Caveats in Release 12.2(18)SXE and Rebuilds

Open Caveats in Release 12.2(18)SXE and Rebuilds

Identifier	Technology	Description
CSCsa87178	QoS	violate-action policed-dscp-transmit defaulted to Drop after bootup
CSCee25454	Unknown	SADB peering process leaks memory after overnight test
CSCeh52330	Unknown	SPA-CT3: EFC Parity Error reported by SPA FPGA
CSCsa57222	Unknown	Intermittent RP Crash seen with maximum mflow plcrs

Resolved Caveats in Release 12.2(18)SXE6b

Resolved Infrastructure Caveats

- CSCsc64976—Resolved in 12.2(18)SXE6b

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

  Cisco will be making free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20051201-http.html

Resolved LegacyProtocols Caveats

- CSCsf28840—Resolved in 12.2(18)SXE6b

  A vulnerability exists in the Data-link Switching (DLSw) feature in Cisco IOS where an invalid value in a DLSw message could result in a reload of the DLSw device. Successful exploitation of this vulnerability requires that an attacker be able to establish a DLSw connection to the device.

  There are workarounds available for this vulnerability.

This advisory is posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20070110-dlsw.html

Resolved Management Caveats

- CSCsf07847—Resolved in 12.2(18)SXE6b

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

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

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

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

Resolved Security Caveats

- CSCsb12598—Resolved in 12.2(18)SXE6b

  Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

  Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

  Cisco IOS is affected by the following vulnerabilities:

  - Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
  - Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
  - Processing Finished messages, documented as Cisco bug ID CSCsd92405

  Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

  This advisory is posted at http: //www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml

  Note: Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link:
  http://www.cisco.com/en/US/products/csa/cisco-sa-20070522-crypto.html

  A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link:
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-crypto.

Other Resolved Caveats in Release 12.2(18)SXE6b

Identifier	Technology	Description
CSCsg70355	Infrastructure	adopt new default summer-time rules from Energy Policy Act of 2005.
CSCse78963	Infrastructure	adopt new default summer-time rules from EPA BADCODE BUG
CSCse04560	IPServices	tftp-server allows for information disclosure .
CSCsd92405	Security	router crashed by repeated SSL connection with malformed finished messag

Identifier	Technology	Description
CSCsg36726	Unknown	Bonham parity errors may cause packet loss on a 7600-SIP-400 module.
CSCsd44517	Unknown	flow control needs to be toggle off/on to become active after no shut

Resolved Caveats in Release 12.2(18)SXE6a

Resolved Infrastructure Caveats

- CSCsf04754—Resolved in 12.2(18)SXE6a

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

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

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

  This advisory will be posted at

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

Resolved Unknown Caveats

- CSCsd75273—Resolved in 12.2(18)SXE6a

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

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

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

- CSCse52951—Resolved in 12.2(18)SXE6a

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

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

  A Cisco Security Advisory for this vulnerability is posted at

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

Resolved Voice Caveats

- CSCsc60249—Resolved in 12.2(18)SXE6a

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

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

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

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

  This advisory is posted at

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

Other Resolved Caveats in Release 12.2(18)SXE6a

Identifier	Technology	Description
CSCek44025	QoS	Hierarchy is not collapsed when FRF.12 is configured
CSCse73539	Unknown	c7600 - crash of active sup720 after inserting a second one

Resolved Caveats in Release 12.2(18)SXE6

Resolved LAN Caveats

- CSCsd34759—Resolved in 12.2(18)SXE6

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

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

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

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

  These vulnerabilities are addressed by Cisco IDs:

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

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

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

Resolved Routing Caveats

- CSCsd40334—Resolved in 12.2(18)SXE6

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

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

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

  This advisory is posted at

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

Resolved Unknown Caveats

- CSCsd68605—Resolved in 12.2(18)SXE6

  Symptoms: If a spoke cannot complete IKE phase I because of a bad certificate, the failed IKE sessions may not be deleted on an IPSec/IKE responder. Such failed sessions may accumulate, eventually causing router instability. These failed sessions can be seen in the output of the **show crypto isakmp sa | i MM** command:

```
172.18.95.21    10.253.34.80   MM_KEY_EXCH        898    0 ACTIVE
172.18.95.21    10.253.34.80   MM_KEY_EXCH        896    0 ACTIVE
172.18.95.21    10.253.34.80   MM_KEY_EXCH        895    0 ACTIVE
172.18.95.21    10.253.34.80   MM_KEY_EXCH        894    0 ACTIVE
172.18.95.21    10.253.34.80   MM_KEY_EXCH        893    0 ACTIVE
...
```

  Conditions: These symptoms are observed when RSA signatures are used as the authentication method.

