Caveats

Note

- All caveats in Release 12.2(18)S also apply to Release 12.2(18)SXD and later 12.2SX releases. See the "Caveats" section in the *Cross-Platform Release Notes for Cisco IOS Release 12.2S* publication:

  http://www.cisco.com/en/US/docs/ios/12_2s/release/notes/122Srn.html
- All caveats in Release 12.2(17d) also apply to Release 12.2(17d)SXB and rebuilds.
- All caveats in Release 12.2(17b) also apply to Release 12.2(17b)SXA and rebuilds.
- All caveats in Release 12.2(17a) also apply to Release 12.2(17a)SX and rebuilds.
- For information about Release 12.2(17a), Release 12.2(17b), and Release 12.2(17d), refer to this publication:

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_release_notes_list.html
- All caveats in Release 12.2(14)S also apply to Release 12.2(14)SX and later 12.2SX releases. See the "Caveats" section in the *Cross-Platform Release Notes for Cisco IOS Release 12.2S* publication:

  http://www.cisco.com/en/US/docs/ios/12_2s/release/notes/122Srn.html

Caveats in Release 12.2(18)SXF and Rebuilds

Note

- The caveat information for Release 12.2(18)SXF and rebuilds is updated frequently.
- Release 12.2(18)SXF2 includes all fixes that are in Release 12.2(18)SXF1, Release 12.2(18)SXE4, Release 12.2(18)SXD7, and Release 12.2(17d)SXB11.
- Release 12.2(18)SXF includes all fixes that are in Release 12.2(18)SXE3, Release 12.2(18)SXD6, and Release 12.2(17d)SXB10.
- If you have a Cisco.com account that supports access to the Bug Toolkit, you can search for the most current Release 12.2SX caveat information at this URL:

  http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs

Open Caveats in Release 12.2(18)SXF and Rebuilds

Identifier	Technology	Description
CSCin96568	Infrastructure	FTS-7514-1: CISCO-PROCESS-MIB support for modular IOS
CSCsb92309	Infrastructure	reimplementation of cache_interface_state under CSCdw09607
CSCsf03710	Infrastructure	ION - Process and Mempool MIB - collapse of ion_mibs_all branch
CSCee25454	Unknown	SADB peering process leaks memory after overnight test

Resolved Caveats in Release 12.2(18)SXF17b

Resolved Infrastructure Caveats

- CSCti25339—Resolved in 12.2(18)SXF17b

  Symptoms: Cisco IOS device may experience a device reload.

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

  Workaround: There is no workaround.

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

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

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

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

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

Resolved LegacyProtocols Caveats

- CSCtf74999—Resolved in 12.2(18)SXF17b

  Summary A router configured for DLSw might crash when it receives a series of certain malformed packets. This issue requires a number of conditions and a narrow timing window.

  Conditions: Cisco IOS devices configured for DLSw.

  Workaround: The only workaround in the device is to disable DLSw if not needed.

  Additional mitigations can be found in the following Applied Mitigation Bulletin: http://tools.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20080326-dlsw

  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 5.4/4.5:

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

  CVE ID CVE-2011-1625 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

- CSCth69364—Resolved in 12.2(18)SXF17b

  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 WAN Caveats

- CSCtd75033—Resolved in 12.2(18)SXF17b

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

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

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

  Cisco has release a public facing vulnerability alert at the following link: http://tools.cisco.com/security/center/viewAlert.x?alertId=19540

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

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

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

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

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

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

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

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

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

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

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

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

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

Additional information about Cisco IOS Software release naming conventions is available in “White Paper: Cisco IOS and NX-OS Software Reference Guide” at the following link: http://www.cisco.com/web/about/security/intelligence/ios-ref.html

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

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

– NTP Access Group

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

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

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

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

– Infrastructure Access Control Lists

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

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

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

```
!---
!--- Feature: Network Time Protocol (NTP)
!---
access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
INFRASTRUCTURE_ADDRESSES WILDCARD eq 123
!--- Note: If the router is acting as a NTP broadcast client
!--- via the interface command "ntp broadcast client"
!--- then broadcast and directed broadcasts must be
!--- filtered as well. The following example covers
!--- an infrastructure address space of 192.168.0.X
access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD host 192.168.0.255 eq
ntp access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD host
255.255.255.255 eq ntp
!--- Note: If the router is acting as a NTP multicast client
!--- via the interface command "ntp multicast client"
!--- then multicast IP packets to the mutlicast group must
!--- be filtered as well. The following example covers
!--- a NTP multicast group of 239.0.0.1 (Default is
!--- 224.0.1.1)
access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD host 239.0.0.1 eq ntp
!--- Deny NTP traffic from all other sources destined
!--- to infrastructure addresses.
access-list 150 deny udp any INFRASTRUCTURE_ADDRESSES WILDCARD eq 123
!--- Permit/deny all other Layer 3 and Layer 4 traffic in
!--- accordance with existing security policies and
!--- configurations. Permit all other traffic to transit the
!--- device.
access-list 150 permit ip any any
!--- Apply access-list to all interfaces (only one example
```

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

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

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

– Control Plane Policing

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

– Filtering untrusted sources to the device.

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

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

```
!--- Feature: Network Time Protocol (NTP)
access-list 150 deny udp TRUSTED_SOURCE_ADDRESSES WILDCARD any eq 123
!--- Deny NTP traffic from all other sources destined
!--- to the device control plane.
access-list 150 permit udp any any eq 123
!--- Permit (Police or Drop)/Deny (Allow) all other Layer3 and
!--- Layer4 traffic in accordance with existing security policies
!--- and configurations for traffic that is authorized to be sent
!--- to infrastructure devices
!--- Create a Class-Map for traffic to be policed by
!--- the CoPP feature
class-map match-all drop-udp-class match access-group 150
!--- Create a Policy-Map that will be applied to the
!--- Control-Plane of the device.
policy-map drop-udp-traffic class drop-udp-class drop
!--- Apply the Policy-Map to the
!--- Control-Plane of the device
control-plane service-policy input drop-udp-traffic
```

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

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

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

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

```
access-list 150 permit udp any any eq 123
!--- Create a Class-Map for traffic to be policed by
!--- the CoPP feature
class-map match-all rate-udp-class match access-group 150
!--- Create a Policy-Map that will be applied to the
!--- Control-Plane of the device.
!--- NOTE: See section "4. Tuning the CoPP Policy" of
!--- http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html#5
!--- for more information on choosing the most
!--- appropriate traffic rates
policy-map rate-udp-traffic class rate-udp-class police 10000 1500 1500
conform-action transmit exceed-action drop violate-action drop
!--- Apply the Policy-Map to the
!--- Control-Plane of the device
control-plane service-policy input drop-udp-traffic
```

