Caveats

Caveats in Release 12.2(33)SXJ and Rebuilds

Caveats Open in Release 12.2(33)SXJ and Rebuilds

Identifier	Component	Description
CSCsx31739	bgp	Outbound policy changes does not reflect by itself in MTR Code base
CSCsy27228	bgp	Eagle_cnh: Match statement fail to match prefixes
CSCsz28538	c3pl	SPA Timeout for All SPA's on Boot-up.
CSCtn39432	c6k-es40	SVI EoMPLS and VPLS not working on ES40
CSCta03464	c6k-sip-400	VPLS VC hardware entry lost upon reroute and TE FRR tunnel shutdown
CSCtq20866	c6k-wan-common	Memory leak observed @ c6k_atom_msg on sp after removing xconnect
CSCtz22632	c6k-wan-common	sxj3: Logs are seen when interface is suppressed
CSCtq64944	cat6000-acl	c2wa1b: TCAM not program'd when new DHCP address received
CSCtz17231	cat6000-acl	Bulk-sync failure due to PRC mismatch when ACL is config with portgroup
CSCsz70263	cat6000-cfm	CFM on ISL links isn't working correctly.
CSCtt36279	cat6000-diag	NAM-3: CONST_DIAG-SW2_SPSTBY-3-HM_TEST_FAIL during OIR
CSCtu01395	cat6000-diag	c2wa1c: ASA in switch 2 resets twice on OIR
CSCtq56225	cat6000-dot1x	Multiple Authorized types seen for dot1x supplicants
CSCsy24099	cat6000-ha	get platform-provided x-matrix table on RP
CSCtl42874	cat6000-l2-ec	C2WA1 : mLACP : "mlacp min-link" errdisable upon backbone intf fail/recv
CSCtu92977	cat6000-l2-ec	LACP Po is retaining hash algorithm command even after removal of PO
CSCsm59426	cat6000-l2-infra	UDE/UDLR: OSPF neighbourship is not getting formed with UDE/UDLR link
CSCtq06060	cat6000-lacp	LACP config re-appeares after PO detele/recreate sequence

Identifier	Component	Description
CSCsx08647	cat6000-ltl	Traceback at bitlist_validbit within vs_ltl_mgr_proc
CSCsu66341	cat6000-mcast	W2: 'MLS MSC' ISSU client needs error buginf, for incompatible case
CSCtj66981	cat6000-mcast	MET2 is not programmed for new SR translation rules added in ISSU RV
CSCsu68054	cat6000-netflow	Cat6k Platform changes required for BGP 4-bytes AS Numbering
CSCsx76244	cat6000-portsecur	Sup720-Standby continuously reboots on psec mac-move violation with prot
CSCsv53086	cat6000-routing	ipv6 traffic route-cache switched at ipv6ip tunnel (over mpls)c tail end
CSCsw70162	cat6000-span	C2W21: Span port capture duplicated port-channel packets after SSO
CSCtl82303	cat6000-svc	c2wa1: Stdby switch crashes @l2_maclimit_update_src_index_change
CSCtq28029	cat6000-svc	VSS: hw-mod mod <ASASM mod#> reset doesn't work Gives invalid error
CSCtr30113	cat6000-svc	Standby reloads and never comes up after SSO in the VSS with fwsm
CSCts84327	cat6000-svc	IDSM/NAM will not come up when power off followed by power on
CSCtt28763	cat6000-svc	NAM-3: command hw-module reset doesn't work at certain condition
CSCtu00733	cat6000-svc	NAM3 got pwrDown by hw-module module reset cmd
CSCsw50021	cat6k-vs-proto	After SSO, FIBIDBINCONS1: An internal software error occurred
CSCtn76064	debug	ACE 30 and ACE 20 reboots in SSO redundency
CSCtb95854	ha-ifindex-sync	%IDBINDEX_SYNC-4-RESERVE: Failed to lookup existing ifindex, on LV & RV
CSCte71854	itasca-scp	ACE 30 and ACE 20 reboots in SSO redundency
CSCtz12715	nat	TB while deleting Static nat entry which has interface as global address
CSCty94040	nat-pat	Nat46 traffic through Arsenal ASA does not flow without ipv6 SVI
CSCsr93564	pem	AUTHZ success with wrong DACL entry.
CSCsy47965	pem	FID:for non existent fid ACL on the switch, authz is success
CSCts05237	pem	"sh epm sess inter <x/y>" dispplays all existing epm sessions
CSCty32463	pki	Kingpin & 1RU Unable to sync in SSO mode w/ 'crypto pki' configuration.
CSCtz20394	socket	Invalid TCB pointer TBs seen on NAM process upon clearing tcp sessions
CSCsz29842	tcp	%TCP-2-INVALIDTCB: Invalid TCB pointer: 0x9BFAC6C0 -Process="RSMP Server
CSCtn12371	vpn-sm	SPA-IPSEC-2GE: XDR-6-XDRLCDISABLEREQUEST / Traceback
CSCtn77107	wlc-kernel	WiSM-2 Data port Down on VSS after multiple SSO or stdby switch reset
CSCts96124	wlc-os	Sessioning to Jian not happening after changing service vlan subnet

Caveats Resolved in Release 12.2(33)SXJ6

Resolved dhcp Caveats

- CSCug31561—Resolved in 12.2(33)SXJ6

  A vulnerability in the DHCP implementation of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

  The vulnerability occurs during the parsing of crafted DHCP packets. An attacker could exploit this vulnerability by sending crafted DHCP packets to an affected device that has the DHCP server or DHCP relay feature enabled. An exploit could allow the attacker to cause a reload of an affected device.

Cisco has released free software updates that address this vulnerability. There are no workarounds to this vulnerability.

This advisory is available at the following link:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130925-dhcp

Note: The September 25, 2013, Cisco IOS Software Security Advisory bundled publication includes eight 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 September 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_sep13.html

Resolved gsr-boot Caveats

- CSCsv74508—Resolved in 12.2(33)SXJ6

  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 ios-authproxy Caveats

- CSCtz99447—Resolved in 12.2(33)SXJ6

  Symptom: Local webauth and HTTP services stop responding on the switch.

  Conditions: A **show processes | inc HTTP Proxy** lists many instances of the "HTTP Proxy" service, and these do not disappear.

  Workaround: The HTTP Proxy service may experience delay due to an incorrectly terminated HTTP or TCP session. In some cases, increasing the value of **ip admission max-login-attempts** works around this issue. In others, the stuck "HTTP Proxy" service will again become available after a TCP timeout.

  Some browsers and background processes using HTTP transport can create incorrectly terminated HTTP/TCP sessions. If webauth clients are under control, changing web browsers or eliminating background processes that use HTTP transport may eliminate triggers for this issue.

  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 5/4.1:
  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:OF/RC:C

  CVE ID CVE-2012-4658 has been assigned to document this issue.

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

Resolved ospf Caveats

- CSCug34485—Resolved in 12.2(33)SXJ6

  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/en/US/products/products_security_vulnerability_policy.html

Other Caveats Resolved in Release 12.2(33)SXJ6

Identifier	Component	Description
CSCub04965	aaa	TCP Session hung causing Packet loss
CSCug62154	aaa	Mk1: High CPU 100% due to TPLUS with tacacs config
CSCuh43252	aaa	unable to login and high cpu when authenticating with TACACS
CSCsl04415	bgp	1000 ipv6 ebgp sessions does not come up on 6vpe , only 300 come up
CSCud08574	c6k-crypto	Vlan Interface over Serial - IPCP nego and Vlan link-up race condition
CSCsu63884	c7600-netflow	7600 netflow: workaround to scale RP sampled flow export per PD ratio
CSCug23641	cat6000-acl	FM missing dot1x feature for interface; IPDT entries & dACLs failing.
CSCub23671	cat6000-dot1x	Authentication loop in dot1x->mab->guest vlan for supplicantless PC
CSCub60449	cat6000-dot1x	Switch starts second authentication after port in guest vlan
CSCud22789	cat6000-dot1x	IGMP joins when port is in auth-fail state not forward to mrouter
CSCue31621	cat6000-dot1x	MAB fails after 6500 reload when port configured for critical voice vlan
CSCug45224	cat6000-dot1x	dot1x auth restart for the host in guest vlan when traffic is sent.
CSCue02511	cat6000-fabric	VSS FPOE incorrect on standby
CSCue53095	cat6000-firmware	ISSU fails between SXI and SXJ on Sup32/S720-10G for certain versions

Identifier	Component	Description
CSCua87594	cat6000-l2	cat6k:Spanning Tree interop between MST0 & RSTP takes 6 secs to converge
CSCug90305	cat6000-l2	Power deny of 6148-ge-tx-AF/AT interface with 2602 factory reset
CSCtu01035	cat6000-l2-infra	OIR heathland module on newly active during standby bootup crash both
CSCuf36123	cat6000-l2-infra	VSS Standby crash after renaming vlan
CSCtw49851	cat6000-mcast	show ipv6 mld snooping explicit-tracking cli o/p changed
CSCue52637	cat6000-mcast	Multicast traffic blackholed after deleting a vlan
CSCuh41546	cat6000-qos	Standby is getting crashed after ISSU Runversion
CSCud18108	cat6000-snmp	CAT6500 SNMP timeouts polling dot1dTpFdbTable
CSCue03531	cat6000-snmp	6500-Transceiver/SFP SNMP polling interrupted when changing port config
CSCua01409	cat6000-svc	C4Ma2:TB and Standby reload on adding & removing fwsm config
CSCtg57657	dhcp	Router crash at dhcp function
CSCub75883	ip-acl	Access-line numbers are NOT persistant after reload
CSCui17285	ip-acl	ip access-list persistent keyword not available in SXJ6 image
CSCee38267	nat	NAT router may reload under heavy load of NAT traffic
CSCtx95334	nat	TCAM entries are not correctly programmed for static nat w/ interface
CSCue21223	nat	Intermitant HSRP hellos not sent w/ IP NAT redundancy configured on SVI
CSCsc97279	nvram	Takes long time (more than 2 minutes) on wr mem
CSCud65003	parser	router crash during config of priv level exec commands
CSCsw43080	rsr-bridging	Traceback seen @ data_inconsistency_error_with_original_ra
CSCtd45679	sla	Removing ip sla probe (configured by SNMP) in CLI reloads Standby Sup
CSCue80816	snmp	Crash while routine config push through SNMP
CSCsd72758	ssh	Scheduler Thrashing in the SSH Process
CSCud79481	udp	Crash on 6500 on executing "show ip helper address"

Caveats Resolved in Release 12.2(33)SXJ5

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)SXJ5

  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)SXJ5

Identifier	Technology	Description
CSCtg48829	—	Memory leak at set_dst_card_ports+
CSCth11657	—	switch reboots during taking core file with standby sup. Simplex ok
CSCtx50235	—	SP and RP mutually resetting each other hides the actual crash reason
CSCty15494	—	Memory leak in cfib_fibsb_chunk
CSCtz36880	—	SXJ3: ACE30 IPv6 RHI throws TB
CSCtz52826	—	SXJ1 VSS crash on redundancy force-switchover
CSCua08468	—	SG Entries installed as Partial-SCs and do not switch to Data MDT
CSCua43298	—	Port loopback mode may not be cleared in corner case
CSCub07847	—	High CPU seen on receiving DHCPINFORM on SVI with pbr enabled
CSCub29359	—	ISSU from SXI to SXJ on VSS resets with WS-SVC-WISM2-K9 installed
CSCub38767	—	Devices connected to WS-X6148E-GE-45AT are unable to ping SVI
CSCub52879	—	CCP loopback test for Jian fails upon removal of service-vlan config
CSCub63550	—	CDP fails when crypto connect is configured on a SPA-2x1GE inteface
CSCub72971	—	inrerface resets counter shows 4294967295 after module OIR/switchover
CSCub94085	—	SXJ: CSM/CSM-S/SSLM modules should be powered down
CSCub94186	—	MPLS TE FRR with auto-bandwidth causes hw adj leak/glean on recalc
CSCuc45901	—	VSS IPv6 RHI route from ACE doesn't get removed
CSCuc50707	—	Crash in idbman_if_clear_vlan_id when doing default switchport
CSCuc65082	—	monitor capture view/privilege setting causes MALLOC failures
CSCuc98078	—	Basic Multi-host mode authorization is broken
CSCud15384	—	Vlan-Based Qos fails for Wism module