Other Resolved Caveats in Release 12.2(18)SXE6

Identifier	Technology	Description
CSCsb11698	AAA	Input Queue Wedge with TACACs
CSCsb12329	ATM	ifAdminStatus of ATM sub-interface is down without shutdown command
CSCef11195	Infrastructure	MIPS platforms take Address Error Exception in malloc()
CSCei32102	Infrastructure	Need an option to disable snmp traps for link during switch failover
CSCeg61169	IPServices	Traceback recorded in tcb_isvalid by TCP Remote Shell Process .
CSCeh35083	IPServices	NAT-PPTP change Call ID wrongly
CSCsd80754	IPServices	HSRP Active-Router not respond to ARP request about VIP
CSCsd34855	LAN	VTP update with a VLAN name >100 characters causes buffer overflow .
CSCsd94687	LAN	sh vlans counters and SNMP counters are incosistent for subif
CSCsd41981	MPLS	TFIB on SUP720 PFC is broken when an OSM (GE-WAN) card was disabled
CSCsb76434	Multicast	PIM: auto-rp group stuck in registering when sparse-mode
CSCse05336	platform-76xx	Packet drop on OSM-2+4GE-WAN+ if sub-if is created or deleted
CSCeh62084	PPP	ifStackStatus drops ifIndex when interface is OperStatus down

Identifier	Technology	Description
CSCsd71119	QoS	ALL ATM PVC DOWN IN FLEXWAN WITH PA-A3-OC3 AND OAM
CSCed87897	Routing	sh ip route missed default gateway after ip default-net command
CSCef11304	Routing	MIB walk on OSPF-MIB involving ospfExtLsdbTable crashes switch
CSCef35386	Routing	BGP does not inform PIM of the second best VPNv4-MDT
CSCeg07274	Routing	BGP IO process uses excessive CPU during convergence
CSCeg52659	Routing	BGP route may not get withdrawn under rare condition
CSCeg77104	Routing	EIGRP neigh over ATM IMA link flaps due to Authentication failure
CSCei26899	Routing	LSNT:Missing prefixes after card reload
CSCsa81039	Routing	EIGRP PE-CE:routing loop when a prefix has no cost-community
CSCsc73436	Routing	BGP: touching neighbor policies causes peer's table version to reset
CSCsc76327	Routing	EIGRP PE-CE: Constant route-flap with a redistributed VRF-static-route
CSCsd03882	Routing	SUP720 RACL Deny ACE not being implemented
CSCsd12904	Routing	OSPF sham-links do not come up
CSCsa63387	Security	Router may crash when CRL expires
CSCsc72722	Security	CBAC - firewall resets TCP idle timer upon receiving invalid TCP packets
CSCsd43903	Security	Memory leak in Crypto IKMP process when using certificate authentication
CSCse11457	Security	show crypto ca timers shows static output
CSCse12154	Security	Bus error crash after executing secure copy (scp)
CSCee34346	Unknown	%EARL-SP-4-EBUS_SEQ_ERROR: Out of Sync error. Errorcode 0x4C10020
CSCeh21210	Unknown	MF: DHCP Snooping crash when server send invalid option 82
CSCeh78411	Unknown	Failed IKE sessions does not get deleted in certain conditions
CSCei06406	Unknown	Ping failure/Wrong C-Shim Hdr on Serial Intf. removed from MLP
CSCei27448	Unknown	Router crashes while displaying sh ip pim mdt bgp
CSCek26186	Unknown	ATM SPA: setup vp fails.
CSCek42027	Unknown	SPA FPD upgrade fails with sip1-CR
CSCin98448	Unknown	controller shut throws up error msg and remote end is not going down
CSCsa85229	Unknown	CPUHOGs and watchdog timeout at earl_well_known_adj
CSCsa86954	Unknown	PortSec adds specific addr to secure table when rx cdp packet.
CSCsa87388	Unknown	cat6000 : ciscoEnvMonTempStatusChangeNotif to many traps - VDB inlet
CSCsb18740	Unknown	High cpu utilisation with heavy WCCP-redirected traffic
CSCsb33258	Unknown	RP crash while mvpns come up - MDFS buildup
CSCsb80141	Unknown	IOS-SLB: no mls ip slb search icmp does not work.
CSCsb91644	Unknown	IPv6 MFIB entry is updated on RP and delayed to update MFIB on SP & DFC
CSCsc24102	Unknown	Fabric sync errors if WS-X6704-10GE is on slot 4 on 7606
CSCsc43862	Unknown	SPA ping failure caused by SIP-200 serial primary channel sync failure
CSCsc65256	Unknown	Connection Count incorrect after ungraceful disconnect/reconnect
CSCsc75381	Unknown	Native vlan mismatch is not detected if native not allowed on trunk .

Identifier	Technology	Description
CSCsc91075	Unknown	IPSEC Connection Count incorrect after unsuccesfull connection attempt
CSCsc92114	Unknown	Port Power Mismapped On 6148-rj21AF
CSCsd05513	Unknown	7600 CBQOS-MIB is missing info which is present in CLI
CSCsd14307	Unknown	PA-MC-8TE1+ PA shows alarm led red even with all controllers shut down
CSCsd19203	Unknown	SIP400:ATM:new LLQ traffic stop flowing on dynamic changes to Policy
CSCsd25532	Unknown	High SP-CPU utili occurs when c7600 recieves IPv6 Multicast traffic
CSCsd33647	Unknown	ER: Improve C2 MET programming under heavy traffic scenarios
CSCsd45167	Unknown	Memory leak in Crypto IKMP Process
CSCsd49723	Unknown	Memory leak in Crypto IKMP Process when using certificate authentication
CSCsd49767	Unknown	Memory leak in Crypto IKMP process
CSCsd56549	Unknown	GRE doesnt get the same port that it req, PPTP change Call ID wrongly
CSCsd58552	Unknown	cwpa2: TCP to NAT addresses cause FR encap change from IETF to cisco
CSCsd90501	Unknown	Minimum/Maximum WRED thresholds for default DSCP stays at 32/64
CSCsd94541	Unknown	Multiple T3 controllers bounce on the SPA
CSCsd98887	Unknown	SP Memory Leak In mls-msc Process
CSCse15728	Unknown	VPNSM does not perform invalid spi recovery in vrf mode

Resolved Caveats in Release 12.2(18)SXE5

Resolved AAA Caveats

- CSCed09685—Resolved in 12.2(18)SXE5

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

  Conditions: This problem happens only with command accounting enabled.

