
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090729-bgp

Resolved Security Caveats

- CSCsx70889—Resolved in 12.2(33)SXI2

  Cisco devices running affected versions of Cisco IOS Software are vulnerable to a denial of service (DoS) attack if configured for IP tunnels and Cisco Express Forwarding.

  Cisco has released free software updates that address this vulnerability.

  This advisory is posted at
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-tunnels

- CSCsz32366—Resolved in 12.2(33)SXI2

  Symptoms: A Cisco router that is running Cisco IOS Release 12.4(25) may crash due to SSH.

  Conditions: This symptom occurs when SSH is enabled on the router. An attempt to access the router via SSH is made.

  Workaround: Do not use SSH. Disable SSH on the router by removing the RSA keys:

  “crypto key zeroize rsa”

  Further Problem Description: This issue has not been seen in Cisco IOS Release 12.4(23) and earlier releases. It also has not been seen in Cisco IOS Release 12.4T images.

Resolved Unknown Caveats

- CSCsy07555—Resolved in 12.2(33)SXI2

  Cisco IOS devices that are configured for Internet Key Exchange (IKE) protocol and certificate based authentication are vulnerable to a resource exhaustion attack. Successful exploitation of this vulnerability may result in the allocation of all available Phase 1 security associations (SA) and prevent the establishment of new IPsec sessions.

Cisco has released free software updates that address this vulnerability.

This advisory is posted at
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-ipsec

- CSCsy15227—Resolved in 12.2(33)SXI2

  Cisco IOS Software configured with Authentication Proxy for HTTP(S), Web Authentication or the consent feature, contains a vulnerability that may allow an unauthenticated session to bypass the authentication proxy server or bypass the consent webpage.

  There are no workarounds that mitigate this vulnerability.

  This advisory is posted at the following link:
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-auth-proxy

- CSCsy68923—Resolved in 12.2(33)SXI2

  Symptom: Cisco IOS device may reload in very rare circumstances after receiving certain packets. The BFD process may restart due to a critical software exception.

  Workarounds: None

Other Resolved Caveats in Release 12.2(33)SXI2

Identifier	Technology	Description
CSCei37916	AAA	Incorrect AAA behavior when both wait-accnt & broadcast accnt is con
CSCei62358	AAA	Downloading callback-dialstring as part of Tacacs+ author leads to crash
CSCsb34770	AAA	AAA Authentication banner for TACACS behaviour
CSCse12395	AAA	Check keys error for accounting does not cause failover
CSCsl63494	AAA	Issue with session accounting in AAA
CSCsz07569	AAA	Session id changes between interim and stop records
CSCsz43356	AAA	CPUHOG and Traceback after multiple SSH logins
CSCea90968	ATM	Bus error crash after (config-if)# atm pvp 1
CSCsx43905	ATM	Router Crash at dlcncia.c on 12.2(33.4.14)SXH
CSCek47612	—	TX cpu stats not displayed in sh hw-module slot proc cpu output
CSCek60142	—	FRR does not work (about 200 ms loss) with E5 SPAs,LC crash on link flap
CSCsd39568	—	stats support for PBR set ip nexthop/set interface
CSCsd45698	—	Cat6K: SLB punted to CPU if src_index is port-channel index
CSCsg35285	—	Slower Cache refresh for int stats when more interfaces up
CSCsh28072	—	ESM may cause rotuer to crash during IPS test attack
CSCsi50091	—	BFD session flaps after executing "undebug all" command.
CSCsj26698	—	Acct-Session-Id in Accounting-Request is different from in Access-Reques
CSCsj89208	—	RP hits TLB exception when SIP-400 OIR with 8k MPBE EFPs
CSCsk62032	—	DHCP snooping support to detect rogue dhcp servers
CSCsl35174	—	Setting Scorpion int MTU < packets injected results in perm 1-way traf .
CSCsm39160	—	TestCFRW shows incorrectly as failed in show diagnostic sanity
CSCsm79995	—	Tracebacks are seen while attaching service-policy in a atm pvc

Identifier	Technology	Description
CSCso39162	—	W2: SCHED-7-WATCH: Attempt to monitor... Process= "NAM_Process" & TB's
CSCso67500	—	mvpn-bidir: Reloading encap rtr and performing sso causes df index issue
CSCso79135	—	Wism controller ports 1 state is down after mod shut/unshut
CSCsq15198	—	EPC:SRD:RSP720:OSPF/BFD flaps when Gi5/2 (RSP gi link) is no shutted
CSCsq69567	—	SSO Switchover + unicast-routing chg cause MC traffic loss for 2 minutes
CSCsr15448	—	C2W2: E-OAM session not established b/w CE and PE on Port mode EoMPLS
CSCsr43461	—	vrf selection source < > missing under sh_run after router reload
CSCsr58151	—	C2W2: EOAM:errdisabled port doesn't recover even if errdisable rcvry en
CSCsr59237	—	OSPF adj flaps on WS-X6548-GETX, due to LTL / RBH programming mismatch
CSCsr62498	—	C2W2: Span dest port continuously sends some traffic on 6748 cards
CSCsr97387	—	Router crashed at crypto_delete_map_routes during ip address change
CSCsu05721	—	C2W2: %NTI-SP-3-AGENT_ERR and TB was seen after issu runversion
CSCsu40166	—	PBR packets send out to wrong next hop MAC after ACL is changed
CSCsu48241	—	memory leak when removing igmp snooping with acl filtering
CSCsu50413	—	RE: acl merge causes high rp cpu for ~50 min after reload
CSCsu52504	—	%LINEPROTO-SP-5-UPDOWN msg is output when changing cdp configuration
CSCsu95857	—	cardDescr (.1.3.6.1.4.1.9.3.6.11.1.3) is returning incorrect value
CSCsu99813	—	C2HD1-SI:Span Distributed Stops Traffic - Centralized Duplicates
CSCsv06453	—	Crashinfo file not created in certain cases when SP crashes.
CSCsv20768	—	After SSO s/wover, atm clock config changes to line and PTB to UNSTABLE
CSCsv24908	—	L2 Fwd Broken on other modules when SIP-400 int flaps
CSCsv27372	—	telnet to a real(directed mode) via GRE tunnel crates SUP crash on SRC2
CSCsv43187	—	120seconds after SSO, Some multicast traffic drops
CSCsv61458	—	[no] mpls ip propagate-ttl needs no mpls ip - mpls ip to take effect.
CSCsv74822	—	Crash on RPR switchover in the rf_proxy_rp_sync path
CSCsv79673	—	Router MAC learned dynamically after add/remove of xconnect on SVI
CSCsv94560	—	c7600/MPLS: Packet reflection over EoMPLS link when vc going up
CSCsv99620	—	Some tunnels are not programmed when ipsec updates GRE in mGRE/TP
CSCsw14147	—	VACL unable to capture traffic from RP
CSCsw21852	—	CSM: memory leak in process "Laminar Icc Event"
CSCsw24172	—	ES20:-%INTR_MGR-DFC2-3-INTR: Parsing Engine (X-Chip) [1]: Inbound Toast
CSCsw28972	—	enh: provide option for port security to not install L2 trap entries
CSCsw31607	—	LTL index incorrect in PI MET table
CSCsw38512	—	T/B upon SSO with VSS
CSCsw40790	—	SNMP Loop on PA-MC-T3+ interfaces (Installed)
CSCsw48824	—	Switchport Block Unicast - prevents RTP on same VLAN
CSCsw49623	—	Router crashes when PfR learn config is displayed on the border

Identifier	Technology	Description
CSCsw59517	—	IGMPv3 snooping drops 'Block Old Sources' report
CSCsw68514	—	SLB probes iin TESTing state while using client cmd in Vserver config
CSCsw69621	—	BR DOWN if inside bgp is only type of learning configured
CSCsw76117	—	TBs seen after redundancy mode change from sso to rpr
CSCsw76910	—	IOS-SLB:Supervisor crashes on configuring/verifying firewallfarm CLIs
CSCsw83488	—	Negative value seen for counters in vpn session
CSCsw91858	—	Misleading error when 6716 is configured for VSL
CSCsw92171	—	multiple "power-input" for new 6kW DC PS do not exist on Standby
CSCsw92386	—	Not able to delete logging filter and crash at Tcl_NewStringObj
CSCsw96176	—	BFD sessions with version 0 do not come up properly following a reload
CSCsx06578	—	SIERRA:MAGO switch got crashed after reload with SIERRA_INTEG_090106
CSCsx07137	—	Invalid " %FM-4-L2_DYN_TCAM_EXCEPTION" error message for some cases.
CSCsx09110	—	Failed to establish ipsec tunnel with CCM
CSCsx09273	—	WEBAUTH(IP adm) is not INITiating if IPDT entry already exists.
CSCsx10011	—	VSS: IO memory leak from pre_process_vsibc_vsda_pak
CSCsx13050	—	tcl doesn't run or Register event failed messages on Modular IOS
CSCsx19210	—	[show epm session ip 0.0.0.0] crashes supervisor
CSCsx20081	—	Local Web-Auth does NOT work when IP Source-Guard is enabled on port
CSCsx20862	—	Peer RP index unknown messages seen on VSS setup
CSCsx21431	—	Logging Filter CLI gets lost after SSO
CSCsx21886	—	ISSU switchover command sync issue
CSCsx22711	—	router crashes if we unconfigure 1024 GLBPv6 grp on intf and do sh mod
CSCsx27836	—	VS: STP state on standby SP shows DWN sometimes and SSO causes high CPU
CSCsx28532	—	VPN SPA freezes when ip mtu changed on tunnel interface
CSCsx29377	—	1 sec multicast loss on standby sup720-10g
CSCsx29645	—	IPv6 Multicast traffic can not converge after SSO
CSCsx34570	—	VSS:remove port-channel from interface causes other members to go down
CSCsx39263	—	TCAM entries are not installed for TCP intercept after SSO
CSCsx46323	—	C2W21: Standby SUP resets due to monitor session on internal PO
CSCsx49071	—	After SSO on Sup4, IPV6 Multicast traffic is not forwarded
CSCsx49326	—	Port-security on TenGig ports doesn't install dynamic mac as secure macs
CSCsx49420	—	HQoS policy attached to main interface cannot set cos to IPv6 traffic.
CSCsx49718	—	Auth Man Single-host-Guest VLAN doesn't trigger reauth on EAPOL start
CSCsx49889	—	SPA-IPSEC-2G-3-ACEI0TCAMFAILE:SpdSpInstall:cannot install Sp TmInsertSp
CSCsx50407	—	show authenticaiton needs to display policies for a session
CSCsx53964	—	Unable to control traffic-class
CSCsx55152	—	Switch does not send TC trap if it is not a root bridge