Additional information on the configuration and use of the CoPP feature can be found in: http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html

Further Description

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

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

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

Other Resolved Caveats in Resolved in 12.2(18)SXF17b

Identifier	Technology	Description
CSCsv82285	Unknown	Cat6k: UDP port 10000 is opened by default
CSCtd09117	Unknown	CSM config sync timing out

Resolved Caveats in Release 12.2(18)SXF17a

Resolved Multicast Caveats

- CSCtc68037—Resolved in 12.2(18)SXF17a

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

  Conditions:

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

Other Resolved Caveats in Resolved in 12.2(18)SXF17a

Identifier	Technology	Description
CSCei16552	Infrastructure	cannot remove snmp-server engineID from running-config
CSCsc33389	Infrastructure	When snmp-server host is deleted, the trap is not sent to other hosts
CSCsx32841	Infrastructure	ceImageDescription may exceed 255 characters

Identifier	Technology	Description
CSCsz72591	IPServices	Router configured as a DHCP client crashes with crafted DHCP packet.
CSCtc26840	IPServices	HSRP-CISCO-MIB snmpwalk results in "OID not incrementing" error
CSCsd91182	Security	crypto pki export pkcs12 hangs when used with SCP
CSCsx42304	Security	Traceback during SCP copy
CSCsc92676	Unknown	Rainier:Traffic captured even after vacl config is removed
CSCsu31088	Unknown	Not able to execute any commands under intf after running SPA FPGA bert

Resolved Caveats in Release 12.2(18)SXF17

Resolved Security Caveats

- CSCsh97579—Resolved in 12.2(18)SXF17

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

  Cisco has released free software updates that address this vulnerability.

  This advisory is posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20090923-tunnels.html.

- CSCsx70889—Resolved in 12.2(18)SXF17

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

  Cisco has released free software updates that address this vulnerability.

  This advisory is posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20090923-tunnels.html

- CSCsq31776—Resolved in 12.2(18)SXF17

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

  Cisco has released free software updates that address this vulnerability.

  This advisory is posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20090923-tunnels.html

Resolved Unknown Caveats

- CSCsy15227—Resolved in 12.2(18)SXF17

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

  There are no workarounds that mitigate this vulnerability.

  This advisory is posted at the following link:
  http://www.cisco.com/en/US/products/csa/cisco-sa-20090923-auth-proxy.html

Other Resolved Caveats in Release 12.2(18)SXF17

Identifier	Technology	Description
CSCin79116	Infrastructure	show memory summary could push the CPU util to 100%
CSCsa91716	Infrastructure	Command sh archive config diff hangs with a remote file in argument

Identifier	Technology	Description
CSCse09553	Infrastructure	no snmp-server sparse-table: ds1 physical layer has none 0 for HC
CSCsj06593	Infrastructure	CPU hog msgs for RFSS worker process and Async write process
CSCsk41686	Infrastructure	PARSER-3-CFGLOG_NOMEM: constanlty in log
CSCsr17897	Infrastructure	SXF : increase the buffer size for config generation
CSCsr60789	Infrastructure	W1.3: VSL crash after preemptive switchover in ifs_open_file_decrement
CSCsx05021	Infrastructure	Router crashes when filesystem becomes full
CSCta43093	Infrastructure	Add a check similar to CSCek58956
CSCef09586	IPServices	CMs stuck in init(d) if DHCP ser. ip addr. overlaps with diff VRF
CSCsa41736	IPServices	Router crash after enable NAT rate-limit feature
CSCsg00102	IPServices	SSLVPN service stops accepting any new SSLVPN connections
CSCsh49973	IPServices	NAT-ALG corrupts offset value of DNS PTR response
CSCsk23972	IPServices	Telnet failed with "No wild listener" error
CSCso42170	IPServices	CPUHOG & Traceback messages seen for IP NAT Ager process.
CSCsx33622	IPServices	Fix MSS calcuation issue in TCP
CSCsy88271	IPServices	6500 - SXF - Nat add-route does not work
CSCsz56393	IPServices	Modular IOS - SUP720 - Sends malformed syslog packet
CSCsz63733	IPServices	Traceback seen with FM Nat configuration
CSCsz89107	IPServices	high cpu due to ip_input process during SNMP trap
CSCta24043	IPServices	"%IPNAT-4-ADDR_ALLOC_FAIL" message seen when all ports are not allocated
CSCtb12332	IPServices	NAT: switch crashes at ipnat_find_map_entry with cat6k SXF16 image
CSCsw85254	MPLS	Bus error and crash at p_enqueue when modifying main:text
CSCsz19255	MPLS	LFIB: Tag rewrites are missing on LC for one of load sharable paths
CSCsz30515	MPLS	SUP720 crash due to tsptun_frr_process process hang
CSCsx15396	Multicast	Mcast IIF stays up while physical interface is down
CSCsx34506	Multicast	RPF failure with no PIM neighbor triggers PIM Hello
CSCsw43022	platform-76xx	HSRP Virtual IP Unreachable for some users
CSCsy38911	platform-76xx	MPLS TE Forwarding broken when enable LDP on TE tunnel
CSCta26106	QoS	RSVP-3-CONSISTENCY error followed by an unexpected reboot.
CSCsh15066	Routing	VRF has 2 ospf process, when one process is removed the router crashed
CSCsh23176	Routing	Router crashes @ rip_timer_process .
CSCsm57494	Routing	BGP update is not sent after reloading opposite router
CSCso07476	Routing	One way audio when RTP header compression is turned on
CSCsq49201	Routing	Password in BGP peer-session template not inherited
CSCsr11662	Routing	EIGRP active routes never go to SIA, queries not sent
CSCsr27794	Routing	BGP updates stuck during peer flap
CSCsr90248	Routing	"aggregate-address advertise-map" not updated dynamically
CSCsx06457	Routing	BGP may modify routes it does not own