  Workaround: Disable command accounting.

Other Resolved Caveats in Release 12.2(18)SXE5

Identifier	Technology	Description
CSCeg62070	Infrastructure	Tracebacks noticed with Radius configs through HTTP Post
CSCeh62781	Infrastructure	%IPC-5-WATERMARK FAST.control.RIL(2070000.E) seat 2070000
CSCej08355	Infrastructure	Memory corruption on MSFC with syncnlmTable
CSCsb22489	Infrastructure	supervisor crashes on removal of IP VRFs in VRF-LITE config
CSCsc08741	Infrastructure	Sup720 may experience Memory leak in *Dead*/Parser-Mode History Table pr
CSCsc44237	Infrastructure	memory leak in client applications iterating over an empty idb list
CSCsc82214	Infrastructure	Bus error crash at SrCheckClassMIBView
CSCsb16512	MPLS	High CPU in CEF Process and CEF scanner due to prefix reresolve

Identifier	Technology	Description
CSCei13579	Multicast	consolidation of some post-reload PIM blackhole issues
CSCek26627	Multicast	CPUHOG when RPF change affects ~30k mroutes
CSCsb23433	Multicast	Need to minimize mcast packet loss with intermittent sources
CSCsb64585	Multicast	RP is down but multicast routing continues to work
CSCsc16148	Multicast	Allow (S,G) expiry timer to be configurable
CSCsc73288	platform-76xx	OSM asic error:SRIC packet data CRC error
CSCin44386	PPP	Multilink interface flaps after a router reload
CSCsa56959	PPP	Show policy output counters not updated for process swiched packets
CSCsb74603	PPP	Router generated traffic does not match output policy
CSCsb97950	PPP	dLFIoATM: Packets with CLP set, get punted to RP.
CSCee58986	QoS	fair-queue nvgen does not happen
CSCsb36818	QoS	Service policies lost on interface bw reconfiguration
CSCsc25204	QoS	Divide by zero at udivmoddi4 when using the show policy-map command
CSCsc95511	QoS	Bus error crash at hqf_scheduler_info_init
CSCea34586	Routing	Bus error crash in ip_arp_merge process
CSCef61721	Routing	IPv6 CEF incorrect entry
CSCeh16989	Routing	BGP number of attributes is constantly increasing, consuming more memory
CSCeh53906	Routing	Stale non-bestpath mpath stuck in RIB with soft-reconfiguration
CSCei07805	Routing	PP:R3:SUP3:FIBDISABLE w/ 500 vrf and 200 IPv6 routes after SSO
CSCei53226	Routing	BGP: fix updgrps for non private-as peers with remove-private-as
CSCei75375	Routing	OSPFv3: Router crashes when area deleted
CSCsa79783	Routing	Loosing routes after reload/OIR when ispf enabled
CSCsa87473	Routing	BGP:MPLS/VPN: After reload PE missing prefixes from RR.
CSCsb09852	Routing	BGP: pathless nets not freed when updgrp members are out of sync
CSCsb24535	Routing	clear ip bgp update-group [ip address] clears all the bgp peers
CSCsb36550	Routing	CPUHOG by OSPF Router process
CSCsb37553	Routing	IPv6 : nexthop address inaccesible after clear bgp ipv6 nei soft
CSCsb40115	Routing	BGP: Failed to find expected # of multipath entries
CSCsb80866	Routing	PE global IP address shows up in traceroute VRF
CSCsc03828	Routing	OSPF continues to advertise a def route to NSSA w/no default route in RT
CSCsc50692	Routing	Global static route w/ non /32 mask to vrf loopback is unroutable
CSCsa67272	Security	Serial number in certificate subject is incorrect
CSCsc52105	Security	ipsec may leak Crypto IKMP memory blocks
CSCee84918	Unknown	DHCP snooping on 3550 drops DHCPNAKs recieved when renewing old IP
CSCee86692	Unknown	LAN-to-LAN tunnel doesnt get established with DPD configured
CSCee93598	Unknown	LSP ping/trace explicit null shimming capability
CSCeg39518	Unknown	Infinite loop on dsx1FarEndIntervalIndex