Identifier	Technology	Description
CSCsx55698	—	auth_mgr: spurious access @ dot1x_rp_auth_client_deleted
CSCsx58097	—	Tracebacks and crash @ lfd_rewrite_mgr_fill_mfi_out_info observed on SSO
CSCsx58488	—	VSL interfaces are not in restricted mode
CSCsx58786	—	Router crash @ routemap_track_nexthop
CSCsx62912	—	W2: update the PM switch vp limits for MST, PVST and Rapid-PVST
CSCsx64668	—	Config change on port of WS-X6148-FE-SFP will move other ports to down
CSCsx64994	—	Memory leaks in ccm processes after redundancy forced switchover
CSCsx65705	—	router crash on no route-map with match ipv6 address access-list
CSCsx76308	—	HA client crashing attempting to free unassigned memory
CSCsx78789	—	Router crash @ flow_sampler_select with traffic
CSCsx78812	—	MLPPP+LFI over ATM : Inconsistent behavior
CSCsx79379	—	IOS Auth Proxy HTTP may lead to bus error adress 0x0
CSCsx82825	—	Shutdown Loopback interfaces in VSS recovery mode
CSCsx83443	—	crypto debug condition leaks messages which lead to high cpu.
CSCsx93160	—	SXI image shut down linecard ports of WS-X6748-GE-TX
CSCsx95302	—	C2W21: %SYS-SP-2-INTSCHED: 'idle' at level 2 -Process= "Port-Security"
CSCsx98446	—	power consumption of act/stb sup720 has inconsistent behavior
CSCsy01275	—	W15:: SYS-2-MALLOCFAIL: Memory allocation message seen after bootup
CSCsy01763	—	15 - 20 packets leek to DST with PACL after SSO
CSCsy03133	—	TestNonDisruptiveLoopback skipped when run as scheduled test
CSCsy03141	—	Copy of CSCsx06578 - to address the original hang problem in Mago
CSCsy08048	—	CF Buffer Pools need to be scaled by platform
CSCsy08838	—	Zamboni allows clear packet inbound on protected interface
CSCsy12800	—	priv-lvl=15 should NOT be required for Local Web-Auth
CSCsy16220	—	a switch may crash due to deadlock between snmp and eem
CSCsy20589	—	Port diagnostic failures following 'redundancy reload shelf' command
CSCsy21797	—	Cat6k-Unexpected SNMP messages occurred
CSCsy22802	—	MPLS VPN broken, vrf connection (permit missing for internal vlan acl)
CSCsy24522	—	Cannot disable " errdisable detect cause dhcp-rate-limit " 12.2(33)SXI
CSCsy24691	—	entPhysicalTable has power-input 3 Sensor for 6kW DC PS1 and not PS2
CSCsy24895	—	Memory leak in ACE HAPI process
CSCsy26526	—	Router is getting crashed at netconf_sessionQs_set_max_message
CSCsy31098	—	reconfigure pim snooping when configure static mrouter port
CSCsy32202	—	6500 IPSEC SPA SSO 'no crypto connect' cmd causes stdby SUP reload
CSCsy34231	—	EZVPN+VRF:Router reloads while unconfigure crypto map with traffic
CSCsy34566	—	Disable VLAN mapping on ME6524, 6148A-GE-TX
CSCsy37175	—	2FE-PA Subintf lost connection after chassis/Flexwan2 reload

Identifier	Technology	Description
CSCsy37390	—	Need to enable earl interrupt after earl initialization is done
CSCsy37652	—	ws-ipsec-3 VSPA crashed in post frag processing
CSCsy38611	—	Mcast traffic blackhole on uplink recvs after reload of RP switch
CSCsy41119	—	C2W2B: Tracebacks observed on RP Console while MIP auto & service config
CSCsy41526	—	PIM msgs duplicated when MPLS configured and IGMP Snooping Off on xface
CSCsy42216	—	VSL Uptime Counter Reset and other Inaccuracies
CSCsy47281	—	vlan distribution is not working in mago
CSCsy48986	—	VSS: reload shelf shouldn't reload remote service module
CSCsy52376	—	Sup crashes after numerous module resets
CSCsy53060	—	0315 ion image tcp.proc crash during bootup caused switch reloaded
CSCsy53336	—	JQL:VSS:VSLcontrol link failure causes VSS unstability and won't recover
CSCsy54365	—	frequent datapath recovery and traffic loss on WS-X6704 with DFC
CSCsy54583	—	TTY data process on DFC leaks memory at prot_tty_malloc_named
CSCsy56389	—	SLCP process is impacted by inserting/extracting modules
CSCsy56433	—	Sh rom intermittently fails to display correct region info for standby
CSCsy58553	—	Linecard reset causes traffic onto frr protected tunnel to be dropped
CSCsy61956	—	Crash in ios-base when running 'show ip route' or 'show bgp' commands
CSCsy62160	—	Vlan state unable to recover after shutdown by mac-limit
CSCsy62753	—	MST configured router crashed after receiving PVST BPDU.
CSCsy66446	—	%BIT-SP-4-OUTOFRANGE ltl_fpoe_defer_notify_with_pri on port-channel flap
CSCsy66794	—	Module Failed SCP dnld observed on ALL WAN CARDS with ISSU.
CSCsy69228	—	Add CLI mls cef tunnel fragment support for non supertycho2
CSCsy69740	—	SXH: Traffic drop on L2 PO after cleared psecurity on rcving L2 ports
CSCsy75971	—	%CWAN_HA-STBY-4-IFCFG_DFLT_LIST_ERROR messages seen on standby
CSCsy76728	—	PfR: Egress BW measured for prefix is incorrect.
CSCsy78851	—	Continous message:C6K_MPLS_LC-SP-3-INVALID_TE_IF_NUMBER with atm bundle
CSCsy78994	—	Memory leak in Service Task
CSCsy81934	—	Non-standard static multicast MAC addresses lose ports after reload
CSCsy82121	—	IGMP Source only not working due to MC_CAP not set
CSCsy83830	—	IOS-RLB crashes while deleting the username sticky
CSCsy85171	—	CDL2 Read Error: Time out
CSCsy86050	—	MAC Move Notifications on VSS between active and down ports
CSCsy86252	—	SP Crash printing "supervisor jamming EOBC. It will be disabled."
CSCsy87619	—	VSS port channel going down when powering down active switch
CSCsy90705	—	GOLD intrusive test after earl reset causes network disruption
CSCsy94866	—	C2W2B: CSM Config sync causes memory leak
CSCsy95520	—	~500msec Pkt loss after transition to HSRP Active on L3 int

Identifier	Technology	Description
CSCsy96102	—	FM-4-MPLS_RSVD_VLAN_ERROR-failed to remove feature when vrf delete
CSCsz01254	—	BIT-SW1_SP-4-OUTOFRANGE Message reported on VSS
CSCsz06187	—	VACL capture for ingress software switched packets
CSCsz09329	—	invalid display for show module command firmware version t_whit21@1.0
CSCsz12369	—	FPD support for SPA-8X1FE-TX-V2 is not enabled
CSCsz19246	—	Crash after 'no dot1x port-control auto'
CSCsz22954	—	Supported WS-X6324-100FX-MM is powered down improperly
CSCsz23448	—	SIP 200 not coming up and Router Crashes after applying card type E3 1 1
CSCsz24554	—	Statndby keeps rebooting.
CSCsz36826	—	6509E fan-tray failed to restore back to HP mode after OIR
CSCsz38798	—	On SSO, Sup engine/DFC module get reset when MET set deleted
CSCsz40969	—	Need to add Me_Kr flow-control status registers back into sierra/whitney
CSCsz44520	—	trunk port in UDLD err-disable when native vlan is shutdown
CSCsz44678	—	Tunnel won't forward traffic across global to vrf
CSCsz48086	—	Default violate-action is missing from 3 color policy
CSCsz52069	—	2nd commit DDTS for CSCsz09329
CSCsz53809	—	Configuring vlan name containing space doesnt work across reload.
CSCsz55834	—	GLBP may provided BIA MAC instead of Virtual MAC for mobile users
CSCsz56229	—	Crashing after receiving an IGMP v2 Leave Message.
CSCsz62046	—	Crash at memcpy after CPUHOG in SNMP ENGINE
CSCsz63359	—	c2w2b:"show mls qos ip" displays vslot interface instead switchid and sl
CSCsz63721	—	high cpu utilization when with 1000 policy and 1000 forced target
CSCsz67334	—	ciscoEnvMonTemperatureStatus trap sent sporadically as NotFunctioning
CSCsz71904	—	VSS switch crashed on pm_assert_fail
CSCsz71970	—	c2w2b: Freed Memory being Accessed by lldp_med_free_local_annex
CSCsz74362	—	Router crash @ af_policer_error_check
CSCsz74896	—	VSS redundancy reload shelf X causes UDLD err-disable
CSCsz75820	—	JQL: VSS hang on SP after RP crashed by software-forced reload
CSCsz83701	—	W2B: SFP-UTP entPhysicalVendorType cevSFP1000BaseSx to zeroDotZero
CSCsz86787	—	IPV6 mcast and IPV4 EMVPN VRF Lite traffic are not forwarded after SSO
CSCsz92137	—	Crash in crypto_destroy_sadb_root() upon unconfiguring tunnel protection
CSCsz96469	—	Tracebacks seen @chunk_free_with_pc while unconfiguring
CSCta06689	—	Rapid PVST:mac address table not flushed after topology change
CSCta10870	—	FPOE takes long time to be programmed on active vss switch
CSCta15415	—	DHCP Snooping functionality is not working fine with private vlan
CSCta22749	—	C2W2b: %CONST_DIAG-SW1_SP-3-BOOTUP_TEST_FAIL:LC powercyled during Multip
CSCta24027	—	See c6k_power_port_mgmt.c:pd_get_sb 98 tracebacks at bootup