Identifier	Technology	Description
CSCsx51299	Routing	Crash when remove and configure ipv6 ACL via telnet and console
CSCsx51596	Routing	TCAM ACL entry not correct after removing IP accounting
CSCsy58115	Routing	Continuous BGP mem increase with non established neighbors
CSCsy84134	Routing	ARP table is flushed when deleting secondary IP address
CSCuk55357	Routing	ALIGN-3-TRACE at ip_broadcast
CSCsb80803	Security	SSH Process: SCHED-3-UNEXPECTEDEVENT error message
CSCsg56609	Security	Crash on talk /tmp/tbdaemon-99/../os/connect.c:1105 seen at bootup
CSCsy17893	Security	Ping to itself doesn't work on IPIP tunnels
CSCsz84055	Security	System crashed unexpected while open ssh2 session
CSCek68108	Unknown	Router crashed at ace_policyloader_util.c after remove crypto map .
CSCek74844	Unknown	sysObjectID is wrong for 7603-S and 7609-S
CSCek77996	Unknown	High CPU caused by data traffic with crypto map in crypto connect mode
CSCsb25490	Unknown	Data is not being hardware switched after OIR/SSO on WS-X6148X2-RJ45
CSCsb88996	Unknown	slb traceback spurious memory access after slb statefull switchover
CSCsb96452	Unknown	IGMPV3 TO_INC{} leave mac entry table do not expire
CSCsc85962	Unknown	Replaying Main Mode packet causing IKE SA deletion
CSCsd45698	Unknown	Cat6K: SLB punted to CPU if src_index is port-channel index
CSCsf05390	Unknown	CPU HOG @ hwidb_iftype_unlist followed by router crash.
CSCsf10203	Unknown	MLD gces not freed even after MLD leaves and L3 traffic stopped
CSCsf27621	Unknown	False Command-Active condition blocking execute-on on MWAM processor
CSCsg32319	Unknown	Probe connections not cleaned up when access/vrf is configured .
CSCsg37484	Unknown	Bus Error in crypto_map
CSCsi54373	Unknown	OSM maps EXP into dBus-CoS during SVI based EoMPLS disposition
CSCsj26698	Unknown	Acct-Session-Id in Accounting-Request is different from in Access-Reques
CSCsk38024	Unknown	VS2: EtherChannel state on standby is incorrect due to out of order FEC
CSCsk87604	Unknown	Device crashes on configuring LPIP with multiple hosts.
CSCsl69123	Unknown	SIP-400:QoS:Police drops MPLSCP, CDPCP negotiation packets - SRA,SRB
CSCso35659	Unknown	L3 traffic rate limited after adding and removing Xcon to a SVI
CSCso75862	Unknown	Negative counter values for input queue on layer 3 interfaces
CSCso93350	Unknown	Boot string fails to set in rommon but no error message
CSCsq69567	Unknown	SSO Switchover + unicast-routing chg cause MC traffic loss for 2 minutes
CSCsr06037	Unknown	the monitor session source is removed by deleting sub-interface
CSCsr12976	Unknown	High CPU in ION ios-base process
CSCsr39272	Unknown	%DATACORRUPTION-1 due to spa sensor temp overruning buffer
CSCsr97097	Unknown	VS: RP IPC-5-WATERMARK msgs due to CARD_RESET, after SSO
CSCsr99518	Unknown	Granikos should not init rekey after recieving new outbound SA at QM3
CSCsu29301	Unknown	C2W21: Ingress SPAN on Sup - ACE module duplicates packets

Identifier	Technology	Description
CSCsu76360	Unknown	Memory Leak in IPSec Key Engine with HA on Sup720 RP
CSCsw17070	Unknown	18SXF: SSO switchover cause portchannel configuation lost in sup uplink
CSCsw21852	Unknown	CSM: memory leak in process "Laminar Icc Event"
CSCsw28582	Unknown	IPSec Tunnels go down after a "show run"
CSCsw43377	Unknown	add user warning for empty classes in OSM qos policy SXF7 and later
CSCsw52819	Unknown	Kernel dumper needs a few enhancements.
CSCsw53362	Unknown	c2w2b: Device crashes with NAT stress test
CSCsw68514	Unknown	SLB probes iin TESTing state while using client cmd in Vserver config
CSCsw87563	Unknown	packets with multicast mac and unicast ip are software routed by cat6500
CSCsw92171	Unknown	multiple "power-input" for new 6kW DC PS do not exist on Standby
CSCsx16206	Unknown	Traffic loss issue from SFM capable modules to other device through DEC
CSCsx21886	Unknown	ISSU switchover command sync issue
CSCsx23929	Unknown	MLPP link are not able pass traffic after SSO even when UP/UP stat on os
CSCsx39263	Unknown	TCAM entries are not installed for TCP intercept after SSO
CSCsx49889	Unknown	SPA-IPSEC-2G-3-ACEI0TCAMFAILE:SpdSpInstall:cannot install Sp TmInsertSp
CSCsx51231	Unknown	Service-policy removed from the interface, but FIE still has NBAR active
CSCsx58248	Unknown	Disable Crypto ACL in SXF
CSCsx67510	Unknown	Memory leak on SP when add/deleting channel groups on PA-MC-2T3+
CSCsx76308	Unknown	HA client crashing attempting to free unassigned memory
CSCsy06804	Unknown	DSCP not preserved during SVI based Eompls Disposition
CSCsy08838	Unknown	Zamboni allows clear packet inbound on protected interface
CSCsy24691	Unknown	entPhysicalTable has power-input 3 Sensor for 6kW DC PS1 and not PS2
CSCsy34566	Unknown	Disable VLAN mapping on ME6524, 6148A-GE-TX
CSCsy54365	Unknown	frequent datapath recovery and traffic loss on WS-X6704 with DFC
CSCsy74418	Unknown	Ping fail with bridging on interface - 6500 w/SUP2 and 6816
CSCsy78994	Unknown	Memory leak in Service Task
CSCsy82121	Unknown	IGMP Source only not working due to MC_CAP not set
CSCsy83830	Unknown	IOS-RLB crashes while deleting the username sticky
CSCsy85171	Unknown	CDL2 Read Error: Time out
CSCsy94866	Unknown	C2W2B: CSM Config sync causes memory leak
CSCsz01976	Unknown	Need a cli to dump the rommon environment and unset rommon variable
CSCsz14742	Unknown	EZVPN config not downloaded on the SPA/VPNSM
CSCsz20625	Unknown	Error message seen if SIP Is OIR'd during Standby SUP bootup
CSCsz42143	Unknown	WS-X6148A-GE-TX module fails keepalives when excessive errors on port.
CSCsz43438	Unknown	Encapsulation change on T1/E1 removes QoS Service Policy
CSCsz55834	Unknown	GLBP may provided BIA MAC instead of Virtual MAC for mobile users
CSCsz55950	Unknown	EoMPLS:DFC LTL programming is not correct for SRP as Core