Identifier	Technology	Description
CSCeh17756	Unknown	ASSERT may not function properly with dual PEs and CEs
CSCeh49742	Unknown	sup720: NMI not working and show version has wrong reason
CSCeh80649	Unknown	SPA: Packets stop passing after T3 line flap
CSCei10218	Unknown	Cronos APS: APS states not getting sync in SSO
CSCei10228	Unknown	CHOC12/DS0 APS:LC power cycles with SSO s/o, APS state wrong on stdb
CSCei21293	Unknown	PP:R3:OC-48 ATM SPA: LC OIR causing traceback + %ENT_API-4-NOALIAS
CSCei22697	Unknown	mvpn tunnel is miss-matched to different VPN rte/fwd table
CSCei30764	Unknown	PP:R3:MVPN:multiple diff tunnels created on some VRFs
CSCei33598	Unknown	PP:R3:SIP-200:CT3 SPA:T3 contr stays down after remote router reload
CSCei37672	Unknown	chevys/c2lc take ~ 180s before resetting following a mandatory proc exit
CSCei38036	Unknown	layer 2 entry not removed when no int vlan
CSCei39181	Unknown	SIP200/POS-SPA:APS states not synced to standby in SSO
CSCei48635	Unknown	ChOC3/STM-1 SPA: many MFR interfaces remain down following microcode
CSCei61913	Unknown	PP R3:CHOC12/DS0 SSO:no shut not synced to stdby, traffic stop on HA
CSCei67673	Unknown	Memory leak during execute-on
CSCei80699	Unknown	multicast tunnel if_number numbers being duplicated
CSCei86192	Unknown	PP:R3:FlexWAN+PA-8xT1/E1: RP crashed MALLOCFAIL due to loveletter
CSCej21698	Unknown	EARL_L2_ASIC- SRCH_ENG_FAIL/ SCHED-DFC9-3-STILLWATCHING
CSCej57810	Unknown	ifOperStatus for Control Plane Interface is always down
CSCej78055	Unknown	Patch CSCei31646,CSCei19659 and CSCej25957 to SXE4 LATEST
CSCej87462	Unknown	SNMP set not-in-service to crcERSpanIFEntry corrupts mem
CSCek03772	Unknown	zamboni: crashes for double fragmentaion
CSCin96328	Unknown	Switching fails with sip-200 reset followed by sup switchover
CSCsa70494	Unknown	TX Chnl Queue Overflow events on freedm with traffic + router reload
CSCsa80620	Unknown	ct3 spa: serial interface efc queue stuck on deleting/adding mlp bundle
CSCsa83541	Unknown	qm_chkpt_add_plcr_to_label msg seen on standby on applying policy
CSCsa85123	Unknown	Cisco 7609 :OSM-1CHOC12DS0-SI :RFI bit should be undefined for VC-12
CSCsa85752	Unknown	H/w entry creation for SSM over GRE Tunnel toggles cont. after reload
CSCsb00473	Unknown	CT3: Scaled config in T1 SF mode fails
CSCsb01861	Unknown	cat6000: 'mls acl tcam default-result permit' command is broken
CSCsb08512	Unknown	SCP subcmd SUBCMD_GET_LTLS_FOR_INDEX_RANGE response is corrupted
CSCsb11224	Unknown	system crashes soon after changes in cos-mutation map
CSCsb12969	Unknown	MQC: Router crashes when a service-policy is added to atm or FR pvc
CSCsb15156	Unknown	Missing MAC addr cause LDP flap after switchover if explicit-null set
CSCsb31368	Unknown	ATM Multipoint bridging on c65xx is broken after SW upgrade
CSCsb34213	Unknown	Few destination ports removed from RSPAN vlan flood index after SSO
CSCsb38396	Unknown	No traffic passes out MFR sub ints after shut / no shut on 1xCHOC3/ChSTM

Identifier	Technology	Description
CSCsb46887	Unknown	MET entry misprogrammed due to high rate of multicast traffic
CSCsb49326	Unknown	Cat6K crashes after EPLD upgrade of WS-X6548-GE-TX
CSCsb50559	Unknown	Need fix for MWAM for CSCee10005
CSCsb54233	Unknown	ISIS hello not rcved on dot1q sub interface on a WS-X6582-2PA
CSCsb62566	Unknown	Add an option to power-down the LC when fabric error is detected
CSCsb66799	Unknown	URL match statement removed from configuration after reload
CSCsb67152	Unknown	MET inconsistent on DFC, multicast traffic is blackholed for an OIF
CSCsb70996	Unknown	IOS SLB drops trailing fragments in VRF and misroutes SLB msgs to GGSN
CSCsb79031	Unknown	Clear counter caused the MSFC to reload the SUP due to RPC timeout
CSCsb80590	Unknown	Enhance IPC buffer usage and IOMEM buffer allocation for Flexwan
CSCsb84746	Unknown	Memory leak ed at qm_process_enqueue/qm_mqc_mesg_to_process
CSCsb85049	Unknown	cwpa2 bridged/routed ATM PDUs lost between Flexwan2 and SUP720
CSCsb85589	Unknown	enable explicit-null cause ldp keeps flapping after switchover
CSCsb89241	Unknown	BRE LTL is not populated properly after reload for flexwan2
CSCsb98702	Unknown	Breakpoint (signal 5 exception) when ltl profiling .
CSCsc00603	Unknown	Sup22 :uRPF check is disabled globally when disabled on any single i/f
CSCsc03429	Unknown	JQL: Linecard in the slot for SUP reloaded by changing redundancy mode
CSCsc03864	Unknown	Service Module sourced packet dropped when recirculation required
CSCsc04015	Unknown	cbQosCMStatsTable doesn't return byte statistic for FastEthernet PAs
CSCsc05210	Unknown	Incoming dscp not trusted after upgrading from 12.2SXD to 12.2SXE
CSCsc05500	Unknown	ENTITY-MIB: SFP in Gi1/1 is not displayed in show inventory
CSCsc05838	Unknown	Changing Sticky Cookie from Dynamic to Insert will corrupt sticky table
CSCsc06620	Unknown	Memory corruption when span session is removed from service module
CSCsc07793	Unknown	Stdby sup reloads after setting stpxMSTInstanceEditVlansMap
CSCsc13720	Unknown	llq functionality with _match input vlan_ broken
CSCsc26048	Unknown	Cat6k: CPUHOG in PIM Snooping Process
CSCsc26490	Unknown	wrong static mac address entry in case of GLBP virtual mac
CSCsc32198	Unknown	IGMP per-port leave with multiple leave nested cases disturbs mcast strm
CSCsc33990	Unknown	Enhancements and Optimizations to TestSPRP InbandPing
CSCsc52306	Unknown	IDSM: span tree not blocking when two IDSM in inline mode
CSCsc52645	Unknown	SIP1-CT3: Whole T1 goes down while doing timeslot BERT on CT3 SPA
CSCsc55949	Unknown	C2 Frequent fabric channel sync errors and rxErrors
CSCsc57156	Unknown	Hardware fault on FWSM ports not causing FWSM redundancy failover
CSCsc59207	Unknown	IKE SAs not replicating to standby chassis
CSCsc61086	Unknown	TCAM entry optimization needed for NAT outside i/fs with big NAT cfg
CSCsc61257	Unknown	Software watchdog timeout in Active-SP causes both sups to crash/reload.
CSCsc68250	Unknown	Packet flow halt on 7600-SIP-400