Identifier	Technology	Description
CSCta32922	—	SP crash due to heartbeat failure.
CSCta57705	—	C2W2b: reg_invoke_vs_ltl_src_index_changed() needs to be added on stdby.
CSCsr27727	Content	Cat6K experiences a reload after %SYS-2-ASSERTION_FAILED: message
CSCsz36400	Content	WCCP router may become confused with incompatible web-cache config
CSCej05426	Infrastructure	HA AutoSAA issuing no rtr react 100001 forces stby into RPR mode
CSCse25551	Infrastructure	IP SLA Group Schedule association with Individual Probes Forgotten .
CSCsj24186	Infrastructure	%SYS-2-NOBLOCK messages from Pool Manager process
CSCsm66896	Infrastructure	IP SLA Monitor strDupOctet memory leak
CSCso74665	Infrastructure	C7600: Active SUP crashes when attaching to crashed FW
CSCsq73498	Infrastructure	Dovetail: ciscoipc Crash Followed by RPC Timeout with MultiOS IPC
CSCsq74185	Infrastructure	Image verification not possible on 12.2(33)SRC for the c7200
CSCsr02336	Infrastructure	long prompt delay after delete harddisk:core/*
CSCsr08750	Infrastructure	router is crashing after giving the command memory reserve critical 1
CSCsr94474	Infrastructure	Running-config stuck: nv_csb_semaphore locked during copy run ftp
CSCsu53150	Infrastructure	Tracebacks on ISSU RV xdr_mcast_notify_event
CSCsv54929	Infrastructure	Cannot save banner bigger than 2048 characters
CSCsv90106	Infrastructure	nested crash leads to incomplete crashinfo
CSCsw14433	Infrastructure	at UBR10K ISSU RV, ipc_do_delayed_init() sometimes delay 1 sec
CSCsw61555	Infrastructure	Router Crashes after doing SSO
CSCsw96293	Infrastructure	Reload in SNMP Proxy Forwarder after IOS upgrade
CSCsx42732	Infrastructure	IOS64: IP-SLA configuration fails due to memory alloc failure on stby
CSCsx55240	Infrastructure	Router crashes at html_config_command
CSCsy24676	Infrastructure	IFS returns false success on error conditions
CSCsy45455	Infrastructure	get-next request of rttMonJitterStatsEntry table fails
CSCsy55455	Infrastructure	Crash at saaComponentGet
CSCsy61259	Infrastructure	IFS buff cache goes into infinite loop on driver errors
CSCsy78382	Infrastructure	sending non IP traffic causes IOSD crash
CSCsy86078	Infrastructure	Memory corruption Failure
CSCsz19466	Infrastructure	C2W1: int range command with port-channel load-defer cause router crash
CSCsz21732	Infrastructure	Reload in SNMP at snmpProxyFwderSearchReq
CSCsz52815	Infrastructure	Crash when 'history hours-of-statistics-kept' has value greater than 9
CSCed01880	IPServices	Not able to configure NAT tcp timeouts beyond 4194 sec
CSCef58137	IPServices	Router Crash after high CPU, when IPNAT configured with route-map
CSCsa41736	IPServices	Router crash after enable NAT rate-limit feature
CSCse66643	IPServices	SYS-2-NOBLOCK error when redistributing NAT routes
CSCsg31017	IPServices	parser view (role based cli) not applied when access via RSH
CSCsh49973	IPServices	NAT-ALG corrupts offset value of DNS PTR response

Identifier	Technology	Description
CSCsj76907	IPServices	IPv6 UDP sockets may incorrectly show "--any--" for local address
CSCsm42110	IPServices	IGMPv3 - Multicast router ignores IGMP leave when SSM mapping configured
CSCso50205	IPServices	DNS based SSM mapping creates interface throttles when DNS is not avail
CSCsr69932	IPServices	Stale HSRP packets are being processed instead of discarded
CSCsw51864	IPServices	CHUNKFREE error and crash when changing NAT config
CSCsw52416	IPServices	NAT: dynamic nat entries do not timeout in certain case
CSCsx23602	IPServices	crash after 'clear ip nat trans *'
CSCsx33622	IPServices	Fix MSS calcuation issue in TCP
CSCsx34372	IPServices	c2w21/C2W2b:OSPF is not working with udlr/ude
CSCsx58889	IPServices	Call fails under load intermittently with cause 47 no resource avail
CSCsx63640	IPServices	Device gets crash @ tcp_find_conn_info
CSCsx74657	IPServices	Many issues with NAT/Multicast feature
CSCsy26750	IPServices	6k Crash with ipnat_ldap_fixup (Redundancy Checks needed)
CSCsy39623	IPServices	cannot ping local vlan interface ip address with NAT configured
CSCsy39667	IPServices	dhcp-proxy-client incorrectly sends DHCPRELEASE in PPP-agg use-case
CSCsy45371	IPServices	NAT: two static nat entry related issues
CSCsy74796	IPServices	Memory leak at ip_multicast_ctl (when creating/deleting interfaces?)
CSCsy76195	IPServices	standby delay timer does not take correct effect if set to >254 seconds
CSCsy77298	IPServices	[DHCPD] IOS DHCP server does not send back option 82 in DHCPNAK
CSCsy97506	IPServices	All nat'ed multicast packets punted to software
CSCsz12488	IPServices	LDAP add with malformed BER attributes causes CPUHOG and MALLOCFAIL
CSCsz16580	IPServices	[UNI]Active RP's CPU% spikes by MLD process after reload or longevity
CSCsz89107	IPServices	high cpu due to ip_input process during SNMP trap
CSCsx61048	LegacyProtocols	%SYS-3-TIMERNEG: negative offset -Process= "IPX RIP In"
CSCsz71787	LegacyProtocols	Router crash by crafted IP packet.
CSCsw66153	Management	Native vlan not displayed in show cdp neighbor detail
CSCsx30903	Management	parser issues in global config mode
CSCsx46383	Management	No SNMP response on Cat6K for IP-FORWARD-MIB with VRF and SNMP Contexts
CSCsy17342	Management	router reload on removing cns config notify interval
CSCsx74883	MPLS	c2w2b: Standby crash @ vrf_delete_if_ready while unconfiguring vrf inte
CSCsy29604	MPLS	VRF leaking on the same router cause CEF to break
CSCsy60668	MPLS	W1.5:: Toggle "mpls tra router-id" cause router crash
CSCsz11877	MPLS	MPLS-TE Tunnel label re-allocation on mid-point router while RSVP-GR
CSCsz75180	MPLS	Crash due to mpls subintf being removed
CSCsz92368	MPLS	MDEBUG-2-ACCESSFREED: @tc_handle_dead_peers Enabling/disabling "mpls ip"
CSCsx15396	Multicast	Mcast IIF stays up while physical interface is down
CSCsx28948	Multicast	I/O Memory leak on 7200