Identifier	Technology	Description
CSCsz62046	Unknown	Crash at memcpy after CPUHOG in SNMP ENGINE
CSCsz67334	Unknown	ciscoEnvMonTemperatureStatus trap sent sporadically as NotFunctioning
CSCsz76015	Unknown	C2W2: Need cli to set PF_BIAS to ensure lower slot# Sup boots as active
CSCsz84544	Unknown	output drops increment on not-connected interface of 6548GE-TX module
CSCsz87648	Unknown	SP/RP and redundant system handshake broken when the kernel crashes.
CSCsz92508	Unknown	SPA module reloads when no response to keep-alive polling
CSCta12382	Unknown	Udld port config does not sync to standby in rpr-plus mode
CSCta12543	Unknown	Linecard takes MAC address from the linecard.
CSCta21771	Unknown	%CONST_DIAG-SP-3-HM_FCI_0_STUCK: Flow control stuck at 0 error on modul
CSCta26529	Unknown	Standby Reset set entPhysicalAssetID on PS1
CSCta27279	Unknown	WCCP s/w switching with Ingress redirection & interface ACL
CSCta32802	Unknown	Umbrella ddts for porting SR HA fixes+ 2T3E3 SPA fixes into SXF
CSCta42989	Unknown	"%CSM parser state" configuring CLI when configuring via XML also
CSCta47653	Unknown	Cat6k: SXF: Console hangs on reapplying running config with ACL
CSCta48521	Unknown	%DATACORRUPTION-1-DATAINCONSISTENCY: copy error
CSCta48968	Unknown	Modular IOS kernel crashinfo has missing information
CSCta52689	Unknown	cat6k crash in RP due to address error with wccp configuration
CSCta53157	Unknown	SPA-4XT3/E3 int in SIP-200 admin-down on standby after fpd upgrade
CSCta55498	Unknown	[Modular IOS] MIPS CP0 registers save algorthim needs a few improvements
CSCta62394	Unknown	RP crashes @crypto_ipsec_profile_map_val on removing vlan with HA config
CSCta71873	Unknown	Mcast traffic stops flowing across fabric to required fpoes
CSCta72199	Unknown	"aggregate-address advertise-map" not updated dynamically with ION image
CSCta76808	Unknown	add CLI command for medium buffer pool
CSCtb02774	Unknown	PI_E scanner needs to check high LTL index(0x740-0x77f) for PO interface
CSCtb23289	Unknown	Major temperature alarm has to force system shutdown
CSCtb23840	Unknown	%SYS-3-CPUHOG in Time Range Process with QoS Time based ACL
CSCtb28032	Unknown	Changing module corrupts Flex Link
CSCtb38547	Unknown	Incorrect CP0 values and empty kernel variable section in kernel crashin
CSCtb68478	Unknown	"Illegal nextSsIndex value" message should be removed
CSCsi56413	WAN	PA-POS-OC3SMI interface output stuck .

Resolved Caveats in Release 12.2(18)SXF16

Resolved AAA Caveats

- CSCsv73509—Resolved in 12.2(18)SXF16

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

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

Workaround: There is no workaround.

Resolved Infrastructure Caveats

- CSCse85652—Resolved in 12.2(18)SXF16

  Symptom: The Cisco IOS HTTP server and the Cisco IOS HTTPS server provide web server functionality to be used by other Cisco IOS features that require it to function. For example, embedded device managers available for some Cisco IOS devices need the Cisco IOS HTTP server or the Cisco IOS HTTPS server to be enabled as a prerequisite.

  One of the functionalities provided by the Cisco IOS HTTP server and the Cisco IOS HTTPS server is the WEB_EXEC module, which is the HTTP-based IOS EXEC Server. The WEB_EXEC module allows for both “show” and “configure” commands to be executed on the device through requests sent over the HTTP protocol.

  Both the Cisco IOS HTTP server and the Cisco IOS HTTPS server use the locally configured enable password (configured by using the **enable password** or **enable secret** commands) as the default authentication mechanism for any request received. Other mechanisms can also be configured to authenticate requests to the HTTP or HTTPS interface. Some of those mechanisms are the local user database, an external RADIUS server or an external TACACS+ server.

  If an enable password is not present in the device configuration, and no other mechanism has been configured to authenticate requests to the HTTP interface, the Cisco IOS HTTP server and the Cisco IOS HTTPS server may execute any command received without requiring authentication. Any commands up to and including commands that require privilege level 15 might then be executed on the device. Privilege level 15 is the highest privilege level on Cisco IOS devices.

  Conditions: For a Cisco IOS device to be affected by this issue all of the following conditions must be met:

  - An enable password is not present in the device configuration
  - Either the Cisco IOS HTTP server or the Cisco IOS HTTPS server is enabled
  - No other authentication mechanism has been configured for access to the Cisco IOS HTTP server or Cisco IOS HTTPS server. Such mechanisms might include the local user database, RADIUS (Remote Authentication Dial In User Service), or TACACS+ (Terminal Access Controller Access-Control System)

  The Cisco IOS HTTP server is enabled by default on some Cisco IOS releases.

  Workaround: Any of the following workarounds can be implemented:

  - Enabling authentication of requests to the Cisco IOS HTTP Server or the Cisco IOS HTTPS server by configuring an enable password

    Customers requiring the functionality provided by the Cisco IOS HTTP server or the Cisco IOS HTTPS server must configure an authentication mechanism for any requests received. One option is to use the **enable password** or **enable secret** commands to configure an enable password. The enable password is the default authentication mechanism used by both the Cisco IOS HTTP server and the Cisco IOS HTTPS server if no other method has been configured.

In order to configure an enable password by using the **enable secret** command, add the following line to the device configuration:

```
enable secret mypassword
```

Replace *mypassword* with a strong password of your choosing. For guidance on selecting strong passwords, please refer to your site security policy. The document entitled "Cisco IOS Password Encryption Facts" explains the differences between using the **enable secret** and the **enable password** commands to configure an enable password. This document is available at the following link:
http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a00809d38a7.shtml

– Enabling authentication of requests to the Cisco IOS HTTP Server or the Cisco IOS HTTPS server by configuring an authentication mechanism other than the default

  Configure an authentication mechanism for access to the Cisco IOS HTTP server or the Cisco IOS HTTPS server other than the default. Such authentication mechanism can be the local user database, an external RADIUS server, an external TACACS+ server or a previously defined AAA (Authentication, Authorization and Accounting) method. As the procedure to enable an authentication mechanism for the Cisco IOS HTTP server and the Cisco IOS HTTPS server varies across Cisco IOS releases and considering other additional factors, no example will be provided. Customers looking for information about how to configure an authentication mechanism for the Cisco IOS HTTP server and for the Cisco IOS HTTPS server are encouraged to read the document entitled "AAA Control of the IOS HTTP Server", which is available at the following link:
  http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a008069bdc5.shtml

– Disabling the Cisco IOS HTTP Server and/or the Cisco IOS HTTPS server functionality

  Customers who do not require the functionality provided by the Cisco IOS HTTP server or the Cisco IOS HTTPS server can disable it by adding the following commands to the device configuration:

  ```
  no ip http server no ip http secure-server
  ```

  The second command might return an error message if the Cisco IOS version installed and running on the device does not support the HTTPS server feature. This error message is harmless and can safely be ignored.