Identifier	Technology	Description
CSCsc88725	Unknown	SPRP ping not triggering the recovery action if only one FIBTCAM device
CSCsc89044	Unknown	IO memory leak with big buffers and EOBC0/0
CSCsc93283	Unknown	R2.5: no mls qos mpls trust exp CLI not effective after reload
CSCsc93607	Unknown	R2.5:RP crash when del service policy after del no mls qos mpls tr exp
CSCsc94266	Unknown	Memory corruption due to Corrupted previous pointer
CSCsc95559	Unknown	R2.5: policy trust effective tho no mls qos mpls tr exp is not config
CSCsd15806	Unknown	r2.5:Tcam is not programmed after shut/no shut on interface
CSCsd20092	Unknown	Device crashes with fabric error on bootup starting from 28th build
CSCeg47659	WAN	cRTP packet drops with Enhanced Flexwan
CSCeh48548	WAN	ntp doesnt sync over reconfigured channel-groups
CSCin46297	WAN	show aps shows different status on the master and slave
CSCsb67941	WAN	PA-8T-V35 - MFR config remains even if PA is removed
CSCsd04219	WAN	Add feature support for ACLs in 12.2SXE on virtual templates

Resolved Caveats in Release 12.2(18)SXE4

Resolved Routing Caveats

- CSCin95836—Resolved in 12.2(18)SXE4

  The Cisco Next Hop Resolution Protocol (NHRP) feature in Cisco IOS contains a vulnerability that can result in a restart of the device or possible remote code execution.

  NHRP is a primary component of the Dynamic Multipoint Virtual Private Network (DMVPN) feature.

  NHRP can operate in three ways: at the link layer (Layer 2), over Generic Routing Encapsulation (GRE) and multipoint GRE (mGRE) tunnels and directly on IP (IP protocol number 54). This vulnerability affects all three methods of operation.

  NHRP is not enabled by default for Cisco IOS.

  This vulnerability is addressed by Cisco bug IDs CSCin95836 for non-12.2 mainline releases and CSCsi23231 for 12.2 mainline releases.

  This advisory is posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20070808-nhrp.html.

Resolved Unknown Caveats

- CSCsb52717—Resolved in 12.2(18)SXE4

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

  Conditions: Affects all IOS versions that support mVPN MDT.

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

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

  ```
  !
  ```

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

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

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

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

Other Resolved Caveats in Release 12.2(18)SXE4

Identifier	Technology	Description
CSCei51155	Access	PP:R3:PA-MC-2T3+: Saturation rate drop 50% due to input overrun
CSCsb21867	Access	PA-MC-8TE1+ in Flexwan: ctrlr detects LOS after restart does not recover
CSCdw25402	ATM	RPM-PR card crashed when provisioning bulk connections from CWM
CSCsb44308	Infrastructure	Cat6k crashes with no snmp-server
CSCds33629	IPServices	Closing Telnet session crashes router..
CSCeg06261	IPServices	Cat4000: Active FTP fails with 12.2(20)EWA
CSCeh48684	IPServices	Identification field is 0 in every tacacs packet with SYN
CSCsb15224	IPServices	HSRP: wrong HSRP mac addr in ARP reply if multiple HSRP groups are used
CSCec64333	Management	Memory leak in SNMP ENGINE while retrieving ciscoIPSEC MIBS
CSCsb09190	MPLS	Next-hop label missing for non-vpn prefixes with dual RRs
CSCsb32695	MPLS	PE lost aggregate label after shut/no-shut
CSCeh93087	Multicast	Need triggered Bidir RP Cache update
CSCeh95160	Multicast	bi-directional PIM DF winner may receive an incorrect unicast metric
CSCsb02976	Multicast	MSDP: Need msdp RP non-dr to send triggered SA immediately
CSCsa93725	platform-76xx	MR-APS: Working router power cycle causes significant traffic loss
CSCsb15183	platform-76xx	OSM:Asic [0] error: TXIF: RXPB bad packet len (low)
CSCdt12296	QoS	RSVP Path message packets are process switched when data is CEF swit
CSCed71844	QoS	show policy interface locks up the c7500
CSCee56209	QoS	ACL counters double counting
CSCeh31441	QoS	Flexwan module powercycles with shaping+dLFIoATM
CSCsb01188	QoS	ATM interface on FW/FW2 PA stops tx on add/remove service policy
CSCsb25607	QoS	dLFIoFR: all lp pkts dropped on oversubscribed mixed traffic
CSCee01688	Routing	NAS crashes at ip2access_add_acl_item() while running stress test
CSCeh09588	Routing	300 second traffic loss with 100 OSPF neighbor after SSO switchover