Identifier	Technology	Description
CSCsx34506	Multicast	RPF failure with no PIM neighbor triggers PIM Hello
CSCsx53084	Multicast	Multiple groups fail with autorp
CSCsx58861	Multicast	Crash due to Stack for iGMP process running low
CSCsy72207	Multicast	multicast rate-limit not applied to new (*,G) entries
CSCsy80910	Multicast	Invalid ICMPv6 packet is sent after transmitting MLD reports
CSCsy96184	Multicast	PIM should not reject assert with all zero source if RPT bit is set
CSCsz48668	Multicast	SYS-2-BADSHARE: Bad refcount in datagram_done
CSCsk04590	PPP	tx cpu crash at blt_pak_holdq_peek on shutdown of a member link
CSCsm93088	PPP	MPPP toward DOM Nortel Active but not traffic crossing
CSCsw20267	PPP	MLP APS across SPA does show in the routing table after failover
CSCee63182	QoS	Router crashes while implementing rate-limit
CSCek42590	QoS	alignment error seen at rsvp_first_object_type & rsvp_next_object
CSCsm97014	QoS	Connectivity breaks for QOS + header compression on virtual templates
CSCsv91699	QoS	"Transmitted pkts/bytes" column showing 0 packets on LSS SIP400
CSCsy26097	QoS	Traceback seen applying Unsupported HFQ Policy
CSCsy28998	QoS	Spurious memory access and tracebacks On Boot
CSCeh66610	Routing	Min hold time from neighbor is not seen in the configuration
CSCsk96581	Routing	BGP sessions fail to establish after int flap due to hold timer expired
CSCsq11897	Routing	Spurious memory seen at idb_get_ip_addrs and idb_get_ip_unnum
CSCsq20928	Routing	CEFv6 dropping IPv6 unicast packets
CSCsq58289	Routing	redistributed connected prefixes not seen as LSA 5 in ospf database.
CSCsr05431	Routing	After SSO, cef removed vrf routes before bgp graceful timers time-out
CSCsr09208	Routing	Memory allocation error of fragmentation when plenty memory available.
CSCsr50704	Routing	dmzlink-bw programs wrong traffic share count in routing table
CSCsr51801	Routing	upon router reload some of the route-maps not permitting the prefixes.
CSCsr72352	Routing	6peinterascrr:Incorrect nexthop advertised between the routereflectors
CSCsr84530	Routing	Static route not properly redistributed into BGP -- backout CSCsl92283
CSCsu11161	Routing	Neighbor x.x.x.x default-originate issues seen in 12.2 code
CSCsu61953	Routing	Labels not getting allocated for BGP prefixes
CSCsu92300	Routing	"sh ip mroute" shows some routes in pruned state
CSCsu96698	Routing	BGP: /32 route being advertised while 'summary-only' is configured
CSCsv73754	Routing	crash during vrf unconfig - bgp_vpn_impq_add_vrfs_cfg_changes
CSCsv91628	Routing	BGP prefixes not exchanged between Route refectors through MP-EBGP
CSCsw29664	Routing	running and startup config out of sync after iprouting.iosproc restart
CSCsw72680	Routing	IP - Packets loop if running Microsoft NLB in presence of PIM
CSCsw73196	Routing	bgp session flap btw GSR and 7600 due to illegal net(MDT grp addr issue)
CSCsw99768	Routing	BGP malformed update sent

Identifier	Technology	Description
CSCsx03301	Routing	Router crashed @ bgp_reset_rcache
CSCsx06457	Routing	BGP may modify routes it does not own
CSCsx08294	Routing	OSPF encounters a bus error crash when running SPF
CSCsx18270	Routing	EIGRP: tags from version 2 peers are not displayed in topology table
CSCsx20177	Routing	"no int loopback" causes stuck prefix in isis level-2 database
CSCsx21482	Routing	Router crashes at ipv6_rip_nvgen_interface when issue wr mem command
CSCsx35205	Routing	Standby ip arp entry is not reinstalled after static arp entry removed
CSCsx39310	Routing	VRRP sends ARP req with Physical MAC if using same virtual IP as int IP
CSCsx47651	Routing	IP LSRR broken with ip unnumbered
CSCsx51299	Routing	Crash when remove and configure ipv6 ACL via telnet and console
CSCsx75004	Routing	BGP CSC-PE advertises wrong out-label.
CSCsx96069	Routing	OSPFv3 maxage LSA remains after Area-ID change
CSCsx98673	Routing	PE not send extended-community to a peer newly added to peer-group
CSCsx99015	Routing	crash if OSPF redistributes another OSPF and interface bw changes
CSCsy15150	Routing	33SXH5: Traceback @ isis_router when default interface configured
CSCsy27394	Routing	Lawful Intercept Tap visible via show ip interface (sub-interface)
CSCsy27511	Routing	4basn: Issue generating update for pfx w/ 255 as# to old speaker
CSCsy28394	Routing	Tracebacks when attaching 62000 loopback interfaces to OSPF
CSCsy29534	Routing	Bus error crash on removing address-familly in router rip config mode
CSCsy32000	Routing	Rtr crash on rcv routes w LinkLocal NH from v6 direct-connected IBGP nbr
CSCsy45838	Routing	show ip ospf border-router crashing router
CSCsy58115	Routing	Continuous BGP mem increase with non established neighbors
CSCsy73123	Routing	Connected route on port-channel subintf not removed when Po is down
CSCsy76404	Routing	Modular IOS: memory leak in CEF background process
CSCsy77842	Routing	TB isis_process_no_router after isis router process deleted
CSCsy84134	Routing	ARP table is flushed when deleting secondary IP address
CSCsy96019	Routing	router reload @ ippkt_check with debug ip packet turned on
CSCsz16724	Routing	BGPv6: default-metric is not being NVGEN'ed and not functionting
CSCsz42043	Routing	OSPF originating orphan TE LSA
CSCsz55293	Routing	wrongly marking IPv4 capability as negotiated, with peer only IPv6 sessi
CSCsz61156	Routing	NH is not stored in BGP table when IPv6 VRF is redistributed
CSCsz78992	Routing	Packet drops when "ip cef accounting per-prefix" configured
CSCsd91182	Security	crypto pki export pkcs12 hangs when used with SCP
CSCsv20285	Security	Whitney:Authentication to the CA server failed using ION.
CSCsv23797	Security	SSH:Crash seen on 7200 on mcp_dev
CSCsv46973	Security	"Change Password" is not properly relyaed
CSCsw50991	Security	Traceback if underlying interface of 6to4 tunnel goes down.

Identifier	Technology	Description
CSCsy16177	Security	scp:copy to router over sshv2 fails with invalid checksum error
CSCsy17893	Security	Ping to itself doesn't work on IPIP tunnels
CSCsy22311	Security	SCP b/w IOS routers fails while the client is receiving file from server
CSCsz40612	Security	GRE keepalive retry behavior is wrong
CSCsi05069	WAN	DCE Sub-interface is not coming up after provisioning
CSCsw31019	WAN	Router crashes while configuring the command "frame-relay be 1"

Caveats Resolved in Release 12.2(33)SXI1

Resolved AAA Caveats

- CSCsv06973—Resolved in 12.2(33)SXI1

  Symptom:

  Router crashes For Authentication RESPONSE with GETUSER and when getuser-header-flags is modified and sent.

  Conditions:

  TACACS single-connection is configured. When authorization is configured Telnet to router and removing authorization,telnet to router again

  Workaround:

  Do not use TACACS single-connection option.

- CSCsv38166—Resolved in 12.2(33)SXI1

  The server side of the Secure Copy (SCP) implementation in Cisco IOS software contains a vulnerability that could allow authenticated users with an attached command-line interface (CLI) view to transfer files to and from a Cisco IOS device that is configured to be an SCP server, regardless of what users are authorized to do, per the CLI view configuration. This vulnerability could allow valid users to retrieve or write to any file on the device's file system, including the device's saved configuration and Cisco IOS image files, even if the CLI view attached to the user does not allow it. This configuration file may include passwords or other sensitive information.

  The Cisco IOS SCP server is an optional service that is disabled by default. CLI views are a fundamental component of the Cisco IOS Role-Based CLI Access feature, which is also disabled by default. Devices that are not specifically configured to enable the Cisco IOS SCP server, or that are configured to use it but do not use role-based CLI access, are not affected by this vulnerability.

  This vulnerability does not apply to the Cisco IOS SCP client feature.

  Cisco has released free software updates that address this vulnerability.

  There are no workarounds available for this vulnerability apart from disabling either the SCP server or the CLI view feature if these services are not required by administrators.

  This advisory is posted at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-scp.

- CSCef52919—Resolved in 12.2(33)SXI1

  Symptoms: A privilege level 1 user is able to log in with a higher privilege level.

Conditions: This symptom is observed on a Cisco platform when the **aaa new-model** command is enabled, when the **privilege level** *level* command is present under the vty lines, and when the *level* argument has any value from 2 through 15.

Workaround: Do not configure privilege level 1 but configure any other privilege level.

- CSCsv73509—Resolved in 12.2(33)SXI1

  Symptoms: When "no aaa new-model" is configured, authentication happens through the local even when tacacs is configured. This happens for the exec users under vty configuration.

  Conditions: Configure "no aaa new-model", configure **login local** under **line vty 0 4** and configure **login tacacs** under **line vty 0 4**.

  Workaround: There is no workaround.

Resolved IPServices Caveats

- CSCsr29468—Resolved in 12.2(33)SXI1

  Cisco IOS Software contains a vulnerability in multiple features that could allow an attacker to cause a denial of service (DoS) condition on the affected device. A sequence of specially crafted TCP packets can cause the vulnerable device to reload.

  Cisco has released free software updates that address this vulnerability.

  Several mitigation strategies are outlined in the workarounds section of this advisory.

  This advisory is posted at
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-tcp

- CSCsv04836—Resolved in 12.2(33)SXI1

  Multiple Cisco products are affected by denial of service (DoS) vulnerabilities that manipulate the state of Transmission Control Protocol (TCP) connections. By manipulating the state of a TCP connection, an attacker could force the TCP connection to remain in a long-lived state, possibly indefinitely. If enough TCP connections are forced into a long-lived or indefinite state, resources on a system under attack may be consumed, preventing new TCP connections from being accepted. In some cases, a system reboot may be necessary to recover normal system operation. To exploit these vulnerabilities, an attacker must be able to complete a TCP three-way handshake with a vulnerable system.

  In addition to these vulnerabilities, Cisco Nexus 5000 devices contain a TCP DoS vulnerability that may result in a system crash. This additional vulnerability was found as a result of testing the TCP state manipulation vulnerabilities.

  Cisco has released free software updates for download from the Cisco website that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

  This advisory is posted at
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090908-tcp24.

- CSCsw18636—Resolved in 12.2(33)SXI1

  Symptoms: High CPU utilization occurs after device receives a ARP packet with protocol type as 0x1000.

  Conditions: This problem occurs on Supervisor 32 running Cisco IOS Release 12.2(33)SXI. This problem may also occur on Supervisor 720. The problem is only seen when you have bridge-group CLI being used, which leads to ARP packets with protocol types as 0x1000 being bridged. The problem does not apply for IP ARP packets.