Identifier	Technology	Description
CSCud83152	—	MVPN traffic punted to RP due to misprogrammed MTU
CSCts87275	Infrastructure	Cat4k with sup7e : same snmp engineID on different cat4k switches
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
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
CSCub65395	IPServices	Sup720 crashes at dhcpd_forward_reply
CSCub78079	IPServices	NAT per VRF: parser fail with route-map applied to static nat
CSCud08682	IPServices	NAT not translating Traceroute's ICMP Unreachables
CSCud09626	IPServices	NAT PPTP use_count 1 entry not removed if TCP data segment with FIN flag
CSCud51025	IPServices	DHCP relay crash @dhcpd_relay_remove_info_option
CSCud89194	IPServices	Backout fix for CSCub22017 for sxj
CSCud95251	IPServices	static nat with vrf looses vrf name after nat translations expire
CSCtd54694	Management	Switch crashes on Show cdp neighbor detail in some conditions
CSCua66870	Multicast	PIM-Dense: OIF on (*,G) is pruned due to RPF changed on (S,G)
CSCub09124	Multicast	MVPN MDT failure due to multicat boundary on non-current RPF interface.
CSCtk37079	Routing	Traceback seen @ ip_sendself
CSCtq49325	Routing	EIGRP graceful shutdown can cause a reload
CSCtr58140	Routing	PFR controlled EIGRP route goes into SIA and resets the neighbor
CSCtt02313	Routing	PfR: Uncontrol TC due to Exit Mismatch
CSCtx04709	Routing	Active routes remain in topology but does not go SIA after route lost
CSCtz84714	Routing	IPv6 : snmpwalk on cIpAddressPfxOrigin does not return /64 subnets
CSCub21480	Routing	Crash at bgp_vpn_impq_add_vrfs_importing when removing import ipv4 cmd
CSCuc63629	Routing	ip vrf forwarding on vlan fails whenever vlan interface shut/no shut

Caveats Resolved in Release 12.2(33)SXJ4

Resolved Routing Caveats

- CSCef01541—Resolved in 12.2(33)SXJ4

  A router processes a packet that is sent to the network address of an interface, if the Layer 2 frame that is encapsulating that packet is specifically crafted to target the Layer 2 adress of the interface or a broadcast Layer 2 address.

  This happens only in the process switching path and does not happen in Cisco Express Forwarding (CEF) path.

  Workaround is to use CEF.

Resolved Security Caveats

- CSCtl59829—Resolved in 12.2(33)SXJ4

  Symptom: Login success and failure messages only display the first 32 bits of the IPv6 source address in IPv4 format.

Source Address FC00::1

*Aug 5 19:39:07.195: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: cisco] [Source: 252.0.0.0] [localport: 23] [Reason: Login Authentication Failed - BadPassword] at 19:39:07 EST Wed Aug 5 2009

Conditions:

- Telnet or SSH from IPv6 enabled device to IPv6 address on router or switch.
- Have login success and failure logging enabled.

```
login on-failure log
login on-success log
```

Workaround: None

Further Problem Description: The IPv4 address is derived from the first 32 bits of the IPv6 address.

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:

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

Resolved Cisco IOS Caveats

- CSCtr88193—Resolved in 12.2(33)SXJ4

  Symptom: Either High CPU or Crash resulting from large number of ipv6 hosts.

  Conditions: This has been seen while sending Multicast Listener Discovery packets with IPv6 and mld snooping enabled.

  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 5.7/4.7:

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

  CVE ID CVE-2012-3062 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)SXJ4

Identifier	Technology	Description
CSCta74577	—	Need to print out module number is message LTL-SP-2-LTL_PARITY_CHECK
CSCtg11421	—	All egress traffic dropped by SIP-400 + BusConnectivityTest failure
CSCtj76176	—	Port-Channel members go to w state (Up Mstr Not-in-Bndl) after SSO
CSCtl58612	—	Stby Sup resets with "boot bootldr", but file doesn't exist on stby
CSCto73878	—	Intermittent PAT Order-of-Operations problem

Identifier	Technology	Description
CSCto95687	—	Failure to aquire sem (l2_se_get_ps_sem) for a long time leads to crash
CSCtr05488	—	Enhanced FlexWAN (WS-X6582-2PA) silently reload during BERT w/o crashinf
CSCtr39973	—	c2w2: Diag failure after second sso with arp policing
CSCtr92285	—	MPLS L2VC down as no SSM ID allocated to VC
CSCts98176	—	RRI routes missing while IPsec SA is up
CSCtt04914	—	Span stops working and must be re-configured to continue working.
CSCtt96152	—	VSS: corrupted Portchannel: LTL missing VSL-link
CSCtw55546	—	Cat6k:sh lacp internal detail output shows wrong Timeout value
CSCtw80411	—	MAB - Fails for devices already connected when enabled
CSCtw81160	—	Auth session successful even when Filter-ID application fails
CSCtw89269	—	Ports in 2X1GE-V2 SPA is not coming UP with configured speed
CSCtx43498	—	cat6500: Some DACL entries may not be pushed to the switch TCAM
CSCty07538	—	Incorrect static NAT translation leads to TCP reset
CSCty20876	—	Show stack does not show correct Information of Last System Crash - SP
CSCty21663	—	EBGP peer flap with mcast traffic cause cpu spike , ospf and ebgp flap
CSCty26260	—	6500 - Stndby Sup not fluching mac when port-security is enabled
CSCty38102	—	STP BPDUs not reaching neighbor switches when capture type span cnfged
CSCty40181	—	VSS: L3VPN traffic not forwarded after switchover
CSCty94405	—	DCP and CCP loopback ondemand tests fail without Jian LAG configured
CSCty97033	—	Duplex not changing using snmpset
CSCty97492	—	Not all ARP queries going out when port-channel (DEC) is brought back up
CSCtz02829	—	IDSM: some config not getting sync'd to standby properly
CSCtz12050	—	Not possible to disable hol-blocking for X6148
CSCtz28302	—	SXJ3: WiSM LAG creation throws %EC-SW1_SP-5-CANNOT_BUNDLE1 errors
CSCtz35247	—	HM_TEST_FAIL TestMgmtPortsLoopback consecutive failure for ASASM on OIR
CSCtz42708	—	Sup720 Storm control on unused port causes TestUnusedPortLoopback fail
CSCua02641	—	Multicast traffic has second drop during SSO/NSF
CSCua32821	—	Stanby console can be get even without "enable standby console"
CSCub21431	—	SXJ4: Jian 2nd data port not getting bundled to LAG upon reload
CSCth83143	Infrastructure	IPv6 access list applied to SNMP community string does not work
CSCti80535	Infrastructure	"Default interface range command" cause standby SUP reset
CSCtk36938	Infrastructure	%SYS-SP-3-CPUHOG @preemption_forced_suspend
CSCtx51515	Infrastructure	backup config using archive feature, generates two files instead of one
CSCsd17017	IPServices	New NAT entry in table when serial int flaps, seeing connectivity issues
CSCsx28822	IPServices	Memory leak in the Redundancy inter-device feature (rf task)
CSCsz24818	IPServices	ASR:MCP_DEV- RP crash observed when trying to telnet using v6 address
CSCtg41289	IPServices	DHCP pad option is garbage

Identifier	Technology	Description
CSCtr30487	IPServices	Memory Leak with static nat - NAT String Chu
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
CSCtc42278	ISDN	%DATACORRUPTION-1-DATAINCONSISTENCY - ISDN incoming call
CSCtz48619	MPLS	LDP Typed Wildcard FEC Capability TLV uses wrong value
CSCto64160	QoS	Path tear not sent for all the sessions on "clear ip rsvp senders * "
CSCtf13343	Routing	Authorization and accounting fail for commands including BGP ASNs
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
CSCtz51004	Routing	VRF route leaking deletes routes on NSF Helper after Switchover
CSCtz60771	Routing	0.0.0.0/1 BGP prefix wrongly originated causing routing issues
CSCty26147	Security	CIPSO pkt. not getting ignored on tunnel interface running 12.2(33)SXI6
CSCto55708	WAN	Build Error @ /ip-core-apps/ntp/ntpcore/src/refim/ntp_loopfilter. c:350
CSCto71384	WAN	892J Source address is incorrect after source interface is down
CSCtt04371	WAN	Need to change the default setting in NTPv4 for faster sync
CSCtw45592	WAN	CLI "NTP Server <dns name>" - does not get synced to standby

Caveats Resolved in Release 12.2(33)SXJ3

Resolved IPServices Caveats

- CSCts12366—Resolved in 12.2(33)SXJ3

  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

Other Resolved Caveats in Release 12.2(33)SXJ3

Identifier	Technology	Description
CSCth40213	—	multiple pre-shared keys with address 0.0.0.0 not supported
CSCth78343	—	Fetching PSK from keyring should not be restricted to local addr config

Identifier	Technology	Description
CSCtj34656	—	debug ip routing shows non-RIB related events
CSCtj40564	—	crypto keyring binding with local address is broken in some scenarios;
CSCtj46927	—	MF:Access Vlan is removed when 802.1x is enabled on port
CSCtl72207	—	Cat2960: MED information missing in LLDP packets
CSCtn05007	—	ip multicast boundary command not filtering in both directions
CSCtn22339	—	Pre-shared-key lost after router reload
CSCtq31974	—	c2wa1b: multicast SR translation not happening after active sup crashes
CSCtq61665	—	c2wa1b: %BIT-STBY-4-OUTOFRANGE: bit 32767 is not in the expected range
CSCts02018	—	Memory leak in Spanning Tree process on SP
CSCts27161	—	VSS:standby reloads due to parser return error command: duplex full
CSCts38007	—	Query Interval mismatch msg appears on a sw where no querier configs
CSCts62391	—	DTP may prevent VSS from fwding UDLD packets to SP after module reload
CSCts66625	—	VRRP master mac-address with Xtag=0 causing high cpu
CSCts82451	—	switch 6509 crash with Bus Error and cv6_new_hwadj
CSCts82932	—	Incorrect dscp-q mapping on trusted interface
CSCts90103	—	Buffer leak on the RP due to IPC messages resulting in a crash
CSCtt23872	—	QoS queueing commands are rejected after manual OIR of module
CSCtt24684	—	GOLD: Minor Errors Incorrectly Reported on a Trifecta Service Module
CSCtt96621	—	TestDCPLoopback fails on data port 2 with Jian LAG configured
CSCtu17483	—	MF:Switch Crashes due to LLDP process
CSCtu22335	—	On a 6500 after a sup switchover arp inspection fails to forward arp
CSCtu36321	—	CVV: Phone mac gets deleted in MATM on CDP 2nd port up/down for MA mode.
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
CSCtw50375	—	NF entry does not get dmac updated after next-hop device sends garp
CSCtw61876	—	IGMPv3 leave results in MCAST packet loss for other receivers
CSCtw83085	—	Parity error message thrown when OIR of T3/E3 SPA in SIP200
CSCtw84639	—	%BIT-4-OUTOFRANGE: bit 32767 is not in the expected range of 1 to 4096
CSCtw85000	—	On 7600, 'snmp trap link-status' out of sync on WAN GiGE interface.
CSCtw93788	—	MDA port during reauth goes to error disabled state on SSO.
CSCtx12231	—	Config Sync: Bulk-sync failure due to PRC mismatch in ACL
CSCtx15569	—	SPA-IPSEC-2G crash packet size above 1800
CSCtx78044	—	6-8 second delay in forwarding mcast after a rapid join/leave/join
CSCtx79489	—	Follow-up ddts for CSCts62391
CSCtx92952	—	SUP crash when issuing show upgrade fpd file ftp/tftp cmd
CSCtx99818	—	ISSU from SXI6 to SXI9 failed