Identifier	Technology	Description
CSCeh20051	Routing	RIPv2: some statics not redistributed in vrf using rip.
CSCeh92012	Routing	OSPF did not redistribute route expectedly
CSCej21891	Routing	crash in rip_update_dbase when default-information originate used
CSCin65241	Routing	ISIS: redistribute commands not being synced to standby RP
CSCsa50971	Routing	Access-list resequence command causes unexpected reload
CSCsa87034	Routing	clear bgp ipv4 unicast command does not clear Routing table
CSCsa95973	Routing	OSPF processes summaries from non-BB links after switchover on ABR
CSCsb08380	Routing	iSPF does not check existing route when attaching stub network
CSCsb69773	Routing	Router Crash with BGP at bgp_netlist_validate
CSCdy80670	Security	SCHED-3-THRASHING error messages in TTY Background process
CSCdz84448	Unknown	Spurious memory access when querying the cbQosREDClassStatsTable
CSCee01435	Unknown	show power command shows PS-Fan status as n/a
CSCef07048	Unknown	SecurID New PIN mode fails with VPN Client
CSCeg03733	Unknown	Sprious Alignment and crash with MIB walk in Cisco Class Based QoS
CSCeh35237	Unknown	7600: 6748GE LC OIR causes spurious mem access and traceback
CSCeh35849	Unknown	New PIN mode and next token code fail with vpn client
CSCeh41511	Unknown	PP::mls qos ip output broken for policy without drop action
CSCeh53682	Unknown	MACs Learned on EtherChannel across L2 Fwding Engine Get Off-sync
CSCeh55293	Unknown	Physical EVC to poch EVC conversion may fail if poch has no member
CSCeh61467	Unknown	Router crashes at pim_reset_updated_nbr on uncfging mdt group
CSCeh73049	Unknown	tclsh mode bypasses aaa command authorization check
CSCeh73110	Unknown	Ucast flooding due to +MN/-MN race condition
CSCeh81794	Unknown	chassis crash due to memory corruption
CSCeh87476	Unknown	show platform tech-support ipmulticast needs support for BiDir
CSCei01237	Unknown	SLB: %SYS-3-CPUHOG messages and crash running slb processes
CSCei02695	Unknown	PP:R3:SIP-200: BCP functionality is broken after linecard OIR
CSCei02826	Unknown	PP:R3:All VoIP(even UDP port) cRTP PKTs were dropped in input queue
CSCei09755	Unknown	SPA-CT3/CHOC-Serial intf line proto down after removing from bundle
CSCei16701	Unknown	PP:R3: SPA ATM/FR MPB: Failed to forward MCAST PKTs from SVI INTF
CSCei20107	Unknown	DFC3A reloaded due to sman interrupt after memory allocation failure.
CSCei20996	Unknown	MPLS-VPN:Ping packet doesnt go through with osm srp interface.
CSCei24139	Unknown	PP:R3:SIP-200: CPU 1 crash on doing linecard reset with ATM SPA
CSCei30999	Unknown	PP:R3:SIP-200 drops 30% of VoIP traffics on cRTP sessions
CSCei33393	Unknown	Drops on sup720 with certain queue-limit and WRED threshold values
CSCei37465	Unknown	After a firmware upgrade the firmware.cfg is corrupted
CSCei37692	Unknown	GTP SLB broken when <mls ip slb search wildcard rp> configured
CSCei41088	Unknown	MVPN Tunnel interface not created with BGP Confedetration