  Workaround: Filter the ARP packet. The device configuration should have bridge-group creation first, followed by interface-specific bridge-group options.

Resolved LAN Caveats

- CSCsv05934—Resolved in 12.2(33)SXI1

  Summary: Cisco's VTP protocol implementation in some versions of Cisco IOS and CatOS may be vulnerable to a DoS attack via a specially crafted VTP packet sent from the local network segment when operating in either server or client VTP mode. When the device receives the specially crafted VTP packet, the switch may crash (and reload/hang). The crafted packet must be received on a switch interface configured to operate as a trunk port.

  Workarounds: There are no workarounds available for this vulnerability.

  This response is posted at
  http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20081105-vtp

Resolved Multicast Caveats

- CSCso90058—Resolved in 12.2(33)SXI1

  Symptoms: MSFC crashes with Red Zone memory corruption.

  Conditions: This problem is seen when processing an Auto-RP packet and NAT is enabled.

  Workaround: There is no workaround.

- CSCsu79754—Resolved in 12.2(33)SXI1

  Symptoms: PIM packets may be processed on interfaces which PIM is not explicitly configured.

  Conditions: Unknown at this time.

  Workarounds: Create an ACL to drop PIM packets to such interfaces.

Resolved Routing Caveats

- CSCsx10140—Resolved in 12.2(33)SXI1

  Recent research (1) has shown that it is possible to cause BGP sessions to remotely reset by injecting invalid data, specifically AS_CONFED_SEQUENCE data, into the AS4_PATH attribute provided to store 4-byte ASN paths. Since AS4_PATH is an optional transitive attribute, the invalid data will be transited through many intermediate ASes which will not examine the content. For this bug to be triggered, an operator does not have to be actively using 4-byte AS support.

  The root cause of this problem is the Cisco implementation of RFC 4893 (4-byte ASN support) - this RFC states that AS_CONFED_SEQUENCE data in the AS4_PATH attribute is invalid. However, it does not explicitely state what to do if such invalid data is received, so the Cisco implemention of this RFC sends a BGP NOTIFICATION message to the peer and the BGP session is terminated.

  RFC 4893 is in the process of getting updated to avoid this problem, and the fix for this bug implements the proposed change. The proposed change is as follows:

  "To prevent the possible propagation of confederation path segments outside of a confederation, the path segment types AS_CONFED_SEQUENCE and AS_CONFED_SET [RFC5065] are declared invalid for the AS4_PATH attribute. A NEW BGP speaker MUST NOT send these path segment types in the AS4_PATH attribute of an UPDATE message. A NEW BGP speaker that receives these path segment types in the AS4_PATH attribute of an UPDATE message MUST discard these path segments, adjust the relevant attribute fields accordingly, and continue processing the UPDATE message."

  The only affected version of Cisco IOS that supports RFC 4893 is 12.0(32)S12, released in December 2008.

  (1) For more information please visit:

http://www.merit.edu/mail.archives/nanog/msg14345.html

- CSCsx73770—Resolved in 12.2(33)SXI1

  Symptom: A Cisco IOS device that receives a BGP update message and as a result of AS prepending needs to send an update downstream that would have over 255 AS hops will send an invalid formatted update. This update when received by a downstream BGP speaker triggers a NOTIFICATION back to the sender which results in the BGP session being reset.

  Conditions: This problem is seen when a Cisco IOS device receives a BGP update and due to a combination of either inbound, outbound, or both AS prepending it needs to send an update downstream that has more than 255 AS hops.

  Workaround: The workaround is to implement **bgp maxas-limit X** on the device that after prepending would need to send an update with over 255 AS hops. Since IOS limits the route-map prepending value to 10 the most that could be added is 21 AS hops (10 on ingress, 10 on egress, and 1 for normal eBGP AS hop addition). Therefore, a conservative value to configure would be 200 to prevent this condition.

Other Resolved Caveats in Release 12.2(33)SXI1

Identifier	Technology	Description
CSCeg80842	—	PA-MC-8TE1 controller stuck (similar to CSCdz72292)
CSCek70131	—	SIP1 crash at vip_mlp_fastsend with HEARTBEAT error for mlppp qos
CSCek71010	—	TB seen at bgp_oer_notify_pep bgp_oer_remove_path bgp_bestpath_old
CSCek77516	—	PPC:SUP720:4k:SW-EoMPLS:%SW_MGR-SP-3-CM_ERROR_CLASS: Connection Mana
CSCse82480	—	ip vrf receive cmd adds connected routes to VRF even interface down
CSCsf08092	—	Deprecate tracking 'rtr' cmd in favour of 'ip sla' cmd
CSCsg83756	—	SPA-8XCHT1/E1 after Reload C/A LED green even if no cable plugged
CSCsg87290	—	SIP1-ChOC3: Extra path flap is observed on ChOC3 SPA interfaces
CSCsh22225	—	CWAN_HA-STDBY-4-IFCFG_PLAYBACK_ERROR:
CSCsh54232	—	Remove external loop option for nx1GE SPAs
CSCsi66012	—	2 garbage values in show module csm x ft details
CSCsi78584	—	T3/E3 SPA:Line protocol is not comin up with E3 and framing bypass
CSCsj19308	—	PE and CE ping fails over multilink ppp bundle. .
CSCsj80015	—	Enhance logic for accurately detecting Semaphore Hog
CSCsk30196	—	BADBUFFER error at pak_copy_contiguous_to_contiguous
CSCsk98751	—	Router crash after issue command "mpls tra backup-path tunnel"
CSCsl44170	—	LI tapped PPPoE LCP/PPP control packets originated from router are bogus
CSCsl46159	—	Cost Minimization Feature keeps moving the traffic and doesn't stabilize
CSCsl99156	—	No_Global bit out of syn between IPRM and BGP, when label no change
CSCsm01389	—	Crash after clearing Auto-tunnel backup
CSCsm44147	—	SSO failure due to mismatched command on SRB1
CSCsm72121	—	W2: bad cookie magic was detected after SSO switchover with sh vtp count
CSCsm74948	—	mVPN RP does not send join to directed connected neigbor PE

Identifier	Technology	Description
CSCsm75818	—	Wrong OIL for data-mdt mroutes: multicast traffic loss
CSCsm76792	—	PM HA bulk sync posting RF_DONE before bulk sync has finished
CSCsm83256	—	IDSM2 Data port operation status not OK after boot OR SSO
CSCsm96309	—	OIR-SP-4-WARN message displayed when PS1 or FAN removed
CSCso29141	—	DFC installs drop index for MAC-address
CSCso35659	—	L3 traffic rate limited after adding and removing Xcon to a SVI
CSCso36570	—	es20 layer 2 interfaces can be configured with MTU other than jumbomtu
CSCso48665	—	vlan filter can't be removed totally
CSCso51749	—	GRE: policing functionality not working with multicast traffic
CSCso59242	—	sierra: show mem detailed all stat is truncated.
CSCso59974	—	BGP session goes idle after SSO switchover
CSCso88183	—	DOME:dumper.proc crashes on dome when another process crashes
CSCsq07729	—	VSS: flowcontrol incompatible msg when standby switch port add in bundle
CSCsq25028	—	Malloc errors with IPC buffers on a Flex-wan
CSCsq31605	—	auth_mgr:session stuck in Running state if clear auth issued during auth
CSCsq48025	—	DACL is not getting programmed untill next Probe interval.
CSCsq56941	—	6500 - Static MAC cleared from port-channel member ints after reload
CSCsq73122	—	Proxy-ARP returns BIA instead of VMAC with LAM
CSCsq82865	—	Parsing error reading route-map match statements if longer than 254 chrs
CSCsq87496	—	"%OIR-6-INSCARD" syslog not being send from the device
CSCsq96144	—	Netflow v9 Exported Data issue in case of ECMP
CSCsr04190	—	Traceback and standby SUP4 reloads after multiple standby resets
CSCsr09062	—	MLP+QoS - Memory corruption with WRED configured
CSCsr15812	—	Traceback: %SW_MGR-3-CM_ERROR_CLASS: Connection Manager Error: on Congo
CSCsr22282	—	All the trap entries are cleared on any port flap in the same vlan
CSCsr27980	—	%C10K_QOS_GENERAL-3-EREVENT: Error @ ../toaster/c10k_rp/mce_qos.c:mce_qo
CSCsr29559	—	WCCP flap corrupts mcast CEF adjacency
CSCsr37131	—	buginf calls in l2trace when 'debug l2trace' is disabled
CSCsr44036	—	IVFS is not supported, using internal matrix table msgs on router bootup
CSCsr56465	—	With diag Off seeing %CONST_DIAG-SP-3-HM_TEST_FAIL on x6708 LC
CSCsr63098	—	VRF-Aware Smart-Call Home requirement
CSCsr63831	—	show platform hardware capacity fabric - incorrect % and time-SXH3
CSCsr64777	—	EPA crash, Corrupted redzone blk, netflow v5
CSCsr68212	—	MVRF name may get truncated if the VRF name is long
CSCsr88845	—	unicast BootP replies dropped by DHCP snooping
CSCsu01372	—	33SB: Result of boot config command not sync to standby RP after reload
CSCsu04446	—	PfR MC/BR crashes under stress with test traffic