Identifier	Technology	Description
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
CSCta67945	Infrastructure	ifInOctets incorrect values when requested every second with other OIDs
CSCti24577	Infrastructure	Loading a config with banner command creates config sync issues
CSCto06915	Infrastructure	Sup720 remains in ROMMON after SP crash
CSCto70125	Infrastructure	High CPU due to IPSLA tcpConnect probess due to multiple start attempts
CSCtw59648	Infrastructure	BOOTLDR missing from show version
CSCtw85356	Infrastructure	delay auto reflexed on channel interface without config
CSCtx13605	Infrastructure	Need CSCtb92791 Ported to 6500 code OSPF MD5 key gets modified
CSCtx68100	Infrastructure	Reload reason not displayed correctly on some platforms
CSCse99493	IPServices	Router crash with NAT overload and large number of NAT translations
CSCsi11368	IPServices	DHCP Relay agent should remove the relay-info option, not overwrite
CSCtl51688	IPServices	NAT Error registering with Transport Port Manager - Standby Reload
CSCtt70568	IPServices	PPTP timeout entries are never removed from NAT table.
CSCtw61104	IPServices	DHCPv6 LQ:cmts crash with "Corrupted magic value in in-use chunk"
CSCtv97307	MPLS	MLPS LDP flaps with high Tag Control and IPRM CPU utilization
CSCts41032	Multicast	%SYS-2-NOBLOCK: suspend with blocking disabled tracebacks.
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
CSCtn78663	Routing	Cat6k No ICMP Mask Reply
CSCtu79372	Routing	Cat6500 "clear ip route vrf" delete connected routes from ip vrf receive
CSCtw81998	Routing	BGP is not leaking the routes in to vrf using route-map if rib-failure
CSCtx01476	Routing	Config Sync: Bulk-sync failure due to PRC mismatch in ACL
CSCto60047	Security	Chunk corruption crash on trying to abort "show tech" over SSH

Caveats Resolved in Release 12.2(33)SXJ2

Resolved Infrastructure Caveats

- CSCtr91106—Resolved in 12.2(33)SXJ2

  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)SXJ2

  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

Resolved Cisco IOS Caveats

- CSCtq36327—Resolved in 12.2(33)SXJ2

  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.

  Further Problem Description: This is a day-1 issue and the fix is available in SXI7, SXJ2 and MA2.

  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)SXJ2

  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

- CSCts38429—Resolved in 12.2(33)SXJ2

  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)SXJ2

Identifier	Technology	Description
CSCek68936	—	6716 fabric asic causing EC performance issue
CSCsj70829	—	CPU hog caused by OBFL uptime logging
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
CSCsm43012	—	Speed value changed during the upgrade automatically from 10M to 100M
CSCsr50385	—	Crash while executing "clear archive" and "show archive" simultaneosly
CSCsu06967	—	auth-proxy-banner must not be displayed on result page
CSCtc99947	—	Switch drops DHCP INFORM packets from DHCP client
CSCtg96982	—	Memleak @ bitlist_chunk_alloc on VSS on standby switch
CSCth31231	—	dACL for MAB still applied for dot1x users
CSCth83455	—	C2WA1b: set default interface <serial interface> is not working
CSCti45609	—	LISP: improve map-cache build-up time
CSCtj84234	—	Packets drop is there when configuring VRF
CSCtk00198	—	Stack master crashed on defaulting ASw interface
CSCtl77057	—	TestErrorCounterMonitor can generate false positive on 67XX cards

Identifier	Technology	Description
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
CSCtn78508	—	vlan range 1002-1005 automatically added to "sw cap allow vlan" command
CSCtn81945	—	MVPN extranet corrupted linkage
CSCto53119	—	ES40:EoMPLS for a vlan X not progmd on LC after allowing&removing frm VE
CSCto53223	—	VSPA\>WS-IPSEC-3 : Failure in VRF Mode acting as EzVPN Server
CSCto90846	—	Tunnel I/F and Vlan I/F stucked on output and dropped packets on Cat6k.
CSCto99774	—	Crash in vtp mib
CSCtq21616	—	Add a cli to line cards to allow viewing of internal framer errors.
CSCtq24526	—	Memory corruption crash in crypto code
CSCtq26766	—	SUP720-3B crash due to large number of IGMP reports received
CSCtq26863	—	Authentication session information sticks when port shut down
CSCtq27016	—	Qos related Memory leak is observed on ES-40
CSCtq34985	—	DCI: A-VPLS VCs not synced to standby Sup
CSCtq35225	—	Any new SVIs -> NOT coming up due to RP process SW VLAN RP getting stuck
CSCtq38187	—	"VPLS_NP_CLIENT-4-WARN: Invalid VC Index 0 " msg seen in presence of TE
CSCtq38419	—	SP crash on continuous reload of trifecta module
CSCtq40606	—	Span replication loop after switchover on Service Module
CSCtq40780	—	VSS STBY Trifecta x86 waiting infinitly for reset from LCP
CSCtq46279	—	Standby crashes on authz failure when voice and critical vlan are same
CSCtq47971	—	On SSO, IPC communication failed with SIP400 cards: VSS goes to RPR mode
CSCtq48027	—	MVRP: Traffic is NOT flowing in the netwok with MVRP enabled
CSCtq48160	—	cbQosPoliceCfgRateType not set to 2 (Precent) when configured via CLI
CSCtq48386	—	Authfail->Guest, show cmd is incorrect
CSCtq48593	—	VSS:A-VPLSoGRE:Imposotion is not programmed properly after toggling FL.
CSCtq50438	—	c2wa1b: JIAN ports not detected on SIERRA 0523 Image
CSCtq51378	—	TestIPSecEncrypDecrypPkt message while reloading VSS or SSO
CSCtq53902	—	A-VPLSoGRE:SIP-400:Ingress WRED drops are seen on POS int
CSCtq54944	—	Minor Error and port down on Failover from SXH2a to SXJ in RPR mode
CSCtq56136	—	Input errors incrementing when interface is shutdown
CSCtq61884	—	DHCP snooping for unicast not working to HSRP DMAC
CSCtq64820	—	6500 SP crash at cmfi_frr_process_stats_counters
CSCtq65338	—	CDP Bypass allows cisco ip phone to bypass aaa in all host-modes.MUSTFIX
CSCtq66013	—	VSS Active switch crashes if Bennu restarted in ACT & then STDBY switch
CSCtq72873	—	MF: Crash @ eap_auth_fail
CSCtq75000	—	SPA3 card crashes when ACL is configured with Port values
CSCtq80246	—	RPW:SVI goes down after removing and adding back the vlan in VE

Identifier	Technology	Description
CSCtq80394	—	mroute entry not create for sparse default-MDT group
CSCtq86628	—	Traceback at SSO SCHED-SW2_SP-7-WATCH uninitialized boolean "rf task"
CSCtq90605	—	mlapc dynamic priority rollover causes unexpected state
CSCtq90744	—	SNMP trap is not sent for SVI up/down
CSCtq94581	—	voice domain cannot authc when port-security is enabled (MDA mode)
CSCtq95922	—	ASASM power-cycled 'off (Module not responding to Keep Alive polling)'
CSCtq98031	—	VSS: Trifecta not online in any slot of STDBY after removal during TFTP
CSCtr01421	—	cont standby reset "ip source binding <#> vlan <#> <ip> int fa3/8" if L3
CSCtr03012	—	On SSO, Mcast RPF-MFD fails only with static join @ RPF i/f
CSCtr10155	—	Crash following defaulting an interface configuration in a port-channel
CSCtr13929	—	Primary member link changing with addition of new member to bundle
CSCtr15379	—	Cat6500 running SXJ1 image tries to boot unsupported ES+ module
CSCtr19129	—	VSS - need to suppress "SIBYTE-SW2_DFC2-3-SB_TX_FIFO_UNDRFL" msgs
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
CSCtr67722	—	SP CPUHOG on VSS setup with span session
CSCtr68112	—	SW installed NF entry does not get updated when next-hop sends garp
CSCtr73095	—	LAG data-ports going into Suspended with extend Vlan
CSCtr78814	—	MAJ, GOLD, diag_get_port_group(): module 8 - port group table is NULL
CSCtr82360	—	%EARL_L2_ASIC-DFC4-4-DBUS_HDR_ERR: EARL L2 ASIC #0: Dbus Hdr.
CSCtr84253	—	cat6k rapidly exhausts system buffers
CSCts03905	—	NAM GUI access causes SNMP CPU 100%
CSCts09685	—	%EC-SP-5-CANNOT_BUNDLE2 is logged against the auto-gen EC for WiSM
CSCts14723	—	Non-rpf global timer inconsistency in SXJ1
CSCts15934	—	VSS: MALLOC failure reported by diag_display_fpoe_entries
CSCts19697	—	VSS:number of inrerface resets shows 4294967295 when switchover
CSCts24348	—	PBR "set vrf" causes destination ARPing for punted packets and drops
CSCts26267	—	Standby VSS switch reloads due to parser return error
CSCts33952	—	rsh command fails from within TclScript
CSCts49137	—	show tech redirect command fails in SXJ1

Identifier	Technology	Description
CSCts49769	—	CVV: crash @ auth_mgr_ctx_destroy when unconfiguring CVV
CSCts55199	—	A-VPLS with ECMP paths:L2 Multicast traffic is affected for few flows
CSCts57516	—	EzVPN server disconnects all PATed clients
CSCts63619	—	Report REQ_MOD_RESET_ECC2 while R2D2 detect Rx/Tx memory ECC2 error
CSCts66142	—	Reconfiguring "mls ip multicast stub" config does not program tcam
CSCts88817	—	ASA-SM and SVC-NAM3 lock up triggering module reload by switch
CSCtt00490	—	snmpwalk for a N/A DOM-value is returning a bogus value
CSCtt16732	—	SP memory display in wrong on SUP720-3B when running 12.2(33)SXJ1
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
CSCtt26784	—	SUP32 crashes on power cycle "registration timer event"at 12.2(33)SXI6
CSCtt27865	—	VSS:A-VPLS:Traffic loss observed for 4 seconds with GRE tunnel
CSCtt30593	—	C6504-E 12.2(33)SXI5 Long ACL cannot setup by Netconf
CSCtt35853	—	Trifecta:VSS - Console Hung Indefinitely at SSO
CSCtt38735	—	SVIs stuck in Administratively Down state, 'no shut' takes no effect
CSCtt41811	—	Disable Support for VSE card in Warren1.Clix Throttle image
CSCtt46982	—	WiSM-2 in switch-1 of VSS loosing native vlan config after reload
CSCtu01427	—	IPSEC-2G in CC on subif reprograms badly icpu vlan map on change
CSCtu23938	—	Device crash @ qos toggling with portchannel config
CSCtu28383	—	Protocol peer down and cannot ping upstream router with load-defer conf.
CSCtu50683	—	Resetting PS on Standby VSS, reduces power from PS on Active VSS member.
CSCsd46369	AAA	IP source address on packets to TACACS server is wrong
CSCee38838	Infrastructure	kadis timer abort reloads router
CSCtb89424	Infrastructure	Crash at saaEventProcessor
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
CSCsb70368	IPServices	Bus error at ipnat_delete_entry with PPTP-TCP entry deletion
CSCsr17315	IPServices	Autoinstall process not correct with BOOTP or DHCP server in same LAN
CSCtn07696	IPServices	6506-E/Sup720 crash related to SYS-3-URLWRITEFAIL: and TCP-2-INVALIDTCB
CSCtq14817	IPServices	Traceback seen @ ipnat_pptp_client_inside
CSCtq41121	IPServices	IOS NAT: unable to reconfigure static nat ports after removal
CSCtr16396	IPServices	TAC+ Code Incorrectly Implements timeout for tacacs-server timeout
CSCts00341	IPServices	CLI requiring DNS lookup cannot be configured when in SSO mode
CSCtt02390	IPServices	VSS: TFTP-Server fails after switchover or when one of the switches down
CSCtg48785	LegacyProtocols	sh x25 hunt-group %DATACORRUPTION-1-DATAINCONSISTENCY: copy err
CSCtq73473	Management	MF: Crash when entering the 'show cdp interface' command
CSCti32641	MPLS	LDP ICCP capability TLV (0x0405) - (0x07) Bad TLV Length