  Please be aware that disabling the Cisco IOS HTTP server or the Cisco IOS HTTPS server may impact other features that rely on it. As an example, disabling the Cisco IOS HTTP server or the Cisco IOS HTTPS server will disable access to any embedded device manager installed on the device.

Further Problem Description: In addition to the explicit workarounds detailed above it is highly recommended that customers limit access to Cisco IOS HTTP server and the Cisco IOS HTTPS server to only trusted management hosts. Information on how to restrict access to the Cisco IOS HTTP server and the Cisco IOS HTTPS server based on IP addresses is available at the following link:

http://www.cisco.com/en/US/docs/ios-xml/ios/https/configuration/12-4/nm-http-web.html#GUID-BB57C0D5-71DB-47C5-9C11-8146773D1127

Customers are also advised to review the "Management Plane" section of the document entitled "Cisco Guide to Harden Cisco IOS Devices" for additional recommendations to secure management connections to Cisco IOS devices. This document is available at the following link:
http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml

- CSCsi13344—Resolved in 12.2(18)SXF16

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

  The Cisco Security Response is posted at the following link:
  http://www.cisco.com/en/US/products/csr/cisco-sr-20090114-http.html

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

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

- CSCsr72301—Resolved in 12.2(18)SXF16

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

  The Cisco Security Response is posted at the following link:
  http://www.cisco.com/en/US/products/csr/cisco-sr-20090114-http.html

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

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

Resolved IPServices Caveats

- CSCsk64158—Resolved in 12.2(18)SXF16

  Several features within Cisco IOS Software are affected by a crafted UDP packet vulnerability. If any of the affected features are enabled, a successful attack will result in a blocked input queue on the inbound interface. Only crafted UDP packets destined for the device could result in the interface being blocked, transit traffic will not block the interface.

  Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are available in the workarounds section of the advisory.

  This advisory is posted at the following link:
  http://www.cisco.com/en/US/products/csa/cisco-sa-20090325-udp.html

- CSCsv04836—Resolved in 12.2(18)SXF16

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

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

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

  This advisory is posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20090908-tcp24.html.

- CSCsw18636—Resolved in 12.2(18)SXF16

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

  Conditions: This problem occurs on SUP32 running 12.2(33)SXI. This problem does not occur on SUP720. The problem is only seen when you have bridge-group CLI being used which lead to arp pkts with protocol types as 0x1000 being bridged. The problem does not apply for IP ARP packets.

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

  Additional Information: This problem is now isolated to command ordering in the startup-config file. The **bridge <>** command is saved before the **bridge-group <>** command (which is run in the interface-config mode) is saved. The linking of IDB to bridge structure is not happening correctly and some check fails in the bridge code that lets the packet to be processed again and again instead of being dropped.

  If the **bridge-group <>** command is removed in the startup-config and only applied after the **bridge <>** command is run, the problem will go away. Please use this workaround until a fix is put in.

- CSCsr29468—Resolved in 12.2(18)SXF16

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

  Cisco has released free software updates that address this vulnerability.

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

  This advisory is posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20090325-tcp.html

- CSCsm27071—Resolved in 12.2(18)SXF16

  A vulnerability in the handling of IP sockets can cause devices to be vulnerable to a denial of service attack when any of several features of Cisco IOS Software are enabled. A sequence of specially crafted TCP/IP packets could cause any of the following results:

  - The configured feature may stop accepting new connections or sessions.
  - The memory of the device may be consumed.
  - The device may experience prolonged high CPU utilization.
  - The device may reload.

  Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are available in the “workarounds” section of the advisory.

  The advisory is posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20090325-ip.html

Resolved LAN Caveats

- CSCsv05934—Resolved in 12.2(18)SXF16

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

Workarounds: There are no workarounds available for this vulnerability.

This response is posted at http://www.cisco.com/en/US/products/csr/cisco-sr-20081105-vtp.html

Resolved Multicast Caveats

- CSCso90058—Resolved in 12.2(18)SXF16

  Symptom: MSFC crashes with RedZone memory corruption.

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

  Workaround: None known at this time.

Resolved Routing Caveats

- CSCsx73770—Resolved in 12.2(18)SXF16

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

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

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

Other Resolved Caveats in Resolved in 12.2(18)SXF16

Identifier	Technology	Description
CSCef97900	AAA	AAAA-3-DROPACCTLOWMEM warning message somewhat misleading
CSCin40015	AAA	telnet to NAS fails when user profile has access-profile
CSCsl29214	AAA	AAA server change leads to bus error crash after "show run" is issued
CSCso95210	AAA	AAA Client creates bad Message Authenticator attr for every first packet
CSCsx28646	ATM	Unable to configure atm pvp l2transport
CSCsx40747	Content	Router hangs while doing ip casa configurations
CSCsc86307	Infrastructure	c3845 crashed @ show_systat
CSCsm32392	Infrastructure	memory corruption crash at nv_ifs_open and nv_ifs_close
CSCso49598	Infrastructure	Stby reloads cont. when upto MAXINT logical int created thru int ran
CSCsq03621	Infrastructure	Timestamps in "show rmon events" wrap at 2^32-1 milliseconds (7+ weeks)
CSCsw35917	Infrastructure	SP syslog messages not sent as SNMP traps by RP's SNMP agent
CSCec72958	IPServices	Software forced crash when translating LDAP packet
CSCsk16821	IPServices	DHCP does not NAK after DHCPREQUEST from unknown client .
CSCso02053	IPServices	NAT does not add dynamic aliases after reload.
CSCso04657	IPServices	SSLVPN service stops accepting any new SSLVPN connections
CSCso54027	IPServices	Spurious memory access in ttcp_rcv_stats