Identifier	Technology	Description
CSCsu05721	—	C2W2: %NTI-SP-3-AGENT_ERR and TB was seen after issu runversion
CSCsu07931	—	cbQosPoliceConformedByte64 counter displays aggregate instead conformed
CSCsu10022	—	L2 traffic is policed when CoPP is enabled
CSCsu10261	—	BFD ISSU peer reload between mcp_dev and sierra image
CSCsu25699	—	OER ICMP Probes using incorrect outbound interface when encrypted
CSCsu36715	—	W2.0 : C2 : ION : Memory Leak in MSDP process
CSCsu36836	—	Conflict when using sockets and files at the same time
CSCsu44534	—	Sup NSF/SSO causes 4 sec traffic loss over EC with uplink ports.
CSCsu45210	—	Upgrade 12.2SXF-> 12.2SXH with Port-Security causes standby boot loop
CSCsu45786	—	Crash on show tcp br after tcp process restart
CSCsu46124	—	SVI ifInMulticastPkts ifOutMulticastPkts are always zero
CSCsu49257	—	Cstn-id timer should be restarted when access-request is seen
CSCsu50611	—	PfR Master Controller crash when shut/no shut
CSCsu67559	—	Copy Run Start does not provide the same functionality as 'wr mem'
CSCsu69660	—	ldcache crashed due to Process Deadlock b/w installer and ldcache proc
CSCsu72026	—	OER MC reports max report limit reach when request all exit links report
CSCsu72496	—	%PM-3-INTERNALERROR: Port Manager Internal Software Error
CSCsu75546	—	C2W21: traffic not span to NAM using span conf mode local-tx source intf
CSCsu77945	—	PfR echo probe shows 0 completes
CSCsu81158	—	Pkt drops on SIP-400 LC due to QoS lock fail for subintfs.
CSCsu81838	—	SA : memory leak @ slb_gtp_echo_response
CSCsu82580	—	6VPE : Traffic dropped under stress configuration with more then 3Kvlan
CSCsu83563	—	MMLS:If rate-lt on when STDBY reloads, doesnt work on swovr:x40/dual RSP
CSCsu84927	—	c2w2:allow DIVC to negotiate red mode when matrix overide check is yes
CSCsu85166	—	Crash @ hwidb_get_firstsw after SSO.
CSCsu86524	—	IKMP process leak: check_ipsec_proposal
CSCsu88008	—	c2w2:standby HSRP router crashed @mcast_igmp_process_join
CSCsu88471	—	Err "Insertion of mld_s_g_type in the grp WAVL tree failed" after SSO
CSCsu88557	—	[no] mdix auto" CLI command not present for WS-X6196-RJ21"
CSCsu90369	—	Whitney2: %XDR-DFC4-6-ISSUBADRCVTFM_DUMP Traceback on Switchover
CSCsu91714	—	IGMP-JOIN is lost from SUP to MSFC
CSCsu92395	—	Crash caused by event manager configuration: "action mail"
CSCsu93936	—	PM_SCP-SP-2-LCP_FW_ERR_INFORM for WS-X6548-GETX-45AF
CSCsu95237	—	SSO switchover,clear packet seen on the wire exposing the inner IP pkt
CSCsu95605	—	Route-map with "match route-type local" not functioning properly
CSCsu95662	—	W2: VSL config got error in mixed type with interface range cmd
CSCsu97020	—	policer on flexwan/multilink is dropping even CIR is not reached

Identifier	Technology	Description
CSCsu97418	—	Standby PRE is resetting when doing "write mem"
CSCsv01136	—	Traffic don't get forwarded after iprouting restart then do SSO with PBR
CSCsv04471	—	CDP 2nd port notification traceback
CSCsv07313	—	SPA timeout observed on reload with scalable access-lists config.
CSCsv07858	—	IfIndex for unconfigured VLAN on 7613
CSCsv09249	—	VSS after dual-active recovery MEC on standby chassis UDLD error disable
CSCsv17989	—	interface in SIP200 show "admin down" when it is physical down
CSCsv18681	—	CLI "sh int transceiver properties switch 1" also display switch 2 ports
CSCsv20339	—	MN history table is flooded with multiple (~500) add/delete entries
CSCsv20920	—	telnet from a GRE tunnel to real address for DNS vserver fails
CSCsv21612	—	High CPU on SP due to PM Callback process with VTP pruning enabled
CSCsv21770	—	PAC re-provisioning fails, AAA generates endless number of Prov Requests
CSCsv22779	—	VRF-PBR: Packets dropped with reflexive acl
CSCsv22913	—	igmp snooping querier disabled when static mrouter port is configured
CSCsv24742	—	PfR exit link is OOP when interface counter wraps
CSCsv28564	—	Policy Base Forwarding marks the packets to cos5 on VSS
CSCsv30307	—	ISSU is broken because of CSCsg52337 commit in SRC
CSCsv30679	—	Sup detetes Vlans from Sup IDSM Config on startup / failover
CSCsv32101	—	QoS: memory corruption traceback when using access-list with time range
CSCsv34159	—	Access control based on EAP, not on Radius type, in conflicting messages
CSCsv36306	—	BFD: Removing BGP on the router makes the neigh router crash
CSCsv36698	—	IPC Open Port Errors observed on 7600-SSC-400/VPN-SPA
CSCsv36892	—	New CLI goto tclsh if previous CLI with tclsh terminated abnormally
CSCsv37543	—	GRE/IPsec misconfig is only resovled through module or chassis reload
CSCsv38928	—	IGMP Snooping does not send out Global query on 2nd TCN < 35 seconds
CSCsv39228	—	VSS-The system didn't display SN of SFP correctly
CSCsv39496	—	TB@rfsc_issu_negotiate_and_open_server_port on RPR upgarde from W1 to W2
CSCsv40523	—	WISM: Gig interfaces show as unknown(4)
CSCsv40770	—	%ICC_ISSU_NEGO-SP-3-OPEN_PORT_RELIABLE: Can't open reliable port
CSCsv40974	—	"wism mod <mod> controller <1
CSCsv43991	—	FWSM's internal portchannel on the cat6k side goes down after upgrading
CSCsv44923	—	MAC move behind phone leads to lost connectivity with MAB
CSCsv52426	—	GRE Recirc index is 0x0 in adjacency hence encap operation fails on DFC
CSCsv52941	—	EEM24: snmp-notif ed policies not triggered after removal and add
CSCsv53392	—	"Mls qos trust device cisco-phone" causes instabilty on the system
CSCsv56974	—	OIR WAN Module w/VPN/SPA interfaces. does not take down Vlan/Tunnels
CSCsv57235	—	duplex is changing automatically on WS-X6148-RJ-45

Identifier	Technology	Description
CSCsv57305	—	VSS: software forced reload with 100Mbps SFPs in supervisor uplink ports
CSCsv58013	—	MLPPP policy-map could not be deleted.
CSCsv58279	—	Reload due to Address Error with multicast configuration
CSCsv60643	—	sup4 when toggled 10g mode the config is not synced to standby sup
CSCsv63799	—	PfR MC/BR bus error crash in ip fast flow
CSCsv64079	—	SXF7: Patching fails with WiSM Card on Cat6500
CSCsv66513	—	PBR controlled application not in DEFAULT with exit interface shutdown.
CSCsv66706	—	IDSM port-channel Allowed-Vlan statements lost on reload
CSCsv66827	—	Clearing the SSH session from a different vty session crashes the box.
CSCsv73299	—	L2 multicast forwarding broken with DHCP snooping & TTL rate-limiter
CSCsv73721	—	ISSU ERP tracebacks on active RP during router bootup
CSCsv76509	—	Cat6k/MSTP in compat mode BPDUs sent in VLAN1 regardless of config
CSCsv80075	—	Pre-release Feature Card VS-F6K-PFC3C (227)
CSCsv86288	—	Sending a hello response with a session-id element causes a crash
CSCsv91278	—	MPLS interface wedged following upgrade to SXI
CSCsv92872	—	10GE link on Sup720-10GE takes more than 30sec to go down during crash
CSCsw17478	—	PVT HOSTS- ports programmed with incorrect rdt index upon bootup
CSCsw18793	—	VRF-PBR: TCAM adjacency not programmed with multiset policy order after
CSCsw32280	—	Diag error on WS-X6148A-45AF card asic with Traffic
CSCsw41168	—	%ALIGN-3-SPURIOUS at sm_get_portEntPhyIndex
CSCsw41439	—	W21,VSL,SNMP,cvsCoreSwitchPreempt,cvsCoreSwitchPriority not SSO aware.
CSCsw41706	—	router reload when registering EEM service diag script
CSCsw43953	—	Card not identified SIP Is OIR'd during Standby SUP bootup
CSCsw45396	—	when STP recovered in uplinkfast,no sent dummy multicast packets
CSCsw48181	—	Unknown Unicast is dropped on Shut/no Shut of a VLAN
CSCsw48824	—	Switchport Block Unicast - prevents RTP on same VLAN
CSCsw51395	—	Proper handling is required for Mac-Filter with Port-security
CSCsw52819	—	Kernel dumper needs a few enhancements.
CSCsw53362	—	c2w2b: Device crashes with NAT stress test
CSCsw73302	—	memory leak in qm_increment_ag_policer_usage on standby-rp
CSCsw75589	—	ip flow-cache mpls label-positions can lead to bus error under load
CSCsw78806	—	Router getting crashed at lat_int_command
CSCsw82732	—	VPN-SPA internal vlan interface wedged in SXH4
CSCsw87352	—	6748's port can not forwarding traffic - port src index wrong
CSCsw87399	—	auth_mgr: crash @ eap_show_context when doing show eap session
CSCsw87563	—	packets with multicast mac and unicast ip are software routed by cat6500
CSCsw90798	—	Bus error crash after configuring vlan name change