Identifier	Technology	Description
CSCtf21128	Multicast	(S, G) fwd int is NULL while (*, G) is correct
CSCtr88242	Multicast	PIM-SM doesn't trigger Join message when RPF is changed
CSCsd39315	PPP	distributed multilink bundle should never show no frags rcvd
CSCsv04412	PPP	%MCT1E1-3-TIMEOUT while deleting bundle with CHT1E1 SPA
CSCtr22007	QoS	Bus Error crash in MPLS TE LM Process on 7600
CSCej87096	Routing	Redistribute OSPF command messed up
CSCek39299	Routing	BGP-NSR:stby keep reset after bulk sync for bgp dampening CLI
CSCsg83966	Routing	Import MAP:sh ip bgp vpnv4 vrf does not show all entities
CSCsw63003	Routing	Continous BGP activity may result in increasing amounts of memory held
CSCtn96521	Routing	When the Spoke (dynamic) peer-group is configured before the iBGP (stati
CSCto84723	Routing	Cat6K Crash when removing ACL with Object Tracking alsol ACE with OG
CSCtq43285	Routing	Routing churn BGP-EIGRP in VRF-Lite
CSCtq62273	Routing	Configuring IPV6 crashes the router.
CSCtr58203	Routing	Upgrade from 12.2(33)SXH5 to 12.2(33)SXI6 ip local policy w/ VRF
CSCtr86436	Routing	Router doesn't respond to ICMP echo-req from vrf to global loopback
CSCts16133	Routing	Sup720 may crash after rebuilding object-group configuration
CSCts43881	Routing	Unexpected RIP route leak/redistribution
CSCts68630	Routing	IPV6 ACLs doesn't match the traffic as configured
CSCsr96084	Security	%SYS-6-STACKLOW: Stack for process NHRP running low, 0/6000

Caveats Resolved in Release 12.2(33)SXJ1

Resolved Infrastructure Caveats

- CSCte01606—Resolved in 12.2(33)SXJ1

  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

Resolved Cisco IOS Caveats

- CSCtj22354—Resolved in 12.2(33)SXJ1

  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)SXJ1

  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

Other Resolved Caveats in Release 12.2(33)SXJ1

Identifier	Technology	Description
CSCsr28710	—	SIP200_MP-4-PAUSE CPUHOG during SIP-200 OIR.
CSCsr95189	—	VSS standby switch reset parser error in IDSM config command
CSCsu65095	—	switch crash w traceback after applying "eou rev all"
CSCsu65401	—	tclsh does not send username to AAA server for command authorization
CSCsv60305	—	DMVPN: Missing listen crypto socket when tunnel interface is up
CSCsw89720	—	CPU-HOG error messages are seen when we query cbQosPoliceStatsTable.
CSCsz72735	—	VSS STP state change over port channel
CSCtc06629	—	crash/tracebacks seen @ crypto_ident_count_ipsec_sas_to_peer
CSCtd58259	—	sw voice vlan - port removed from STP if snmpset commands are executed
CSCtd70009	—	IPphone second port notification not clearing session on 2k
CSCtd74965	—	DSCP marking on VTP packets needs to be changed
CSCte95228	—	ES+ combo keeps reloading after cable OIR
CSCtf17152	—	C2W2C: LACP Auto Interleave HA issue
CSCtg09619	—	Web Auth host gets dropped after DHCP renewal with DHCP snooping enabled

Identifier	Technology	Description
CSCti14287	—	Unable to display Jian-L CCP and GoreTex SPROM data using show idprom
CSCti23324	—	Remove recirculation for L2 DEC when all ports on ABA cards or later
CSCti28450	—	Show auth session port...and oid returns different results
CSCti33299	—	RP crash due to TLB exception following crypto-map configuration
CSCti92970	—	MF: WoL not working in Multi-Auth
CSCtj41144	—	Tracebacks seen with MLACP config SM-SP-4-BADEVENT: Event 'ct_expired'
CSCtj44456	—	CSM redundancy sync via CLI causes Standby SUP crash if ANM used
CSCtj60028	—	%MGMTINFRA-3-EICORE:Request droped and OOM-0-HIT_MEMORY_THRESH msg seen
CSCtj60836	—	Traceback @ lacp_sm_post_mux_bundle_sync
CSCtj76591	—	WS-X6548-GE-TX:Outdiscards is counted on only SPAN dest port
CSCtj84500	—	Cat6500 - Locked semaphore after config change for CSM WS-X6066-SLB
CSCtj95352	—	SUP32 resets with System NMI:**** SP System NMI: reason 0x00000009
CSCtj99724	—	SXI1: Memory leak in "mls-msc Process"
CSCtk18890	—	Protected tunnel went down after FRR kicked in
CSCtk31978	—	c2wa1: VSS Act (SW2) reloads after ISSU LV and AV if NAM card is in SW1
CSCtk33826	—	C2WA1: ISSU cycle from sierra->SXI with 256PO not working
CSCtk66648	—	Traceback Spurious memory access pm_get_bcast_supp_discard_counters
CSCtk69755	—	Trace route in mpls TE not working
CSCtl03781	—	ISSU:ONLINE-SW1_SPSTBY-6-INITFAIL: Module 6: Failed to bring up DFC
CSCtl05514	—	IDSM etherchannel fails after SSO
CSCtl05684	—	XAUTH user remains if authenticated by different user during P1 rekey
CSCtl13134	—	"SVCLC SCP communication failed" observed on SUP during ACE reload
CSCtl23179	—	Incorrect TCAM Programming when new DHCP address received.
CSCtl23494	—	Dot1x not functioning properly with 3rd party ip-phones
CSCtl24871	—	GLBP virtual mac not programmed in tunnel internal vlan
CSCtl42871	—	Show Transceiver Detail Should Show N/A for all fields Instead of 0.00
CSCtl47635	—	KB lifetime incorrect in "show crypto session detail"
CSCtl54046	—	Standby Sup crashes@dot1x_get_supp_sb with cts dot1x/manual
CSCtl55179	—	CPU HOG in mlacp process on core isolation
CSCtl56002	—	Traceback seen @ "SCP Write Process"
CSCtl58697	—	c2wa1: Swapping WiSM with JIAN fails to bundle JIAN port in LAG
CSCtl58831	—	small buffer leak on WS-X6708-10GE
CSCtl70909	—	c2wa1: Type6 password encryption is not wrking in Aggressive Mode
CSCtl71282	—	Traffic of Promiscous port is not sent when sec VLAN mode is changed
CSCtl73660	—	c2wa1: IP ACL TCAM doesn't get reset after removing ACL filter from MPA
CSCtl75972	—	CPUHOG for "Virtual Exec" seen when removing/adding ACL on VSS
CSCtl76154	—	c2wa1: WiSM-1 controller 2 status o/p not available in standalone setup

Identifier	Technology	Description
CSCtl76189	—	On inserting JIAN the SVC ips of all WISMs/JIANs in the system flushed
CSCtl76575	—	C2WA1: ISSU RPR downgrade followed by upgrade fails with mlacp
CSCtl79336	—	Unable to ping ipv6ip tunnel ipv6 whose tunnel dest ip learned thru MPLS
CSCtl82493	—	c2wa1: After stdby switch reset some Jians and WiSM mgmt ip ping fails
CSCtl82681	—	Not able to configure IPV6 when xconnect is present on main interfacex
CSCtl83517	—	C2WA1: ISSU cycle from sierra->SXI with 256PO not working - red_mode
CSCtl85689	—	c2wa1b : SM Internal Po remains down due to QOS attribute mismatch
CSCtl85771	—	Both ports in DHD goes to P state on doing SSO in Standby POA
CSCtl87979	—	Flexwan card crashes on single bit parity error
CSCtl88070	—	IPv6 VRF configuration causes software punt for global uRPF
CSCtl98884	—	Crashes noticed in AAA create user (kron /console buffer got corrupted)
CSCtn00835	—	Traceroute via mpls cloud does not show egress PE in 3C mode
CSCtn01848	—	Switch crash after shutdown dot1x routed port
CSCtn03582	—	TTL Failure rate-limiter not working
CSCtn11825	—	MVRP error disables L3 interface part of 6148A LC when match registerN/A
CSCtn12198	—	Watchdog timeout after enabling NetFlow
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.
CSCtn18962	—	ospf :s72033-lanbase-mz image missing subsystems
CSCtn26516	—	C2WA1 : mLACP : Can't unconfig the backbone intf in down state after SSO
CSCtn27004	—	PS AC/DC input sensor is not detected
CSCtn27447	—	Existing option 82 not overwritten but additionally created
CSCtn41851	—	c2wa1:IDSM along with sup not reverting back to cross-bar mode from bus
CSCtn43662	—	Slow memory leak at watcher_create_common (TCP, telnet, watched boolean)
CSCtn49482	—	CONFIG_NV_NEED_OVERRUN and config lock after configuring IDS module
CSCtn52363	—	"channel-group" command missing from member link on module reset
CSCtn52549	—	"show interface" and "show interface counter" is different value.
CSCtn55070	—	call-home http hang, should not use printf in backgroud process
CSCtn57039	—	Memory leak in RADIUS and EAP Framework processes with dot1x configs
CSCtn60147	—	6500 SXI - L2 traffic is policed when CoPP is enabled
CSCtn68317	—	Cat6500/SXI: DHCP snooping removed from vlan on module OIR
CSCtn74068	—	CSCtl71282 Traffic from Promiscous port isn't switched on mode change
CSCtn94479	—	NAM-3 on VSS:can't reverse telnet & TB after system sso
CSCtn96481	—	wrr-queue cos-map can't be configured
CSCto05381	—	AutoQos on WS-X6716-10GE maps cos values 3,4,6,7 to empty Rx queues
CSCto33424	—	After SSO "mls cef error action reset" cli gets added on standby