Identifier	Technology	Description
CSCsq60504	IPServices	Modular IOS Sup720: crashed with tcp timeout logs
CSCsr08771	IPServices	Crash seen @ dhcpd_pool_nvgen and dhcpd_copy_bootfile
CSCsx32283	IPServices	Malformed L field in LDAP crashes 6k with NAT
CSCsh33167	LegacyProtocols	Dlsw transparent cache holds MAC address for disconnected circuit
CSCsk41552	Management	T/B %SCHED-3-THRASHING of cdp2.iosproc process_wait_for_event
CSCsb52253	MPLS	IPv4 iBGP multipath in MPLS network needs to be blocked or hardcoded
CSCsc78971	MPLS	LDP:Incorrect address withdraw after IP address removal on shutdown i/f
CSCse22900	MPLS	w/mis-config'd dup vrf CEF/BGP table MPLS label mismatch may occur
CSCsk99530	MPLS	LFIB untagged entries while LIB has valid lables in CSC MPLS VPN c12000
CSCsm70668	MPLS	OIR over E3:POS impacting complete Traffic with biscuit tunnel
CSCsu45425	MPLS	FIB/LFIB not updated correctly on GSR runing 12.0(33)S1 after route-flap
CSCsw19951	MPLS	SP & DFC crash when forwarding a packet with MPLS
CSCse03637	Multicast	PIM Dense Mode - Prune sent in error after assert is won .
CSCsj88725	Multicast	Wrong (S,G) RPF after route change, no upstream join
CSCsm77608	Multicast	IP Multicast packets are Process switched.
CSCsr09312	Multicast	crash when doing mrm stop
CSCsr49316	Multicast	Crash ipv6_static_route_find after configured & executed show ipv6 rpf x
CSCsv99150	platform-76xx	status led of ge-wan module not showing proper status
CSCsg25664	PPP	dLIFoMLPPPoATM PA: Corrupted PC crash PR
CSCsr81271	PPP	Invalid VCD error messages upon PVC flap
CSCek63384	QoS	Service-Policy is Lost When the Multilink Interface is Reset .
CSCsv85791	QoS	Flexwan+/PA-MC-2T3+ introduce 5+ seconds delay on egress
CSCee30355	Routing	Memory leak at ip_multicast_ctl
CSCeg49075	Routing	MSFC2 remark lines in ACLs duplicated in the NDR MSFC
CSCei86031	Routing	changing match command on fly does not filter route correctly .
CSCej49366	Routing	Removing default-metric under EIGRP deletes routes erroneously
CSCek75079	Routing	Problem in type7 to type5 translation if summary-addr configured
CSCsa72878	Routing	ISIS: clns route from end-system not in database
CSCsb15164	Routing	Security holes while configuring a standard ACE with host address
CSCsc01880	Routing	%FIB-4-FIBCBLK: Missing cef table for tableid 770 during routing table e
CSCse53019	Routing	redistribution not triggered when BGP as-path/community changes
CSCse68877	Routing	CEF/BGP table MPLS label mismatch YW3 Non Multi-path
CSCsg46366	Routing	OSPF NSSA LSA forwarding address set even when P bit wil be clear.
CSCsg68717	Routing	A weird behavior in maxpath configuration in ebgp+ibgp case
CSCsi01324	Routing	Modifying acl concerned with distribute-list withdraw summary route
CSCsi03434	Routing	Memory leak @ ospf_redist_work_enqueue
CSCsj09838	Routing	RR some prefix might not be sent after bgp neighbor flaps .

Identifier	Technology	Description
CSCsj13911	Routing	Cat3750:EIGRP does not receive reply for query between some Vlan
CSCsk35688	Routing	Aggregate routes not processed if child routes are deleted pre-maturely
CSCsk72259	Routing	Auto-repair not updating inconsistent cef entries
CSCsl32318	Routing	OSPF: new fix for CSCsk36324 SPF loop
CSCsl84712	Routing	Error- %OSPF-4-FLOOD_WAR: Process 123 re-originates LSA ID 10.55.122.148
CSCsm50741	Routing	Removal of DCbitless LSA causes problems
CSCsm95129	Routing	"no ip next-hop-self eigrp" not working when redistribute from BGP
CSCsm96901	Routing	Unable to ping between vrfs through transparent bridge
CSCso08786	Routing	Standby reloads due to config sync failure on inherit peer-policy cmd.
CSCso54167	Routing	BGP peer stuck with table version 0
CSCsr67361	Routing	I/O memory leaks when BGP neighbor points to a local address
CSCsr88362	Routing	eigrp routes aren't updated after SSO switchover
CSCsu24087	Routing	Cisco7609 crashes after "clear ip bgp neighbor x.x.x.x soft in"
CSCsu36709	Routing	Unable to boot IOS image on PE (vrf-enabled) router - software fault
CSCsv01474	Routing	'ip rip advertise' command lost after interface flap/clear ip route
CSCsv27607	Routing	BGP: Outbound route-map updating withdraw only one member
CSCsw28893	Routing	Cost no longer showing with each eigrp route after IOS upgrade
CSCsw65441	Routing	ARP packets drops due to excessive ARP requests sourced from SVI
CSCsx15841	Routing	aggregate-address does not NVGEN upon switchover on cat6k
CSCsc91824	Security	SSH from router disconnects vty session if there is no matching cipher
CSCsd81870	Security	Teraterm + TTSSH2 does not work in SSH Ver.2
CSCeh00399	Unknown	RRI: refcount not inc on rekey in certain circ lead to route removal
CSCei29284	Unknown	Rockies3 SUP32 SNMP:Traceback msg when execute private vlan script
CSCek28863	Unknown	Need to change default SCP keepalive timeout on IOS to CSM module
CSCsc73409	Unknown	IGMPv3 report suppression doesnt send out group records correctly
CSCsc98850	Unknown	ZAMBONI:Could not send pmtu information vlan 65535 pmtu 0 Error
CSCsd04937	Unknown	Crash in chunk_free called from mfib_const_rp_free after (*,G) HW enable
CSCse12518	Unknown	MET optimized update can cause blackholing and duplicates
CSCsg14926	Unknown	Standby can not boot because of insufficient memory with 32K interfaces
CSCsg53526	Unknown	Some packets to vip are denied by inbound acl after server nat
CSCsh22225	Unknown	CWAN_HA-STDBY-4-IFCFG_PLAYBACK_ERROR:
CSCsh98849	Unknown	SIERRA: Active and stby SP and active RP crashed@rf_proxy_fatal_error
CSCsi14145	Unknown	runt counter not implemented correctly
CSCsi66012	Unknown	2 garbage values in show module csm x ft details
CSCsi88920	Unknown	MLD rcvr in SVI stops receiving v6 mcast trffc if another rcvr leaves
CSCsk23521	Unknown	EARL-SPSTBY-2-SWITCH_BUS_IDLE is seen with SW switched traffic
CSCsl02190	Unknown	ICMPv6 to all node multicast address fail .