Identifier	Technology	Description
CSCei51175	Unknown	PP:R3:SIP-200:1490 bridging - CPU1 crash with egress pol on main int
CSCei52441	Unknown	default ACL programming not correct under certain condition
CSCei64940	Unknown	Service Module sourced packet dropped when recirculation required
CSCei76358	Unknown	cleanup of user interface data
CSCei80006	Unknown	Same Proxy, Multiple Peers, both RRI routes deleted
CSCei93397	Unknown	SPA-CTE1: Fails at configuration if HW version is 2.0 or greater
CSCin78325	Unknown	PA-MC-8TE1+ admindown serial interfaces continue to process packets
CSCin94752	Unknown	SLB crash in slb_probe_wc_install
CSCsa69060	Unknown	packets tagged with agg label not matched by CPP
CSCsa70274	Unknown	LSP trace crash when rx of dsmap with multipath length set to 0.
CSCsa76801	Unknown	Major bootup failure on Sup720 causing other linecards to PwrDown
CSCsa76812	Unknown	ICC gets stuck after reload if RM agiing is configured to no_aging
CSCsa77655	Unknown	System keeps crashing if PF_REDUN_CRASH_COUNT is not set properly
CSCsa80358	Unknown	Connectivity lost on native vlan on etherchannel trunk betn 2 cat6ks
CSCsa82640	Unknown	LSP ping/traceroute times out at untagged hop for MFI images
CSCsa82912	Unknown	CPUHOG for scp_lc_event_mgr on switchover of sup2
CSCsa91175	Unknown	no login authentication appears as default after vty is configured
CSCsa95287	Unknown	MIB OID csgQuotaMgrStats missing in the snmpwalk
CSCsa95660	Unknown	SP may crash if it follows some code path
CSCsb01086	Unknown	CSG: Newly configured VLAN not allowed on trunk until module reload
CSCsb02590	Unknown	Changing the RP bridge from 0x381 to 0x387
CSCsb03192	Unknown	VPNSMi:DMVPN: incorrect socket created in spoke after hub add changed
CSCsb04346	Unknown	crash l2_aging_proc after changing Spantree mode
CSCsb10662	Unknown	PI_E lost on Supervisror after +MN received on DEC with Plus
CSCsb12076	Unknown	VPN-SM: GRE RP pkts coming to IPSec with tvlan causing route flaps
CSCsb14175	Unknown	SLB real servers stay at MAXCONN after open/close IP PDP with sticky on
CSCsb14306	Unknown	GTP SLB may reload when gtp sticky unconfiged during PDP deletion
CSCsb16146	Unknown	FREEBAD: Bus error at ace_polo_send_hapi
CSCsb16396	Unknown	Unicast flooding with Shut on one of the DEC members
CSCsb16475	Unknown	Etherchannel throughput limited message with WS-X6548-GE-TX
CSCsb23906	Unknown	spurious memory accesses with 12.2(18)SXE1 in cwan_convert_mac_address
CSCsb24320	Unknown	PP:R3:VPLS+QoS:PWAN2: shaping queue is not created after bootup
CSCsb29783	Unknown	Cat6500 may crash if dot1x auth is disabled during authentication
CSCsb29951	Unknown	IEEE 802.1x authentication time is high (~150 sec for 270 supplicants)
CSCsb33744	Unknown	service-policy stops packets via MPLS / VPN
CSCsb34354	Unknown	netflow process hogs SP cpu even after netflow is disabled
CSCsb34985	Unknown	const_mpls_prog_vlan_recirc_adj: bad params vlan keep logged & CPU high

Identifier	Technology	Description
CSCsb36874	Unknown	DHCP packet corruption with snooping enabled
CSCsb37618	Unknown	GTP SLB: Doesnt relay create response to SGSN even after max reassigns
CSCsb38242	Unknown	LSP Traceroute shows no labels when last hop P is a 7600 12.2 18 SXE
CSCsb38273	Unknown	L3 Traffic flood over DEC due to incorrect Flood region FPOE
CSCsb38885	Unknown	RRI routes dont get deleted after VPNSM reload with HA configuration
CSCsb48015	Unknown	All bundle links do not recover following MFR bundle flap
CSCsb48739	Unknown	GTP SLB:Session reassigned even when sticky entry exists
CSCsb55343	Unknown	linkDown trap sent out for control plane interface when sys bootup
CSCsb60453	Unknown	Need improved logs for severe fabric errors which triggers fab swover
CSCsb70303	Unknown	CSM: CSM hang or both become active/active after rpr+ switchover
CSCsb70335	Unknown	Flexwan crash when fragmentation is enabled under MFR interface
CSCsb70973	Unknown	igmp snooping explicit tracking and report suppression issues
CSCsb71242	Unknown	MMLS NSF/SSO: Mcast Failover time very high for the first switchover
CSCsb77592	Unknown	7600/6500 crash by removing ACL tied with vpn configuration.
CSCsb77716	Unknown	dot1x:SP crash at sm_destroy_instance on OIR or link flap
CSCsb79590	Unknown	MST: designated port doesnt become boundary geting TC from other region
CSCsb84405	Unknown	dscp mutation not working after reload
CSCsb84998	Unknown	MLS-MSC ASSERTION FAILED with T/Bs after hw-module reset
CSCsb95851	Unknown	Cat6K crashing by bus error at msc_sc2vdb_unlink
CSCeg04325	WAN	CPUHOG in process = Serial Background
CSCeh97017	WAN	PP:R3:(FlexWAN+cRTP): show ip rtp header-compression fails to count
CSCsa43553	WAN	After RPR+ switchover, flexwans ingress traffic doesnt hit SLB
CSCsa80223	WAN	Error adding idb to macaddr idb list messages are logged on console
CSCsb09250	WAN	Flexwan - spurious accesses at cwpa_egress
CSCsb64812	WAN	Memory Leak Net Background process
CSCsb86675	WAN	Multicast Packets are forwarded out on down PVC on ATM Bundle

Resolved Caveats in Release 12.2(18)SXE3

Identifier	Technology	Description
CSCsb09190	MPLS	Next-hop label missing for non-vpn prefixes with dual RRs
CSCei76358	Unknown	cleanup of user interface data
CSCeh73049	Unknown	tclsh mode bypasses aaa command authorization check

Resolved Caveats in Release 12.2(18)SXE2

Resolved AAA Caveats

- CSCee45312—Resolved in 12.2(18)SXE2

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

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

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

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

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

Resolved Security Caveats

- CSCeb47225—Resolved in 12.2(18)SXE2

  If a key is configured on a tunnel interface, the inbound access-list on that interface is ignored.

  This problem is seen with a configuration that is similar to the following

```
interface Tunnel0
 ip address 192.168.1.1 255.255.255.0
 ip access-group 100 in
 tunnel source FastEthernet0/0
 tunnel destination 172.16.1.1
 tunnel key 1
end
```

  Problem does not occur if “tunnel key” is not configured.

  Workaround is to remove the “tunnel key”.