Identifier	Technology	Description
CSCto34230	—	RRI: C6K not remove routes when SAs removed by DPD.
CSCto35831	—	LLDP: incorrect PMD value causes incorrect physical media capability
CSCto48396	—	6500 LLDP Enabled Capabilities not reporting Bridge capabilities
CSCto56118	—	ACL: Adding a duplicate ACE via an object-group is not rejected
CSCto59387	—	NRGYZ:ERROR:Database uninitialized when walking CISCO-ENERGYWISE-MIB
CSCto69916	—	Apply ACL in order of IPv4 then IPV6 disables TCAM screening on int.
CSCto82241	—	Cat 6500 - MVRP getting enabled on the internal FWSM portchannel
CSCto98855	—	Supervisor crashes in VS mode when VSL LC crashes
CSCtq06964	—	Old Phase ID is used when EzVPN client connect with different ID
CSCtq09449	—	CMTS boot failed and PRE4 crashed for OBFL
CSCtq26863	—	Authentication session information sticks when port shut down
CSCtq35225	—	Any new SVIs -> NOT coming up due to RP process SW VLAN RP getting stuck
CSCtq38187	—	"VPLS_NP_CLIENT-4-WARN: Invalid VC Index 0 " msg seen in presence of TE
CSCtq38419	—	SP crash on continuous reload of trifecta module
CSCtq40780	—	VSS STBY Trifecta x86 waiting infinitly for reset from LCP
CSCtq46279	—	Standby crashes on authz failure when voice and critical vlan are same
CSCtq47971	—	On SSO, IPC communication failed with SIP400 cards: VSS goes to RPR mode
CSCtq48027	—	MVRP: Traffic is NOT flowing in the netwok with MVRP enabled
CSCtq48593	—	VSS:A-VPLSoGRE:Imposotion is not programmed properly after toggling FL.
CSCtq50438	—	c2wa1b: JIAN ports not detected on SIERRA 0523 Image
CSCtq53902	—	A-VPLSoGRE:SIP-400:Ingress WRED drops are seen on POS int
CSCtq66013	—	VSS Active switch crashes if Bennu restarted in ACT & then STDBY switch
CSCtq66622	—	Trifecta Bennu and NAM3 not powered up in Warren1.Bubb throttle image
CSCtq75000	—	SPA3 card crashes when ACL is configured with Port values
CSCtq86628	—	Traceback at SSO SCHED-SW2_SP-7-WATCH uninitialized boolean "rf task"
CSCtq95922	—	ASASM power-cycled 'off (Module not responding to Keep Alive polling)'
CSCsc49958	AAA	aaa authentication fallback to enable caches previously typed password
CSCsi83685	AAA	AAA fallback to radius causes GET_PASSWORD debug message
CSCtd21058	AAA	dACL attribute parsing failed when 'aaa author' debug turned ON
CSCtl54415	AAA	win11(FIT) - dut crashed after trying to ssh to the dut with no key
CSCtl77241	AAA	MF: webauth login triggers switch crash
CSCtn19927	AAA	radius-server attribute 44 Acct-Session-Id not found due to broken CLI
CSCed73951	Infrastructure	banner login #$(hostname)# doesnt work
CSCsw81502	Infrastructure	SNMP HC Poll issue with configurable timer.
CSCta09049	Infrastructure	memory leak in encrypto proc or Pool Manager
CSCtf96250	Infrastructure	IDBMAN-4-CONFIG_WRITE_FAIL and standby sup crash
CSCtn50281	Infrastructure	SNMPv3 uses wrong mac for snmp engine ID

Identifier	Technology	Description
CSCtn78758	Infrastructure	Crash on Modular IOS on cat6k
CSCsu31853	IPServices	TIMEWAIT TCP sessions cause buffer usage until session expires
CSCsv02395	IPServices	Telnet hostname /vrf <name> does not work
CSCtl21288	IPServices	NAT: "%Port xx is being used by system" even after the CSCtd16493 fix
CSCtl21294	IPServices	NAT: Port numbers are lost from running cfg if route-map option is used
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
CSCtn27504	IPServices	track CLI removed after the reload
CSCtn48455	IPServices	short TCP connections can fail in tcp_open, even if they should work
CSCtq41121	IPServices	IOS NAT: unable to reconfigure static nat ports after removal
CSCto59020	LAN	stp/vtp config change triggers vtp to prune all vlans from forwarding
CSCtk64425	LegacyProtocols	DLSW Ethernet Redundancy not passing ARP with ip arp inspection enabled
CSCtl52345	LegacyProtocols	C3825 bounces back packets with non-owned MAC strangely
CSCtn12726	Management	'show cdp neighbor detail' causes phone outage in dot1x environment.
CSCto68456	Management	odr incorrectly installs default route out of an L2 interface.
CSCsd39315	PPP	distributed multilink bundle should never show no frags rcvd
CSCsz82587	QoS	Active crashed on module reset[ES20] with LSM configs
CSCej87096	Routing	Redistribute OSPF command messed up
CSCsx27496	Routing	Rtr Crash when imported path is selected as mpath & src route del in RIB
CSCtf51640	Routing	corrupt debug ip packet detail # output
CSCtg74011	Routing	BGP -IPv6 and IPv4 Capability
CSCtk15123	Routing	BGP updates not sent out with update group
CSCtl12492	Routing	Config sync failure after SSO
CSCtn16784	Routing	VRF static route with global keyword not installed in routing table.
CSCtn78957	Routing	High CPU seen with large IPv6 neighbor table
CSCto46716	Routing	TE tunnel is not added into RIB even its found in forwarding-ad and OSPF
CSCtk31401	Security	Router crashes @ssh2_free_keys when exiting the SSH session from client
CSCtn07728	WAN	ntp_ipv6 subsystem missing in SUP720 Lanbase image

Caveats Resolved in Release 12.2(33)SXJ

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

- CSCti25339—Resolved in 12.2(33)SXJ

  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 IPServices Caveats

- CSCta98734—Resolved in 12.2(33)SXJ

  Symptom: DNS Memory Leak in DNS queries

  Conditions: DNS server configured: 'ip dns server'

  This bug can only possibly surface if the "ip dns-server" is configured, and then only when specific malformed datagrams are received on the DNS udp port 53. This specific datagram malfrmation is that the udp length field indicates a zero-length payload. This should never happen during normal DNS operation.

Workaround: No Workaround at this time

Resolved LegacyProtocols Caveats

- CSCth69364—Resolved in 12.2(33)SXJ

  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.

Resolved Routing Caveats

- CSCti33534—Resolved in 12.2(33)SXJ

  Symptoms: After launching a flood of random IPv6 router advertisements when an interface is configured with "ipv6 address autoconf", removing the IPv6 configuration on the interface with "no ipv6 address autoconf" may cause a reload. Other system instabilities are also possible during and after the flood of random IPv6 router advertisements.

  Conditions: Cisco IOS is configured with "ipv6 address autoconf".

  Workarounds: Not using IPv6 auto-configuration may be used as a workaround.

  Further Information: Cisco IOS checks for the hop limit field in incoming Neighbour Discovery messages and packets received with a hop limit not equal to 255 are discarded. This means that the flood of ND messages has to come from a host that is directly connected to the Cisco IOS device.

  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 6.1/5.5:

  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:OF/RC:C

  CVE ID CVE-2010-4671 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 Security Caveats

- CSCth45540—Resolved in 12.2(33)SXJ

  Symptom: Device crashes in SSH Process

  Conditions: SSH process has to fail to allocate memory for the new connection. This would only occur in extremely low memory conditions.

  Workaround: None.

Resolved Cisco IOS Caveats

- CSCsc60686—Resolved in 12.2(33)SXJ

  Symptom: Failed IKE SAs are created when sending specifically formatted IKE messages.

  Although these IKE SAs can be created with 12.4(4)T, they were also created when tested against the IOS c7200-jk96-mz.CSCsc06695 as well which contained a fix for CSCsc06695.

  After IKE SA's are created by the method, they are never auto-removed.

  Conditions: Normal operation.

Workaround: “clear crypto isakmp 0” which deletes all of the failed IKE SAs

- CSCth87458—Resolved in 12.2(33)SXJ

  Symptoms: Memory leak detected in SSH process during internal testing. Authentication is required in order for a user to cause the memory leak.

  Conditions: This was experienced during internal protocol robustness testing.

  Workaround: Allow SSH connections only from trusted hosts.

  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-2011-2568 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)SXJ

Identifier	Technology	Description
CSCin99433	AAA	config sync PRC failure seen with kerberos password command
CSCsb46724	AAA	AAA server group doesnt failover with mismatched keys for login
CSCsc49958	AAA	aaa authentication fallback to enable caches previously typed password
CSCsw77313	AAA	failed authentication with login command changes the logged user
CSCtb19166	AAA	Access-Request with EAP Identity Response should not include State attr.
CSCtg40901	AAA	TACACS single connection crashes @tplus_increase_sock_write_event_count
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
CSCti00011	AAA	MF: NAD sending previous state attribute in EAP Identity request
CSCtn19927	AAA	radius-server attribute 44 Acct-Session-Id not found due to broken CLI
CSCsm26150	ATM	WR-CEOP-SPA: Router crashes @atm_match_vc_group
CSCti10891	ATM	6500 crash due to ATM following upgrade to SXI4
CSCdx30874	Cisco IOS	show cry eng conn active shows incorrect interface name on GRE ints
CSCed01286	Cisco IOS	Traceback at em_unlock_internal
CSCef71929	Cisco IOS	DMVPN: HUB displays TED message when TED is not configured.
CSCek52883	Cisco IOS	without IC new peers are added to dyn map instance
CSCin99139	Cisco IOS	oakley_begin_qm seen during XAUTH
CSCsb02158	Cisco IOS	RSA-SIG without CA not working with usage-keys on 2811
CSCsb58856	Cisco IOS	dialer interface does not kick off interface is cef or fast switchin
CSCsb59455	Cisco IOS	Wrong NAS-Port-Id in Radius accounting
CSCsb79586	Cisco IOS	ISR: eToken removal timeout does not work after hostname change
CSCsb94509	Cisco IOS	With 50 ACLS configured on server ezvpn client connection fails

Identifier	Technology	Description
CSCse29460	Cisco IOS	distribute-list route-map match source-protocol not working for ospf
CSCsg03916	Cisco IOS	tacacs sys_acct system stop and start not sent after reload
CSCsg49757	Cisco IOS	Combining Gig-Sub-intf & crypto connect & vlan with crypto engine
CSCsg78501	Cisco IOS	IKE should not delete established tunnel upon RSA key regeneration
CSCsg96436	Cisco IOS	EZVPN router using cumulative missed keepalives instead of consecutive
CSCsg97955	Cisco IOS	Small Buffer Leak in send_nat_keepalive w/ crypto isakmp nat keepalive
CSCsh50275	Cisco IOS	DMVPN-ISAKMP Phase 1 gets attached to wrong ISAKMP profile breaks Phase2
CSCsi57874	Cisco IOS	ID payload protocol/port should be 0/0 instead of 17/0 in aggressive mod
CSCsi83806	Cisco IOS	High CPU on IP Input on MPLS/VPN PE acting as DMVPN Hub
CSCsj19194	Cisco IOS	SP crashes after %PM-3-INTERNALERROR due to switchport flapping
CSCsk28857	Cisco IOS	Packet drops seen during Stress test after first Re-key
CSCsm81529	Cisco IOS	Editting a crypto profile while a console deletes that same prof reloads
CSCsq45161	Cisco IOS	High CPU usage on Virtual-Exec due to renewal of DHCP Snooping database
CSCsr39340	Cisco IOS	MPLS packets are not sent across tunnel
CSCsr57766	Cisco IOS	clear crypto session local <ipaddr> caused CPU HOG crash
CSCsr62489	Cisco IOS	No mask on LC/SP for directly connected prefixes
CSCsu67919	Cisco IOS	SIP crashes - hqf_cwpa_pak_enqueue_local
CSCsu69515	Cisco IOS	auth_mgr: supplicant-name not correctly displayed
CSCsv90904	Cisco IOS	Cat6k: UDP port 2228 is opened by default
CSCsw36363	Cisco IOS	SUP32 temperature sensor AUX-1 temperature: N/O
CSCsx96689	Cisco IOS	Bulk sync failed for stp with 802.1x/MDA
CSCsy08264	Cisco IOS	ES40 QoS: incorrect error handling after running out of bw profiles
CSCsy33145	Cisco IOS	ES+ intf default queues need to be limited to 1% of intf bw on port cong
CSCsz72735	Cisco IOS	VSS STP state change over port channel
CSCta24271	Cisco IOS	6500 removes switchport access vlan after a dot1x authentication
CSCta35728	Cisco IOS	IPSec deletes wrong tunnel when peer has address change
CSCta86571	Cisco IOS	c4hd1: BIT-SW2_SP-4-OUTOFRANGE TB seen during SS0
CSCtb05389	Cisco IOS	Alignment errors seen when IKE phase1 failed due to malformed ike packet
CSCtc14506	Cisco IOS	mvpn:PIM neigh over MDT tunnel doesnot come up on del & add vrf on VSS
CSCtc32207	Cisco IOS	Need better accuracy in RP crash reporting
CSCtc69463	Cisco IOS	Interface input rate is doubled the output when BFD is configured
CSCtc86019	Cisco IOS	Infrastructure for VSS SNMP traps transmission
CSCtc95709	Cisco IOS	Called strlen on unitialized (non-null termating) patch digest
CSCtd17586	Cisco IOS	Kron policy cli show tech removed from configuration after occurrence.
CSCtd69074	Cisco IOS	VSS: No resv vlan assigned after del-add VRF after SSO.
CSCtd74905	Cisco IOS	Sup2T-VSL:logging buffered command is not synced with standby after SSO
CSCtd84111	Cisco IOS	IOS SLB doesn't add the CASA input features on an interface