Identifier	Technology	Description
CSCsm31178	Unknown	policy-map stops working on a good int if wrongly applied on another int
CSCsm43962	Unknown	Cat6k L2TP packet looped through blocked port
CSCsm66023	Unknown	IPv6 VTI RP crashed ace_reverse_map when changing tnlsrc from v4 to v6
CSCsm75286	Unknown	bgp route-map doesn't work correctly when deleted part of sequences
CSCsm76792	Unknown	PM HA bulk sync posting RF_DONE before bulk sync has finished
CSCsm85936	Unknown	UUT cpu at 40% with bi-dir traffic across a single tunnel
CSCsm93648	Unknown	C2W2:080226 Rtr crashed when moving tunnels from VTI to GRE/TP
CSCso11822	Unknown	LACP PC switchport, on OIR, "channel group 112 active" config gets lost
CSCso29141	Unknown	DFC installs drop index for MAC-address
CSCso88042	Unknown	Wism module Allowed-Vlan statements lost on reload
CSCso88772	Unknown	sp-inband tx capture causes primary SUP to hang
CSCsq22383	Unknown	SP crash due to CPU hog by online diags
CSCsq42885	Unknown	Line card crashes with %IPC-2-ONINT error on OSM
CSCsq51378	Unknown	ATM PA Interface shows up/up after force redundancy, no cables connected
CSCsq56941	Unknown	6500 - Static MAC cleared from port-channel member ints after reload
CSCsq73122	Unknown	Proxy-ARP returns BIA instead of VMAC with LAM
CSCsq75704	Unknown	FW2 FE PA Interface stays up/down with no conn and goes up/up after sso
CSCsq80145	Unknown	VACL does not work against self initiated packet
CSCsq83789	Unknown	LTL for unknow unicast is wrongly programmed for some L3 interfaces
CSCsq84116	Unknown	Cisco 7604 with OC3, Flexwan crashes into ROMMON
CSCsq90844	Unknown	bridge-group config make packets be routed
CSCsq94136	Unknown	Burst of traffic cause anti-replay check to fail
CSCsr29559	Unknown	WCCP flap corrupts mcast CEF adjacency
CSCsr37131	Unknown	buginf calls in l2trace when 'debug l2trace' is disabled
CSCsr45495	Unknown	PBR with deny statements : TCAM running out of masks
CSCsr51799	Unknown	pa-mc-8t1 interface down after stopping BERT prematurely
CSCsr69929	Unknown	ACL based uRPF check is causing acl permit packets to be dropped
CSCsr88625	Unknown	Seeing ME_AR#0 WARNING: Cannot FLUSH Dic#0 when WS-X6708-10GE boots
CSCsr88845	Unknown	unicast BootP replies dropped by DHCP snooping
CSCsu05800	Unknown	C2W2: need to extend the wait time for bus sync after sso
CSCsu07931	Unknown	cbQosPoliceConformedByte64 counter displays aggregate instead conformed
CSCsu18231	Unknown	IKE process fails to start phase1 if in up-no-ike and DPD triggered
CSCsu33707	Unknown	Multicast traffic will not stop after PIM prune
CSCsu37481	Unknown	Netflow Incorrect Octet value with packet-based sampling
CSCsu37899	Unknown	SXF15: autostate configuration missing after SSO
CSCsu45210	Unknown	Upgrade 12.2SXF-> 12.2SXH with Port-Security causes standby boot loop
CSCsu46982	Unknown	I/O rate counter inaccurate when applying serv policy and MPLS traffic

Identifier	Technology	Description
CSCsu49002	Unknown	ciscoIpMRouteBps sometimes indicates wrongful value
CSCsu49257	Unknown	Cstn-id timer should be restarted when access-request is seen
CSCsu57958	Unknown	DHCP-Snooping not intercepting DHCP messages from the Server
CSCsu68698	Unknown	No syslogs and stack on console when SP crashes due RP boot timeout
CSCsu86524	Unknown	IKMP process leak: check_ipsec_proposal
CSCsu91725	Unknown	Bus crash problem due to cipSecGlobalStats MIB query
CSCsu99270	Unknown	CPUHOG observed when configuring more vlan interfaces
CSCsv07858	Unknown	IfIndex for unconfigured VLAN on 7613
CSCsv10229	Unknown	Failed to assert Physical Port Administrative State Down alarm
CSCsv17989	Unknown	interface in SIP200 show "admin down" when it is physical down
CSCsv18579	Unknown	'recognized & transferred a satvcl packet' observed on 6708 / module 1
CSCsv63144	Unknown	Controller remains DOWN after switchover
CSCsv64079	Unknown	SXF7: Patching fails with WiSM Card on Cat6500
CSCsv66827	Unknown	Clearing the SSH session from a different vty session crashes the box.
CSCsv85551	Unknown	SP crash due to consume all scp triggered by OIR loop when PS go off
CSCsw35155	Unknown	reduce move count for SAs in SXF
CSCsw38075	Unknown	%SYS-2-GETBUF: Bad getbuffer error messages after IOS upgrade
CSCsw43953	Unknown	Error message seen if SIP Is OIR'd during Standby SUP bootup
CSCsw65477	Unknown	MLD snooping broken in SXF16 engg (pre-release) images
CSCsw68032	Unknown	Serial links UP/DOWN after SSO on OSM Module
CSCsw69911	Unknown	SIP-400 POS WRED queues tail dropping without random drops
CSCsw75293	Unknown	18SXF: RP Mapping not seen in last hop router in Sup2 image
CSCsw82431	Unknown	18SXF16:Device crashes while unconfiguring PBR configs.
CSCsw96891	Unknown	CPUHOG observerd after issuing exec commands
CSCei77073	WAN	NTP client need to reset auto learnt source IP address

Resolved Caveats in Release 12.2(18)SXF15a

Identifier	Technology	Description
CSCsu45425	MPLS	FIB/LFIB not updated correctly on GSR runing 12.0(33)S1 after route-flap

Resolved Caveats in Release 12.2(18)SXF15

Resolved Caveats for Product 'all' and Component 'bgp'

- CSCsk69927—Resolved in 12.2(18)SXF15

  Symptoms:

  All the BGP routes are dropped when IOS device receives BGP update with atomic-aggregate length as 254 (0xfe).

Conditions:

The topology consists of two eBGP peers with test traffic across the link. The BGP process does not crash, and routes are not restored after the event.

Workaround:

None.

Resolved Caveats for Product 'all' and Component 'mlp'

- CSCsa49019—Resolved in 12.2(18)SXF15

  Symptoms: A memory leak may occur in the "Multilink Events" process, which can be seen in the output of the **show memory summary** command:

```
0x60BC47D0 0000000024 0000000157 0000003768 MLP bundle name
0x60BC47D0 0000000028 0000000003 0000000084 MLP bundle name
0x60BC47D0 0000000044 0000000001 0000000044 MLP bundle name
0x60BC47D0 0000000048 0000000001 0000000048 MLP bundle name
0x60BC47D0 0000000060 0000000001 0000000060 MLP bundle name
0x60BC47D0 0000000064 0000000013 0000000832 MLP bundle name
0x60BC47D0 0000000068 0000000008 0000000544 MLP bundle name
0x60BC47D0 0000000072 0000000001 0000000072 MLP bundle name
0x60BC47D0 0000000076 0000000001 0000000076 MLP bundle name
0x60BC47D0 0000000088 0000000018 0000001584 MLP bundle name
```

  Conditions: This symptom is observed when two interfaces are configured in the same multilink group or are bound to the same dialer profile.