Identifier	Technology	Description
CSCsw93969	—	%ICC_ISSU_NEGO-SP-3-OPEN_PORT_RELIABLE: Can't open reliable port
CSCsw98231	—	SDBY stuck @ CEF RRP RF Client(5025) after ISSU RV
CSCsx06578	—	SIERRA:MAGO switch got crashed after reload with SIERRA_INTEG_090106
CSCsx09273	—	WEBAUTH(IP adm) is not INITiating if IPDT entry already exists.
CSCsx10011	—	VSS: IO memory leak from pre_process_vsibc_vsda_pak
CSCsx15038	—	NVgen issue with violate-action commands under policy-map class
CSCsx15138	—	Crash at qos_feature_get_fo
CSCsx16206	—	Traffic loss issue from SFM capable modules to other device through DEC
CSCsx26114	—	IOS tagging certain commands as level 1 in config mode
CSCsx28532	—	VPN SPA freezes when ip mtu changed on tunnel interface
CSCsx29645	—	IPv6 Multicast traffic can not converge after SSO
CSCsx32416	—	BFD session flaps during router/LC bootup after reload
CSCsx34570	—	VSS:remove port-channel from interface causes other members to go down
CSCsx37615	—	VSS: rem comm standby-rp sh plat hardware capacity may reset switch
CSCsx48991	—	Disable LI CLI
CSCsx49718	—	Auth Man Single-host-Guest VLAN doesn't trigger reauth on EAPOL start
CSCsx53257	—	Minor diag error - TestNetflowShortcut failed
CSCsx55543	—	auth_mgr: with vlan assignment reauthentication takes 30sec to start
CSCsx58786	—	Router crash @ routemap_track_nexthop
CSCsx62912	—	W2: update the PM switch vp limits for MST, PVST and Rapid-PVST
CSCsx64668	—	Config change on port of WS-X6148-FE-SFP will move other ports to down
CSCsx76308	—	HA client crashing attempting to free unassigned memory
CSCsy03141	—	Copy of CSCsx06578 - to address the original hang problem in Mago
CSCsc78999	AAA	Address Error exception at TPLUS
CSCsk40765	AAA	crash due to AAA/TACACS+ server-private re-configuration
CSCsq37815	AAA	Case sensitive Username authentication is passed with wrong user name
CSCsq94524	AAA	"aaa accounting update newinfo" causes extra "jitter maximum 0" option
CSCsr70963	AAA	Crash when remove DEAD radius server from config
CSCsv02117	AAA	session flapping cause %IDMGR-3-INVALID_ID: bad id in id_get (Out of IDs
CSCsw17553	AAA	Radius-server pac keyword is not nvgened when used with automated tester
CSCsw19816	AAA	cat6000: IOS login enhancments not creating logs for telnet with AAA
CSCek78237	ATM	High CPU on ATM PA Helper process on PA-A3-T3
CSCso64050	ATM	HA functionality is not working when policy attached to atm pvc
CSCsr86103	ATM	ATMoMPLS: Traffic stops flowing on applying service-policy on atm pvc
CSCsr27727	Content	Cat6K experiences a reload after %SYS-2-ASSERTION_FAILED: message
CSCsx40747	Content	Router hangs while doing ip casa configurations
CSCef82896	Infrastructure	When removing the user name from auth dialog, http crashes

Identifier	Technology	Description
CSCin79116	Infrastructure	show memory summary could push the CPU util to 100%
CSCsc77704	Infrastructure	region_find_by_addr goes into infinite loop when spurious memory occurs.
CSCsc86307	Infrastructure	c3845 crashed @ show_systat
CSCse41523	Infrastructure	bootldr config caused stbyPRE reset if file does not exist on stby-bootf
CSCse49151	Infrastructure	3800 clock slip over times verified in lab
CSCsh85011	Infrastructure	DSGS7: Router crash at saaEnhancedHistoryFreeTab
CSCsj46707	Infrastructure	ubr7200 G1 hangs during bootup
CSCsj57479	Infrastructure	Traceback found at data_inconsistency_error_with_original_ra
CSCsj87744	Infrastructure	Parser mode change issues
CSCsk80396	Infrastructure	Inconsistant router Crash seen when jitter operation takes place
CSCsl61281	Infrastructure	Show logging command should be a privileged command
CSCsm33221	Infrastructure	IP SLA Probe type DHCP with no relay-agent IP add. on Dhcp disc. packet
CSCsm54810	Infrastructure	router stops producing the auth-proxy login page intermittently
CSCso21611	Infrastructure	Crash at internal idb counter increment function
CSCsq73498	Infrastructure	Dovetail: ciscoipc Crash Followed by RPC Timeout with MultiOS IPC
CSCsr07557	Infrastructure	Memory leak in parser_chunk_malloc after get/set on Auth Framework obj
CSCsr50834	Infrastructure	CPU HOG after changing logging buffered up to 50MB
CSCsr60789	Infrastructure	W1.3: VSL crash after preemptive switchover in ifs_open_file_decrement
CSCsu57889	Infrastructure	banner exec CLI ignoring lines starting with #, !, and ;
CSCsu78906	Infrastructure	Wrong "%SYS-5-CONFIG_I: Configured from x.x.x.x by snmp" messages
CSCsv34988	Infrastructure	Console/Telnet/SSH login banner not properly formated after upgrade
CSCsv50606	Infrastructure	SNMP: ISSU incompatibility with message type 20
CSCsv80900	Infrastructure	W21:: EARL-SPSTBY-2-SWITCH_BUS_IDLE & PF_ASIC-SPSTBY-3-ASIC_DUMP @boot
CSCsv86766	Infrastructure	Signature fail while copy, causing system:/running-config to be deleted
CSCsw15188	Infrastructure	Router crashes with "debug isdn q931" enabled
CSCsw16658	Infrastructure	Unavailable ipv6 ACL prevent configuring ipv4 ACL
CSCsw35917	Infrastructure	SP syslog messages not sent as SNMP traps by RP's SNMP agent
CSCsw51126	Infrastructure	High CPU on Virtual Exec process after vty session timeout exec setup
CSCsw61555	Infrastructure	Router Crashes after doing SSO
CSCsw76894	Infrastructure	Problems faced with ipv6 SNMP when ipv4 address is not configured
CSCsx32841	Infrastructure	ceImageDescription may exceed 255 characters
CSCek10384	IPServices	7200 NAT dropping Out to In ESP Packets
CSCsl11712	IPServices	Router crashes when DGVPN is configured with VRF . .
CSCsm89795	IPServices	Orbitty repeatedly Crashes - Succeptible to Denial of service attacks
CSCso39062	IPServices	C2W2: %SYS-3-INVMEMINT: Invalid memory action message & TB's with PAT.
CSCso54027	IPServices	Spurious memory access in ttcp_rcv_stats
CSCsq14311	IPServices	7200 crash - ipnat_unlock_parent_entry (PPTP)

Identifier	Technology	Description
CSCsq22397	IPServices	DLSw peer connection initiated from interface IP and not local-peer IP
CSCsq81365	IPServices	MFI: UDP forwarded-protocols from VRF are leaked into global table
CSCsu38774	IPServices	FTP'ing a file from a router will fail if the FTP account cannot delete
CSCsu64215	IPServices	ip tcp adjust-mss command results in packet loss for non-TCP traffic
CSCsu67461	IPServices	Router crashes when "show track brief" entered
CSCsu72176	IPServices	Crash:Process Deadlock in Standby while reloading UUT with DHCP configs
CSCsu74400	IPServices	File descriptor leak with FTP of a DHCP database
CSCsu77597	IPServices	Frames with virtual MAC dest address are dropped with bridging enabled
CSCsu95319	IPServices	IGMP report was not sent to helper address.
CSCsv12265	IPServices	HSRP stuck in INIT when learning and if address changed
CSCsv16987	IPServices	nat pool size more than 16 bit long should not be configured
CSCsv27480	IPServices	VRRP MAC aging out due to being stored as dynamic entry after reload
CSCsv54324	IPServices	HSRP stuck in INIT state after a reload on a c3845 gig-eth interface
CSCsv54510	IPServices	Router is not getting pruned after shutting the interface
CSCsv56160	IPServices	BGP session flap due to TCP selective-ack
CSCsv86201	IPServices	Modular IOS : max sockets overflow
CSCsv99443	IPServices	standby delay reload doesn't work on SUP/RSP720
CSCsw16698	IPServices	DHCP database could not be locked DHCPD process could not lock semaphore
CSCsw64000	IPServices	3800: Ethernet controller wrongly programmed when using DHCP and PIM
CSCsw66082	IPServices	Router crash seen at ip_mcast_address_lookup in ssm-map router
CSCsw73391	IPServices	ip igmp limit gets stuck
CSCsw96272	IPServices	nat overload command not translating packets
CSCsx09343	IPServices	Name resolution triggers pager in non-interactive mode.
CSCsx32283	IPServices	Malformed L field in LDAP crashes 6k with NAT
CSCsr04069	LAN	ifOutOctets for vlan subint with GTS/ratelimit is inaccurate
CSCsw81485	LegacyProtocols	Unconfiguring IPX crashes the switch
CSCsb84797	Management	ATM or FR main interface resets when disabling CDP or deleting subint
CSCse29570	Management	router crashes when pulling config from CNS containing no config initial
CSCso35250	Management	unexpected reload while communicating with CNS server
CSCsu10229	Management	The cdpCacheAddress mib not providing GLOBAL_UNICAST Address
CSCsv48296	Management	cns image retrieve command is forcing to router crash
CSCsv93351	Management	CNS ID Change unexpectedly
CSCsq49176	MPLS	7200 Bus error crash on invalid address, charlotte_post_coalesce_rx
CSCsr15969	MPLS	MPLS TE: extended tunnel id may not be 0.0.0.0
CSCsu50374	MPLS	FRR tunnels doesn't go down if TE flooding is disabled on the headend.
CSCsv00773	MPLS	Loose Path Reopt not applied when link costs changed
CSCsv13738	MPLS	slow convergence when use vrf definition instead of ip vrf