Identifier	Technology	Description
CSCtd91871	Cisco IOS	EZVPN - memory leak after ungraceful disconnect of client behind PATl
CSCte01410	Cisco IOS	lost packests between FWSM and engine when switchover by SSO
CSCte44826	Cisco IOS	memory leak in cfib_alloc_sb running SXH3a
CSCte64898	Cisco IOS	Vacl capture won't work in Ringar when on different Metro
CSCte69094	Cisco IOS	Hash for the energywise secret changing constantly
CSCte71999	Cisco IOS	Replace ISSU capability negotiation workaround for 4k
CSCte75473	Cisco IOS	SPA-IPSEC-2G is dropping ISIS L2 packets
CSCte76841	Cisco IOS	Adding SP and RP in the middle of crashinfofiles for cat6000
CSCte81219	Cisco IOS	Inband notification mechanism needed for packet drops due to throttling
CSCte90818	Cisco IOS	MPLS Label to GRE traffic stops on toggling 'mls mpls tun-recir'
CSCte95492	Cisco IOS	C2W2C: Continuous Tracebacks are seen after Second SSO
CSCte95819	Cisco IOS	failover from dot1x to webauth bypassing MAB when dot1x pre-empts MAB
CSCte96453	Cisco IOS	Switch intermittently crashes bringing up port with energywise level 10
CSCte99373	Cisco IOS	extranet: mrib S,G entry never removed after pim disabled on IIF
CSCtf21851	Cisco IOS	BFD session flap after interface get up status
CSCtf23313	Cisco IOS	C2W2C: Standby Crashes continuously after ISSU LV
CSCtf25141	Cisco IOS	Mem leak seen msc_create_met_set, msc_update_met_set & hal_send_met_job
CSCtf28866	Cisco IOS	Ping and routing protocols go down on VS after RR mode change due to ltl
CSCtf33948	Cisco IOS	PC behind phone authenticates twice.
CSCtf49490	Cisco IOS	dot1x authentication manager inactivity crash upon trunk interface flap
CSCtf50155	Cisco IOS	CDP neighbors aren't seen on layer2 subinterface
CSCtf61757	Cisco IOS	4sup: Power to module in slot 7 set off (Module Failed SCP dnld)
CSCtf71990	Cisco IOS	Call-home message not sent on reload if source-ip-addr is configured
CSCtf76561	Cisco IOS	c2w2c: VSS MEC caching can fail /w vlan change on VS Act, if stdby down
CSCtf78122	Cisco IOS	EAPOL "seen" flag is not set when MAB is pre-empted by 802.1x
CSCtf80540	Cisco IOS	VSS: Memory Leaks with EAP Framework with CTS dot1x/manual links.
CSCtf83906	Cisco IOS	W2.Clix: after apply/remove/re-apply v6 ACL's, TCAM full
CSCtf88089	Cisco IOS	VSS: TB's seen with SSO
CSCtf91665	Cisco IOS	CSCtf56694 creates auth fail retry anomaly
CSCtf93027	Cisco IOS	sup 720 crashes while executing show file desc continously
CSCtf93876	Cisco IOS	"sh plat hardware capacity multicast" does not work after switchover
CSCtf98621	Cisco IOS	Recreating a deleted vlan comes up with "act/lshut" state
CSCtg06121	Cisco IOS	W2.Clix:Active sup crashes on doing ICA reset of the standby vss switch
CSCtg08019	Cisco IOS	Several Malabar-RL under test being reset while perform Sup switch-over
CSCtg09360	Cisco IOS	dot1x security violation with RSPAN configured
CSCtg17979	Cisco IOS	vs_ltl_set_ucast_source_indices slot 19 num_ports 8 fail msgs on bootup
CSCtg18269	Cisco IOS	Event 'soft_reset' is invalid for the current state 'remote_soft_reset':

Identifier	Technology	Description
CSCtg18877	Cisco IOS	After insert PS2, appear "%C6KENV-SP-4-PSFANFAILED..."messeage.
CSCtg20098	Cisco IOS	SVI needs to be created for EW client to connect to the switch
CSCtg26870	Cisco IOS	Bridge Assurance broken on root port
CSCtg29266	Cisco IOS	Increasing DHCP snooping database size
CSCtg30383	Cisco IOS	vif int address change causing vlan/vpn programming mismatch in sp
CSCtg32588	Cisco IOS	Unknown unicast traffic drop sso with pseudo class config with VPLS TE
CSCtg32797	Cisco IOS	c6k long failover issue with multicast MVPN
CSCtg34169	Cisco IOS	VSS: cannot boot standby after 2nd switchover
CSCtg37826	Cisco IOS	Inter range command doesn't work
CSCtg41173	Cisco IOS	Checkout CSCte68072 (CoPP for VRRP,BFD,GLBP) from w2clix
CSCtg41420	Cisco IOS	PIM/BGP takes 60-70 sec to establish on ip-tunnel on serial interface up
CSCtg44661	Cisco IOS	ASR router crashes when unconfiguring route-map
CSCtg45139	Cisco IOS	4sup: vs_ha_slc_sync_startup_config:Getting local startup config failed
CSCtg47088	Cisco IOS	Sticky mac-address entry not removed from running-config
CSCtg50990	Cisco IOS	6500 DHCPv6 relay does not forward on layer 3 vlan interfaces.
CSCtg54603	Cisco IOS	IPC Standby port not transitioning to Active Ports after RP Switchover
CSCtg54691	Cisco IOS	Met2 is not programmed when p2p gre tunnel is IIF for service reflect gr
CSCtg57151	Cisco IOS	Cat6500 running 12.2933)SXH4 modular IOS crashed without RP crashinfo
CSCtg58235	Cisco IOS	Minor Error @ bootup on multiple 8xCHT1/E1 SPA cards.
CSCtg60424	Cisco IOS	Fast-UDLD:Some ports connecting to VSS stby getting err-disalbed on boot
CSCtg63240	Cisco IOS	cat6500/12.2(33)SXH6 - SNMP-WALK: slow memory leak (SNMP SMALL CHU)
CSCtg68012	Cisco IOS	%SCHED-3-THRASHING: Process thrashing on watched mssg event
CSCtg73213	Cisco IOS	c2w2c - Crash seen on Configuring ATMoMoGRE
CSCtg73798	Cisco IOS	BPDU PW goes down on one side when peer LC is reset twice
CSCtg78883	Cisco IOS	Patch triggers EARL Recovery.
CSCtg79692	Cisco IOS	W2C: Multicast traffic duplicated when OIR card comes back up
CSCtg82121	Cisco IOS	CLIX: Z switchover does not work
CSCtg85476	Cisco IOS	CAT6K NTI ERR and stdby hangs with abortversion while stdby reloading
CSCtg85484	Cisco IOS	No RST packets send to client for an idle out connection with VRF LITE
CSCtg89262	Cisco IOS	Switch sends eapol response packet, during bootup with aaa guarantee fir
CSCtg92327	Cisco IOS	MET entries are not deleted properly
CSCtg94067	Cisco IOS	MLS-MSC ASSERTION FAILED with Bidir traffic drop on ISSU RV
CSCtg94220	Cisco IOS	BIT-SP-4-OUTOFRANGE:bit 50463232 is notin d expectd rangeof 1920 t 8191
CSCtg94601	Cisco IOS	C4HD1: Continuous TBs @ EthChnl assert failure: on VSS
CSCtg98525	Cisco IOS	ISSU MLS MSC Client(6036) incompatible while issu btn SXI2a->SXI4.FC2
CSCth01912	Cisco IOS	Tbs @VSL manager on SSO
CSCth02812	Cisco IOS	Unicast flood on ingress asymmetric L2 device after TCN event

Identifier	Technology	Description
CSCth04998	Cisco IOS	[VSS] DFC installs drop index for MAC-address
CSCth05276	Cisco IOS	VSS: WS-X6716-10GE TestLoopback fails occasinally in slot 2 port 1
CSCth07233	Cisco IOS	SPA Crypto Connect SSO fails with SVI to Physical int
CSCth10626	Cisco IOS	C2W2C: Memory leak due to OIR of WiSM Module
CSCth12206	Cisco IOS	6500 with 12.2(33)SXI3 May Not Forward Multicast With SLB Configured
CSCth13500	Cisco IOS	SXH: Member entries missing for port-channel in ifStackTable for SUP32
CSCth13572	Cisco IOS	C2W2C: WS-X6716-10GE Failed TestMacNotification and reset after VSS SSO
CSCth15109	Cisco IOS	Flowmask conflict between "Intf full flow" and "full flow least"
CSCth18024	Cisco IOS	xconnect: not show pseudowire status syslog on remote PE
CSCth23534	Cisco IOS	2960: Crash when host is in auth fail vlan and ACS not reachable
CSCth23794	Cisco IOS	Heathland & RR interfaces errdisable with "vlan inte all poli des" cfg
CSCth26739	Cisco IOS	UTIL-3-TREE Data structure error--attempt to remove is seen.
CSCth26920	Cisco IOS	TCL: ungraceful exit from tclsh can leave the Tcl Server running
CSCth29861	Cisco IOS	VSS: Crash at validate_memory/checkheaps after ISSU from SXI3 to SXI4
CSCth29986	Cisco IOS	ip2tag fragmentation not working with TE tunnel
CSCth29993	Cisco IOS	Upgrade Atlas FPGA for javelin SPAs on 6500 platform
CSCth33985	Cisco IOS	LLDP-MED Network Policy TLV DSCP set to 45
CSCth34752	Cisco IOS	Cat6k crashes at 'show ip mroute vrf'
CSCth35011	Cisco IOS	memory leak in name_svr.proc on devices running modular IOS
CSCth36813	Cisco IOS	VSL PO goes down while changing the switch fabric mode
CSCth37830	Cisco IOS	12.2(33)SXI3 - xconnect traffic stops when neighboring xconnect removed
CSCth38120	Cisco IOS	RIP offset 0 command is not synced to the standby PRE
CSCth40444	Cisco IOS	Tracebacks on inserting 6708 in 6500 with SXI3
CSCth41644	Cisco IOS	6716 in performance mode has incorrect input/output rate counters
CSCth42709	Cisco IOS	AToM/ATM AC: pvc cell-packing change causes continious flaps if pw redun
CSCth43783	Cisco IOS	No hardware entries for EoMPLS pseudowire
CSCth45241	Cisco IOS	CE1-CE2 ping is not wroking with GRE tunnel
CSCth48435	Cisco IOS	Tracebacks seen on reduncdancy force with BFD
CSCth48803	Cisco IOS	VS2 - Heathland fast-hello link faills after chg port-grp mode
CSCth49187	Cisco IOS	Alloc-Proc *Dead* in VTPMIB EDIT BUFFER using vtpmib_download_config
CSCth52866	Cisco IOS	Cat6k - changing interface value via SNMP with "parser config cache int"
CSCth55383	Cisco IOS	%EARL-DFC2-2-SWITCH_BUS_IDLE message after "show tech"
CSCth55689	Cisco IOS	ssm ids are down on clearing xconnect before Primary VCs are up
CSCth60232	Cisco IOS	SXH: Port-channel interface flap when changing vlan mask
CSCth60242	Cisco IOS	l2tp-class password <TYPE 0> got encrypted to TYPE 7 in sh run
CSCth61317	Cisco IOS	Message Severity for Noc Payload Crc Error should be 3
CSCth61622	Cisco IOS	Crash seen on carson split Image