Other Resolved Caveats in Release 12.2(18)SXE2

Identifier	Technology	Description
CSCei12574	Access	MPLS-ATOM:FR:VC failed to come up after an OIR of some slot.
CSCsa82886	Infrastructure	RP crashes when argument for tftp-server command longer than 67 char
CSCsa98777	Infrastructure	Memory corruption on MSFC with syncnlmTable
CSCef87449	MPLS	RRR LM: Admin shut handler does not preempt LSPs
CSCeh05594	MPLS	MPLS-TE FRR: Router crash in tfib during FRR operation
CSCeh78455	MPLS	Interface description duplication on MPLS/LDP enabled int:ifAlias
CSCsa85588	MPLS	Per VRF Aggregate Label not in lfib
CSCeg83460	Multicast	c6msfc:bidir pim df not elected with multiple RPs after link down
CSCeh01390	Multicast	MSDP does not create (S,G) when IGMP modifies the (*,G) olist
CSCsb13441	platform-76xx	GE-WAN tag-switching MTU broken for RP handled packets again

Identifier	Technology	Description
CSCeh41652	PPP	Packet classification fails on MFR after RPR-Plus switchover
CSCeh54083	QoS	random-detect aggregate cmd not working for virtual-template
CSCsa57101	QoS	Crash in k_rsvpSenderEntry_get
CSCeh13489	Routing	BGP shouldn't propogate an update w excessive AS Path > 255
CSCeh61778	Routing	GRP crash by SYS-2-WATCHDOG in process IS-IS Update
CSCsa73843	Routing	DMVPN - Buffer leak due to delayed NHRP processing
CSCsa74271	Routing	OSPF NSF not working, traffic drops for a few seconds
CSCsa78259	Routing	IOS reload due to specific BGP routing update
CSCsa80861	Routing	BGP to IGP redistribution broken with mutual redistribution points
CSCsa98059	Routing	OSPF not flushing external LSA from BGP redist on route change
CSCsb18066	Routing	ip routing protocol purge interface does not work
CSCsa78580	Security	Crypto IKMP process can get blocked if router fails to fetch CRL
CSCsa81928	Security	CRL checking fails if PKI URI recevied for CDP is UPPER CASE
CSCee58827	Unknown	SLB crash with replicate slave enabled without replicate casa
CSCeh40945	Unknown	Same MAC addreees are learnt by different VLAN
CSCeh51894	Unknown	12.2SXE2: TestLoopback and TestInlineRewrite failed diags
CSCeh54217	Unknown	GTP-SLB should not reassign session when sticky object exists
CSCeh54533	Unknown	IOS SLB with Egress ACL under SVI breaks L2 icmp traffic
CSCeh56398	Unknown	T48+, G+-CR2 in C+/Legacy configuration boot with multiple errors
CSCeh56439	Unknown	ATM SPA may reject wred policy
CSCeh62351	Unknown	ALIGN-1-FATAL:Corrupted program counter. Show Tech cause router cash
CSCeh62522	Unknown	igmp snooping source only doesnt work for certain range of group ad
CSCeh65221	Unknown	VPNSM: Pkt looping to wmac
CSCeh65615	Unknown	Rockies2:TestL3VlanMet failed online diag on T48+
CSCeh71584	Unknown	7600 as dmvpn spoke does not work with VRFs
CSCeh82971	Unknown	Router crashed at watcher_delete_common during FPD upgrade
CSCei00856	Unknown	CWAN-QOS:oc-3:col2 crash with external memory address
CSCei16381	Unknown	Same MAC addreees are learnt by different VLAN
CSCei18018	Unknown	Diagnostics HM crash
CSCin78324	Unknown	PA-MC-8TE1+: check to drop runts packets missing in driver code
CSCin90971	Unknown	Enhanced FlexWAN FPD Package needs to be bundled with IOS image
CSCsa48259	Unknown	VPN-SM: rp crash triggered by crypto_ss_print_table
CSCsa70835	Unknown	SUp720 may see random packet loss when host leaves or joins; OIF +- 85
CSCsa77084	Unknown	IntMacRx-Err counts TX errors
CSCsa78705	Unknown	Memleak in l3_mgr_tunnel_is_hw_not_supported_internal after stress
CSCsa87127	Unknown	Some features using re-direct index fail on RPR+ switchover SSO working
CSCsa89917	Unknown	unable to change dot1x max-req vlaue and dot1x timeout tx-period

Identifier	Technology	Description
CSCsa90830	Unknown	WCCP ingress redirect in Mask assign/GRE mode not using ACL TCAM Adj
CSCsa91166	Unknown	GTP SLB : Cannot assign same sticky group to two different gtp vservers
CSCsa91749	Unknown	A router may reload when trying to free memory at clear_path_ids
CSCsa91816	Unknown	c6k sends notPresent Temperature StatusValue Value =0 trap
CSCsa94063	Unknown	Rockies2: Mroute Active Rate counter is not updated properly
CSCsb01729	Unknown	show platform tech-support ipmulticast command problems on EARL7
CSCsb09997	Unknown	Enhanced FlexWAN: dropping IS-IS 01:80:C2:00:00:14-15 packets as BPDUs
CSCsb10226	Unknown	DMVPN: rp crash trig by crypto_ss_print in the hub
CSCsb17320	Unknown	Mcast src-only timer does not work for configured timer intervals
CSCeh68965	WAN	large ospf packets truncated when f/r ietf

Resolved Caveats in Release 12.2(18)SXE1

Identifier	Technology	Description
CSCsa76290	Unknown	Inter-fabric throughput in MPLS CE to PE is much lower than 18SXD.