Identifier	Technology	Description
CSCsv31126	MPLS	snmpwalk of mplsTunnelTable may not show all MPLS TE Tunnels
CSCsv41456	MPLS	Tracebacks seen at IFMGR-3-DUP_IFINDEXifDescr"Virtual-Access2-mpls layer
CSCsv62004	MPLS	standby crashes with ipbase image and VRF config
CSCsw35638	MPLS	FRR Interoperability issue between Juniper PLR and IOS MP
CSCsw82028	MPLS	BGP graceful restart is not supported on IP service image
CSCsb77148	Multicast	sh ip mpacket x.x.x.x quality output is wrong after counter wraps around
CSCsc52732	Multicast	Enabling PIM on sub-IF causes mcast packet drops on other sub-IF
CSCsl32142	Multicast	crash from memory corruption from malformed auto-rp Multicast
CSCsl52213	Multicast	PIM assert timer mechanism problem
CSCsu86494	Multicast	Assert flag is not cleared after PIM neighbor loss
CSCsv29659	Multicast	RP configured inside the nat not shown on uut outside the nat
CSCsw29463	Multicast	The adjacency/oce lookup should not be done in mcast fast switching path
CSCsw36940	Multicast	Router crashed at "mrm_manager_sender_commands"
CSCsx15396	Multicast	Mcast IIF stays up while physical interface is down
CSCsf07760	PPP	MLP: Crashes/buffer leaks when large number of sessions come up at once
CSCsr81271	PPP	Invalid VCD error messages upon PVC flap
CSCsu70011	PPP	ipv6 static route pointing to multilink (flexwan) dissapears after sso
CSCsh39945	QoS	PRE3:Router crash with 'show int random' with 40k+ pppoeovlan sessions
CSCsh57935	QoS	%RSVP-3-BAD_RSVP_MSG_RCVD_AUTH_WIN after shut/no shut
CSCsl94263	QoS	Router crash at stile_update_fast_flag due to random-detect dscp-base
CSCsm28515	QoS	Marking not happening on FlexWAN interface with SXH after oir/reload
CSCso97991	QoS	policy with bc value less than default(4ms) will cause drops on WAN int
CSCsq55678	QoS	c2w2: Policy on control-plane is not working with acl log option
CSCsr05501	QoS	% NBAR Error: hwidb could not found shows up when reload
CSCsv12372	QoS	Spurious memory access @ fr_oqueue
CSCsv85791	QoS	Flexwan+/PA-MC-2T3+ introduce 5+ seconds delay on egress
CSCsv91699	QoS	"Transmitted pkts/bytes" column showing 0 packets on LSS SIP400
CSCsw36285	QoS	Incorrect Police rate under calss-default
CSCee30355	Routing	Memory leak at ip_multicast_ctl
CSCef65457	Routing	EIGRP and RIP advertise null0 static routes after they are removed
CSCef67010	Routing	NHRP registrations shouldn't do a routing table lookup
CSCsb15164	Routing	Security holes while configuring a standard ACE with host address
CSCsc98813	Routing	Set metric in route-map effects other RIP routes hop count
CSCsd25753	Routing	BGP Aggregated supernet routes not Advertised properly
CSCse45978	Routing	BGP to RIP redistribution breaks as RIP nexthop moves to alternate path
CSCse68877	Routing	CEF/BGP table MPLS label mismatch YW3 Non Multi-path
CSCsh54161	Routing	dune, Nov image goes unstable - creates eigrp routing loops

Identifier	Technology	Description
CSCsj42399	Routing	Redistributed static covered by network statement sets metric to 0
CSCsk87526	Routing	T/B ipv6_rib_process_changeQ after shut cmd applied Int. running RIPng
CSCsm63632	Routing	Continuous XDR IPC errors (inability to create an IPC buffer)/Watermark
CSCso56038	Routing	%DUAL-3-INTERNAL traceback at igrp2_packet_community_add_item
CSCso90107	Routing	SNMP: bgpPeertable and cbgpPeertable shows only results for ipv4 peers
CSCsq36206	Routing	MDT tunnels not getting created on 7206 Device
CSCsr01403	Routing	cefswitching2.1:More time taken(12 mts) to converge after Adjacency flap
CSCsr21670	Routing	elected more routes than expected routes as multipath
CSCsr40997	Routing	IPv6 RIP: Unconfiguring RIP from an interface doesn't update RIB on peer
CSCsr67361	Routing	I/O memory leaks when BGP neighbor points to a local address
CSCsr88705	Routing	BGP route getting lost after "shut/no shut" of BGP peering interface
CSCsu01272	Routing	MPLS PE 7600 changes RT when a BGP soft clear is executed
CSCsu05464	Routing	System out of mem on SSO switchover with more than 32K ipv6 ref-acl flow
CSCsu06447	Routing	EIGRP:static route redistribution not working with distribution-list
CSCsu08935	Routing	bgp as-override on 2 byte PE does not overwrite AS 23456 properly
CSCsu32217	Routing	Redistribution from BGP to OSPF vrf fails for high metric prefixes
CSCsu39689	Routing	crash @ipv6_nd_prefix_delete_by_handle with rip 6pe_scaling_performance
CSCsu42077	Routing	next entries didnot function after added new entry on ACL
CSCsu53624	Routing	bgp multicast shows unicast information in show ipv6 protocol
CSCsu62356	Routing	RIPNG 'last gasp' message not seen on Interface down in some IOS branch
CSCsu63996	Routing	OSPF flaps after SSO switchover causes traffic loss after SSO switchover
CSCsu69767	Routing	Global to VRF and VPN import route-map depends on configuration order
CSCsu76993	Routing	EIGRP:Routes not tagged with match source redistribution-source
CSCsu79988	Routing	4BASN: BGP path/bestpath memory usage is 14% higher
CSCsu86338	Routing	<cr> missing in ip extcommunity-list command
CSCsu97177	Routing	switch crashes querying (old) IPv6 MIB
CSCsu97834	Routing	On module reset, 'ip route' statement loses 'name' argument
CSCsv00604	Routing	IPv6 host with static default route still learns ND default router
CSCsv01474	Routing	'ip rip advertise' command lost after interface flap/clear ip route
CSCsv05009	Routing	%OSPF-4-FLOOD_WAR: error during heavy flaps for type-5 and type-7 LSAs
CSCsv17933	Routing	Static route in VRF is not redistributed by RIP after link flap
CSCsv27607	Routing	BGP: Outbound route-map updating withdraw only one member
CSCsv51298	Routing	c3825 faces chunk memory leak @ bgp_do_ipv4redist_callback
CSCsv59334	Routing	Connected nets redistr from eigrpTObgp when no net 0 is set under eigrp
CSCsv62777	Routing	High CPU process caused by stucked VTY line
CSCsv85052	Routing	Crash observed when "ispf" is issued in vty with ip routing disabled
CSCsv89643	Routing	OSPF: MAC address of next hop unresolved on ptp eth by adjacency bringup

Identifier	Technology	Description
CSCsv97472	Routing	CSCso62166_dcq_issue_rn_walktree_timed_locking is changed
CSCsw24286	Routing	TE tunnel bandwidth command breaks isis topology
CSCsw24611	Routing	Router crashes at bgp_set_path_attr
CSCsw24826	Routing	OSPF crash during type-9 maxage
CSCsw30941	Routing	ospfNbrStateChange trap sent by non-DR
CSCsw65441	Routing	ARP packets drops due to excessive ARP requests sourced from SVI
CSCsw65933	Routing	Prefix not learned from PE to CE
CSCsw79397	Routing	Device crashing at bgp_command_af_specific
CSCsw89080	Routing	changed L1 area address not updated in L2 lsp with multi-area config
CSCsw92379	Routing	Crash seen on releasing snooping bindings after LC OIR
CSCsx11776	Routing	show ip bgp version 1 causes router crash
CSCsx15841	Routing	aggregate-address does not NVGEN upon switchover on cat6k
CSCsx17446	Routing	Tunnel route and a non-tunnel (IGP) route with same metric (TE metric)
CSCsx18270	Routing	EIGRP: tags from version 2 peers are not displayed in topology table
CSCea11368	Security	CRL fetch using ldap fails if vrf configured in trustpoint
CSCeg49153	Security	PKI: crl checking takes too long to timeout if the server is down
CSCeh75136	Security	TACACS+ rem_addr field empty after first SSH authen attempt fails
CSCsc91824	Security	SSH from router disconnects vty session if there is no matching cipher
CSCse80892	Security	isakmp-profiles and VRFs: IPSEC sa fails to come up for the below config
CSCsk22496	Security	Router crashes @ssh_command when remoove crypto key
CSCsm70719	Security	Memory allocated @ add_new_cdp_to_list Leaked
CSCsq51052	Security	SSH server on IOS reporting bogus protocol version
CSCsu54801	Security	Cannot get s/w adjacency header information on DFC for IPv6 in v6 tunnel
CSCsu90280	Security	NHRP IPv6 registration not working
CSCsv86113	Security	On modular IOS, SSH on VRF int is allowed irrespective of vrf-also key
CSCsv04674	VPDN	Random Vector AVP in ICCN isn't marked as Mandatory
CSCsv04733	VPDN	A LAC might diconnect a tunnel by StopCCN for tunnel-passwords > 31 char
CSCsv68584	VPDN	LAC crashed @sw_mgr_cm_inQ_handler/free
CSCsw78939	VPDN	PDSN(LAC) fails to bring up the VPDN calls after stressing for long time
CSCso62193	WAN	Standby resets due to parser return error "no frame-relay vc-bundle"
CSCsq47900	WAN	OIR operation on POS interfaces with APS result in ALIGN error