Identifier	Technology	Description
CSCth62957	Cisco IOS	IPv6 link local packet loops endlessly when L2VPN/RP SPAN configured
CSCth63715	Cisco IOS	VSS:VPLS TE traffic not forwarded after twice switchover
CSCth66667	Cisco IOS	S,G expiry timer is updated during about 2min more after stop S,G stream
CSCth69504	Cisco IOS	7600 - Small buffer leak on SP due to IGMP snooping
CSCth70481	Cisco IOS	LC frame-relay context missing in advipservices SXI4 Image
CSCth73181	Cisco IOS	Connectivity issue on Cat6k due to index2dvlan table misprogrammed
CSCth73553	Cisco IOS	dot1x phone unregistered during SSO switch-over
CSCth74953	Cisco IOS	SPI Value shown incorrectly as zero for ipsec sa with crypto profiles
CSCth76204	Cisco IOS	TestSPRPInbandPing - No swover/crash after failure threshold reached
CSCth76325	Cisco IOS	OSPFv2 not present in SXI4 base image
CSCth79661	Cisco IOS	MPLS packets missing in TE tunnel accounting
CSCth83634	Cisco IOS	RSTP: Shut/No shut on unrelated neighbour causes root flap
CSCth84848	Cisco IOS	IPv6 OID's not getting polled IPServices feature set
CSCth87458	Cisco IOS	SSH: Memory leak in ssh_buffer_get_string
CSCth87937	Cisco IOS	Crash after configuring 'ip multicast boundary'
CSCth92639	Cisco IOS	Extranet MVPN: the triggered pim join functionality is not working
CSCth93066	Cisco IOS	IPV6 mcast traffic is SW forwded over standby uplink with DCEF-only mode
CSCti00272	Cisco IOS	MultiHost: Web Authentication is triggered after 802.1x authentication
CSCti00548	Cisco IOS	Invalid get detected for Object cpwVcCreateTime
CSCti01426	Cisco IOS	Switch crashes after configuring 'auto qos voip trust'
CSCti01971	Cisco IOS	Active router crashes @ bfd_ipv6_get_local for scaled bfd ipv6 configs
CSCti02581	Cisco IOS	MF:State attribute from previous EAP exchange included in Access Request
CSCti04670	Cisco IOS	Crash found @ sw_mgr_show_feature_base
CSCti14287	Cisco IOS	Unable to display Jian-L CCP and GoreTex SPROM data using show idprom
CSCti22519	Cisco IOS	%ILPOWER-7-DETECT doesnt display with 6500Sup720 wid IOS train 12.2SX
CSCti23872	Cisco IOS	traceroute double hop with set vrf due to double ttl decrement
CSCti30359	Cisco IOS	Client in guest-vlan sending EAPOL start cause security violation on int
CSCti32358	Cisco IOS	linkup is detected earlier than that of the connected device
CSCti35158	Cisco IOS	sup720: L2TP forward L2 PDU received on flexlink backup interface
CSCti35668	Cisco IOS	IoS "show mod" output display wrong
CSCti36805	Cisco IOS	show facility-alarm status shows negative alarm counts
CSCti37172	Cisco IOS	Ingress SPAN on Sup duplicates packets to ACE module
CSCti47250	Cisco IOS	MVPN: S,G entry not created in mroute table for default-MDT group
CSCti48407	Cisco IOS	Incorrect TTL handling in MPLS traceroute if TTL=1
CSCti53769	Cisco IOS	Standby reloads continuously when DA exclude link is Lo2147483647
CSCti54470	Cisco IOS	Cat6K Mcast Packet loss with IGMP snooping and frequent join/leave
CSCti55894	Cisco IOS	Service Policy applied twice on multilink interface when bounced

Identifier	Technology	Description
CSCti57096	Cisco IOS	6500 OIR causes crash w/ service policty on Distributed Etherchannel
CSCti60740	Cisco IOS	crash after disconnect command
CSCti64429	Cisco IOS	Bus Error Crash at fm_process_nf_dbase_clr_timer
CSCti65529	Cisco IOS	Gold diag will fail TestTrafficStress with the Wism installed .
CSCti67447	Cisco IOS	C2wa1-NSF/SSO:- Traffic loss for 8-12 sec with LDP GR enabled
CSCti68459	Cisco IOS	ISSU aborts at runversion due to BOOT var using sup-bootflash
CSCti71807	Cisco IOS	cnfTopFlowsOutputIfIndex returns value 0, instead of destIf
CSCti72095	Cisco IOS	c2wa1: Switch crashed after ISSU runversion from latest sierra to SXI2a
CSCti72424	Cisco IOS	Memory leak in dot1x auth process
CSCti83055	Cisco IOS	CLI: Parser ambiguity with "show platform hardware .." options
CSCti83486	Cisco IOS	c2wa1:Crash @pm_is_rspan_vlan with 7600-SSC with spa-ipsec-2g while boot
CSCti84025	Cisco IOS	VRFs hardware re-mapping causing MLS/CEF inconsistencies
CSCti84655	Cisco IOS	Crash when voice and access VLAN are misconfigured as same VLAN id
CSCti84718	Cisco IOS	CPUHOG @ ipnat_ipalias_check_waitlist+E8 after sh/nosh PBR po int
CSCti85352	Cisco IOS	W1.8: Removing vlan-group from fw mod,vlan-gp already assign get removed
CSCti89368	Cisco IOS	polling xbar using bogus index causes VSAPI-SW1-3-VSAPI_ASSERT &TB
CSCti89747	Cisco IOS	VSS: L2 traffic on healthland gets punted to CPU causing high CPU utilz
CSCti93310	Cisco IOS	With static IGMP outgoing port not programmed in hardware after reload
CSCti94107	Cisco IOS	c2wa1:BOOTUP_TEST_FAIL: Switch 2 Module 1: TestQos failed
CSCti99869	Cisco IOS	IOMEM memleak: DHCP snooping in relay agent environments - Middle buffer
CSCtj01590	Cisco IOS	Unexpected Crypto-routes removals and wrong refcount on RRI routes
CSCtj04562	Cisco IOS	PBR with 'set interface null' causes incorrect tcam programming
CSCtj05198	Cisco IOS	With 2 EIGRP AS, PfR fails to control the route
CSCtj06411	Cisco IOS	crash on single bit parity error with ECC memory
CSCtj06432	Cisco IOS	Crash seen @ msc_destroy_met_set during SSO
CSCtj07133	Cisco IOS	Incorrect switchover to SPT with Multipath configured
CSCtj11375	Cisco IOS	Traffic leaks between secondary vlans when promisucous port is converted
CSCtj15088	Cisco IOS	c2w2:MDEBUG tracebacks @ qm process while applying service policy.
CSCtj22529	Cisco IOS	some mcast shortcut are process switched in ISSU RV.
CSCtj27523	Cisco IOS	On Standby Sup SP, Memory leak seen related to MET
CSCtj28482	Cisco IOS	Cat6k QoS: priority-queue cos-map cmd inserts also rcv-queue cos-map cmd
CSCtj38057	Cisco IOS	QOS ACEs with 'eq' for dst ports not programmed when LOUs/label exceeded
CSCtj45154	Cisco IOS	DUT crashes upon removing dot1x global cmd (auth_mgr_context.c:2375)
CSCtj52310	Cisco IOS	C2wa1: VSS coming up in RPR after switchover w/ dual-active fast-hello
CSCtj58219	Cisco IOS	Standby switch crashes when repl mode is changed to egress in ISSU RV
CSCtj59721	Cisco IOS	%PM_SCP-2-LCP_FW_ERR_INFORM: module 8 is experiencing the following err
CSCtj60445	Cisco IOS	clear crypto sa vrf may be removing sa in the wrong vrf.

Identifier	Technology	Description
CSCtj61261	Cisco IOS	DFC has misprogrammed i2k_slvan for private vlan after reload
CSCtj63031	Cisco IOS	SNMP syslog trap for OER_MC-5-NOTICE msg is not sent
CSCtj69212	Cisco IOS	MAB Framework leaking memory
CSCtj72688	Cisco IOS	SNMP: need to disable snmp flowcontrol setting for VSL interfaces
CSCtj84908	Cisco IOS	Options data following option82 lost with DHCP-Snooping option82 enabled
CSCtj90091	Cisco IOS	PFC3C fragment entry is not created when ICMPv6 ACL is applied
CSCtj91384	Cisco IOS	IPC Crash Seen In SXH
CSCtj91928	Cisco IOS	C6K PBR set ip nexthop verify-availability w/ tracking & nexthop tunnel
CSCtj91961	Cisco IOS	nvlog contents are cryptic. power_oper_type 62
CSCtj95068	Cisco IOS	SPAN session gets enabled by snmp set operation
CSCtj95352	Cisco IOS	SUP32 resets with System NMI:**** SP System NMI: reason 0x00000009
CSCtj96421	Cisco IOS	Leak in SP Buffers. Seen when C6KPWR-SW1_SP-4-PSOUTPUTDROP is logged
CSCtj96837	Cisco IOS	Blank occurred on show run when the system switchover.
CSCtj97582	Cisco IOS	Setting AdminSpeed to autoDetect10100 on cat6500 returns WRONG_VALUE_ERR
CSCtk00056	Cisco IOS	Port Flow-Control Deafult changed after CSCsq14259 on Sup WS-SUP720-3B
CSCtk02666	Cisco IOS	Double dip of scalable EoMPLS traffic on HA switchover
CSCtk05146	Cisco IOS	IPv6 Solicit dropped by RAguard
CSCtk05747	Cisco IOS	TCAM remerge seen on interface up/down, causing 100% CPU
CSCtk06057	Cisco IOS	Enable ESM for sup32 image in sierra
CSCtk10374	Cisco IOS	Crash @ cts_dot1x_authc_supp_info.
CSCtk10626	Cisco IOS	Cat6k - CLNS frames cropped by flexwan
CSCtk14496	Cisco IOS	WA1: system crash when issue {red reload peer} on VS setup
CSCtk16232	Cisco IOS	MVPN traffic software switched due to mtu failure
CSCtk31747	Cisco IOS	RRI route deletion is not proper if same peer ip is across differentFVRF
CSCtk31870	Cisco IOS	FPD upgrade hangs with 'Failed to configure the line card' error message
CSCtk31978	Cisco IOS	c2wa1: VSS Act (SW2) reloads after ISSU LV and AV if NAM card is in SW1
CSCtk32622	Cisco IOS	WS-X6748-GE-TX May Reset If All Ports Are Shutdown With Interface Range
CSCtk33826	Cisco IOS	C2WA1: ISSU cycle from sierra->SXI with 256PO not working
CSCtk36622	Cisco IOS	Ingress PE routers do not join data MDT of other with connected source
CSCtk48038	Cisco IOS	c2wa1:SP:macedon_b2b_is_failover: msg seen when shut/noshut crypto vlan
CSCtk53130	Cisco IOS	Command "pseudowire" rejected at Virtual-PPP interface with ipv6
CSCtk54650	Cisco IOS	Modifying IPv6 ACL completely change the ACL configuration
CSCtk59111	Cisco IOS	"txDrops" counter in "show fabric channel-counters" has increasing.
CSCtk60169	Cisco IOS	config sync not happening after setting crcSpanDstPermitListEnabled obj
CSCtk61460	Cisco IOS	Set vlanPortVlan on a port to diff access vlan disconnect IP phone
CSCtk64490	Cisco IOS	c2wa1: XDR ISSU is bypassed on WAN cards while not bypassed on SUP side
CSCtk66648	Cisco IOS	Traceback Spurious memory access pm_get_bcast_supp_discard_counters

Identifier	Technology	Description
CSCtk76633	Cisco IOS	Wrong FPOE programing after replacing the chassis with different type
CSCtl00236	Cisco IOS	Policy-routing looses dhcp next-hop
CSCtl03781	Cisco IOS	ISSU:ONLINE-SW1_SPSTBY-6-INITFAIL: Module 6: Failed to bring up DFC
CSCtl05514	Cisco IOS	IDSM etherchannel fails after SSO
CSCtl45122	Cisco IOS	CSCsv76509 seen again in SXI4
CSCtl50744	Cisco IOS	crash on 6k when dot1x accounting feature is turned on
CSCtl58697	Cisco IOS	c2wa1: Swapping WiSM with JIAN fails to bundle JIAN port in LAG
CSCtl71282	Cisco IOS	Traffic of Promiscous port is not sent when sec VLAN mode is changed
CSCtl76154	Cisco IOS	c2wa1: WiSM-1 controller 2 status o/p not available in standalone setup
CSCtl82493	Cisco IOS	c2wa1: After stdby switch reset some Jians and WiSM mgmt ip ping fails
CSCtl85771	Cisco IOS	Both ports in DHD goes to P state on doing SSO in Standby POA
CSCtl98884	Cisco IOS	Crashes noticed in AAA create user (kron /console buffer got corrupted)
CSCtn12243	Cisco IOS	T/b @ icc_send_mcast_request upon bootup
CSCtn14939	Cisco IOS	Crash and Mem Leak under L2 PIM Snooping config after ISSU LoadVer
CSCtn16303	Cisco IOS	The notification was generated incorrectly by ME-C6524GT-8S.
CSCtn18962	Cisco IOS	ospf :s72033-lanbase-mz image missing subsystems
CSCtn27004	Cisco IOS	PS AC/DC input sensor is not detected
CSCtn27447	Cisco IOS	Existing option 82 not overwritten but additionally created
CSCtn52363	Cisco IOS	"channel-group" command missing from member link on module reset
CSCtn74068	Cisco IOS	CSCtl71282 Traffic from Promiscous port isn't switched on mode change
CSCtn96481	Cisco IOS	wrr-queue cos-map can't be configured
CSCsi25430	Infrastructure	JQL: VS2: ActiveVS crash@show_one_proc_one_event_list
CSCsr18177	Infrastructure	Traceback after denied "do" command - 12.2SRB
CSCsz45087	Infrastructure	Incorrect Behavior of Ip sla react-config action-type
CSCsz56169	Infrastructure	crash by memory corruption after executing 'show user'
CSCta09049	Infrastructure	memory leak in encrypto proc or Pool Manager
CSCta15808	Infrastructure	Router Crashes on V6 sanity test:tcrashes in trace_caller()
CSCta78502	Infrastructure	Banner: %r raw data support instead of %s output
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
CSCtc51940	Infrastructure	Error message thrown while executing redirect command
CSCtf27594	Infrastructure	ME-C3750 CPU util. spike to 100% related to BFD
CSCtf45681	Infrastructure	%SCHED-3-SEMLOCKED:SNMP ENGINE after warmstart SNMP ENGINE
CSCtg06597	Infrastructure	Memory leak pointing to hc_counter_force_64bit_cntrs
CSCtg17902	Infrastructure	Logger Process spiking the CPU utilization
CSCtg19572	Infrastructure	Memory leak in two dfs processes
CSCtg64468	Infrastructure	indefinit loops in get_bufferpool_info() & get_buffercachepool_info()

Identifier	Technology	Description
CSCth01674	Infrastructure	*Dead* memory increasing in (coalesced)
CSCti01692	Infrastructure	RP Crash at ifs_buffer_write upon "show run"
CSCti02428	Infrastructure	Configuration mode lock up
CSCti10016	Infrastructure	Huge amount of disk size loss after format
CSCti54695	Infrastructure	cannot remove snmp-server engineID from running-config
CSCti60077	Infrastructure	Memory leak in IP SNMP Process on cat6k
CSCtj31116	Infrastructure	logging discriminator stops severity filtering
CSCtj56019	Infrastructure	WA1: mibwalk dot1dBridge using mst context does not return correct info
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
CSCtf75053	IPServices	10K is corrupting DHCP-NACK while option 54 is missing in DHCP Request
CSCtf88851	IPServices	tcpConnState in a trap has value zero
CSCtf92314	IPServices	Bus error crash at snmpnat_port_avl_compare
CSCtg52885	IPServices	HSRP on subinterfaces stay stuck in INIT after link flap
CSCtg71467	IPServices	Ospfv3 gets deleted after reload or SSO if virtual ipv6 addr on intf
CSCti05663	IPServices	DHCPACK dropped on relay when Ether-Channel active member link shut down
CSCti13845	IPServices	tftp-server will not serve files of same name in different directories
CSCti28796	IPServices	removing group from class-map type multicast-flows does not change igmp
CSCti71843	IPServices	Ping to NAT outside neighboring interface fails
CSCtk95464	IPServices	Static arp removed after HSRP switchover
CSCtf69187	LAN	changes of Vlan on the sever with VTPv3 is not updated on client with v2
CSCtg25721	LegacyProtocols	DLSw ER crashes in dlsw_get_sb_from_rhandle
CSCtj00728	LegacyProtocols	ASR crash when configuring DECnet
CSCtk95992	LegacyProtocols	DLSw fails to set up circuit using UDP with peer-on-demand
CSCte68677	Management	PC behind C7941G does not get IP address when connected to 6500 switch
CSCtf61362	Management	Connsistent High CPU on cdp2.iosproc with steady traffic running
CSCtf03656	MPLS	Router crashes @ ip_route_delete after deleting vrf from interface.
CSCtf90182	MPLS	Traffic drop of more than 80sec after multiple SSO with 1PW configured
CSCti08115	MPLS	config-sync failure due to deleted idb with mpls ldp advertise-labels
CSCti53167	MPLS	ION: crash in hw_api_vrf_platform_capability from is_pervrfaggr_enabled
CSCti54908	MPLS	TE-LM leaks bandwidth when Resv's bw not same as Path's bw
CSCsy00657	Multicast	Bus error crash after PIM neighbor DR change
CSCtf74238	Multicast	crash with ip multicast ip multicast boundary command
CSCtg91572	Multicast	duplicate mcast traffic due to non-DR sending PIM join

Identifier	Technology	Description
CSCth02725	Multicast	Sending PruneEcho message incorrectly, without changing source IP addr
CSCth38699	Multicast	Auto-RP for multicast triggers RP-Discovery with 0 RPs
CSCth36280	QoS	Drop rate for parent hierarchical shaping policy is incorrect
CSCeh32332	Routing	rip lost interface when transmitted-interface flapping
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
CSCsk56788	Routing	High CPU Proces='BGP Router',when remote neighbor router bgp not active
CSCsu88191	Routing	Cannot remove static route when a similar one is pointing to an intface
CSCsx22124	Routing	CnH: static ip route does not take effect until reconfigured again
CSCta23373	Routing	Eigrp packet size more than ip mtu of gre tunnel
CSCtb98722	Routing	Memory leak on eigrp_timer_init
CSCtc25791	Routing	EIGRP crash when issuing relevant "show" cmd while removing EIGRP config
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
CSCtf33336	Routing	Offset-list access-list set to 0 in rip configuration.
CSCtf64231	Routing	Inbound route-map change shouldn't be effective immediately
CSCtg01873	Routing	EIGRP summary inherits manually set AD from more specific summary
CSCtg18726	Routing	Network (type-2) LSA is not generated for new interface.
CSCtg27206	Routing	Static route not redistributed by RIP after link flap
CSCtg37404	Routing	RPPREFIXINCONST error comes up continuously due to checksum error
CSCtg54878	Routing	All static routes are not installed in route table
CSCth03694	Routing	C4HD1: Standby keeps reloading due to ISSU incompatibility after reload
CSCth05272	Routing	ISIS/LB removes one route after TE FRR failover and recovery
CSCth09200	Routing	4948 crashes with "show bgp all peer-group xyz sum" command
CSCth20144	Routing	clear ip route with a /31 address breaks arp table
CSCth46888	Routing	VRRP master sends ARP request with non local MAC as Source
CSCth74576	Routing	NSF for EIGRP is not configurable in the IPBASE images for SXI4
CSCth84995	Routing	Crash at fibidb_subblock_message doing issu runversion
CSCth89352	Routing	redistributed static is deleted from rip db when interface down
CSCti10518	Routing	Potential memory leak in ipigrp2_redist_process
CSCti20690	Routing	Request for show running config without displaying ACL configs
CSCti30149	Routing	soft-reconfig route not removed from RIB
CSCti32742	Routing	DSGS4: Stand-by is reloading continuously with Virtual-TokenRing1 int
CSCti61949	Routing	Chunk corruption with MDT enabled VRF
CSCti67102	Routing	Tunnel disables due to recursive routing; holddown timer expires
CSCtj00039	Routing	EIGRP:some prefixes are not being passed from PE to CE router

Identifier	Technology	Description
CSCtj25775	Routing	Default route redistribution from bgp to rip with wrong metric
CSCtj32574	Routing	Deleting redistribute command into eigrp doesn't get synced to stdby
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
CSCtj88224	Routing	Effect of CSCsu96698's improvement "no bgp aggregate-timer" at SRD4
CSCtj99048	Routing	NSF: type-5 lsa remains even after type-7 becomes unroutable v3 and v2
CSCtk16643	Routing	EBGP EBGP Dynamic neighbor not up in multihop scenarios
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'
CSCed66047	Security	CRYPTO sems inadequately documented
CSCek43562	Security	Not able to close the SSH connection from third party SSH client package
CSCek44782	Security	Double free within mtree code on malloc failure
CSCek57606	Security	set peer <fqdn> dynamic should not resolve for each ACL entry
CSCsa99387	Security	crypt ca truspoint with two-word name disappears after router reload
CSCsb40163	Security	TCP SYN packet from an async interface may fail encapsulation with CBAC
CSCsb85643	Security	Frgmented IP packets fails b/w Linux Cisco sw vpnclient and IOS ipsec
CSCsc56040	Security	IPSEC router failed to coalesce pak - With certain crypto ACL's
CSCsd64304	Security	Router crashing while importing certificate:crypto pki import msca-root
CSCse42951	Security	Spurious memory access detected during CA enrollment
CSCsg92744	Security	IOS SSH client does not display refuse-message when line busy
CSCsi24939	Security	software forced crash at strncmp after 'crypto ca authenticate'
CSCsi67268	Security	Memory leak in Crypto IKMP process when using certificate authentication
CSCsk25491	Security	Bus error crash at mgd_timer_propagate_dbg_info
CSCsm27467	Security	switch crashes if kron used to copy over config via scp
CSCsq47980	Security	Router Crashes @process_run_degraded_or_crash while testing OCSP
CSCsz05583	Security	crypto pki config nvgened before ip config on which it depends - slow
CSCsz97833	Security	PKI: CRL requests get corrupted
CSCtg11808	Security	VSS: Standby supervisor reloads when crypto pki trustpoint removed
CSCtg84011	Security	mac-address on SVI does not work for EIGRP hello packets
CSCth79917	Security	AAA Banner not displayed for a SSH login session
CSCti26768	Security	Bus error while re-configuring a trustpoint
CSCte91471	WAN	NTP v4 takes several hours to sync when multiple servers are configured
CSCtf03928	WAN	NTP packets received but ignored by the NTP process
CSCtf88705	WAN	NTP sync fail after change of interface ip.
CSCth66604	WAN	Modify Action routines of few cli's for ISSU compatibility

Identifier	Technology	Description
CSCti42915	WAN	Interoperability test for NTPv4 and NTPv3 using authentication
CSCti46834	WAN	NTP sync problem with satellite link
CSCti82141	WAN	ntp pps-discipline CLI gets removed after reload when inverted included
CSCtj69886	WAN	NTP multicast mode not working over MVPN
CSCtk10401	WAN	Local log archive shows 'ntp authentication-key 1 md5 pwd' in clear text
CSCtn07728	WAN	ntp_ipv6 subsystem missing in SUP720 Lanbase image