  Workaround: There is no workaround.

Other Resolved Caveats in Release 12.2(18)SXF15

Identifier	Product	Component	Description
CSCsg18288	all	aaa	Enable authentication ignores Tacacs+ configuration in rare situation
CSCso95426	all	aaa	Exposure of Radius-Keys in debugs.
CSCei33231	all	atmcommon	ATM PVC bundle protected group test failed with bumping exhausted
CSCek74474	all	atmcommon	no/default proto ip inarp cmd ineffective until ATM VC bounced.
CSCsd92325	all	bgp	Config sync: no neighbor 192.168.240.34 triggers standby reset
CSCsf06946	all	bgp	Removing loopback interface causes continuous standby RP reloading
CSCsi27696	all	bgp	oldest ebgp bestpath not retained in eibgp multpath cases
CSCsi68795	all	bgp	PE wrongly assigns local label to a vpnv4 confederation prefix
CSCsi98730	all	bgp	CEF/BGP table MPLS label mismatch in IOS 12.4(6)T5
CSCsl92283	all	bgp	Unable to add into routing table if static route use interface + gateway
CSCso62166	all	bgp	Crash @ bgp_netlist_validate when ibgp established with metric
CSCso93535	all	bgp	Upon removing a VRF, BGP route timers in other VRF's get reset
CSCsq13938	all	bgp	reload on 'show ip bgp vpnv4' when import src delinked by BGP deconfig
CSCsq21198	all	bgp	PE loses VPNv4-MDTs from a RR when another RR fails (or shuts neighbor)
CSCsl04386	all	cat6000-env	%BIT-STDBY-4-OUTOFRANGE : Traceback on Bootup .
CSCse53517	all	cat6000-wireless	WiSM: Tracebacks seen after SSO switchover

Identifier	Product	Component	Description
CSCsm78651	all	csg	malloc memory issue in standby SP supervisor
CSCsi15183	all	eigrp	change MTU value causes %DUAL-3-INTERNAL in ipigrp2_add_item_dest
CSCsm70580	all	ftp	c2w2:ciscoFtpClientMIB: ftp_fs.proc extra processes can deadlock & crash
CSCsi76936	all	glbp	Crash in GLBP if debug is enabled and it rcvs pkt from unknown group
CSCsl70070	all	hsrp	CPUHOG when doing HSRP SNMP query
CSCsq29165	all	install	Rockies-sup3:UUT hangs during installation
CSCsm45634	all	ip	BGP VPNv4 route is not actived immediately after receving update
CSCsl60092	all	ipc	Active SP crashed @ipc_fragment_cleanup with VSL shut/no shut test
CSCsl92316	all	ipmulticast	LNS: %SYS-3-CPUHOG when clear l2tp tunnel, sessions have multicast
CSCsl26998	all	ip-pbr	Switch crashes on applying PBR with next-hop verify-availability
CSCsm04442	all	ip-rip	Router crash at rip_find_sum_idb
CSCeg35237	all	ipsec-core	Watchdog crash after sh crypto session
CSCsm13389	all	ipsec-routing	RRI is not called be if QM rekey timer expiry forces SA deletion
CSCsh38140	all	isis	CEF drops when using CEF LB paths and active link recovers from failure
CSCsm30973	all	mpls-lfib	bgp multipath with ipv4+label nexthop: label missing in cef
CSCso22730	all	mpls-lfib	Prefixes get assigned imp-null local label after OIR linecard
CSCsi77983	all	netflow-switch	RP crashed ipflow_pak_pre_check on shutdown the trunk port
CSCso87348	all	netflow-switch	Corruption in subflow code
CSCsm04256	all	neutrino	CPUHOG and crash after 'show memory detailed all statistics' issued
CSCsm69827	all	neutrino	%SYS-2-MALLOCFAIL:Process= "GraphIt" in SXH1_fc3
CSCsg32308	all	ntp	copy/paste of ntp-authentication-key statement is not possible
CSCek58956	all	os	Need process_ok_to_reschedule check in process_may_suspend
CSCsq50429	all	osm-qos	OSM card unexpected reload @ cwtlc_qos_create_global_qid_info
CSCsa73179	all	ospf	Memory corruption/crash when 'no default-information orig' under RIP
CSCsm91801	all	ospf	ASBR not updating metric in LSA-5 redistributing from 2-nd OSPF process
CSCsm01126	all	parser	PRE-B crashes while in progress to standby cold-config
CSCsj49293	all	pas-2pos-7xxx	POS Interface Output Rate (200 mbps) > Line rate (155 Mbps)
CSCsd14706	all	pim	PIMV2 router send PIMV1 RP-reachable messages loading recieve router CPU
CSCsq14151	all	pim	RPF of (S,G) is set to NULL, When (S, G, R) entry is convered to (S, G)
CSCsd62013	all	snmp	Traceback on Standby RP@add_lpmapping_entry_private+74
CSCsj91738	all	spa-ipsec-2g	Non-ip packet with mcast-mac addr cause high CPU with VPN-SPA VRF mode.
CSCso26788	all	ssh	Re-work CSCin91851 for SXF
CSCsr60782	all	ssh	Fix SA warnings in ssh2_support.c
CSCsr85093	all	ssh	SXF15: SSH session fails withRSA signature verification failed after SSO

Identifier	Product	Component	Description
CSCsq48201	all	trans-bridging	c7300:Bridge IRB-Router crash and traffic flow issue
CSCsi63649	all	ts	%SYS-3-TIMERNEG:Cannot start timer with negative offset,TTY Background
CSCsd37499	c12000	ifs	%IFS-3-FSMAX: Failed to add ?, maximum filesystems 64 msg with Traceback
CSCsq48271	c6venus-slb	laminar	adding redundant CSM causes config sync to indicate in sync when not
CSCsk32095	c7200	pas-2fast-ethernet	PA-2FE-TX port flaps on applying qos policy
CSCsq20970	c7500	7x00-t1e1	ATM option missing, while configuring T1 controller for mode atm
CSCsg22830	c7600	c7600-ha	Standby not coming up after sso switchover
CSCsj43677	c7600	c7600-ha	Active Sup720 crash when removing Standy supervisor
CSCsq19146	c7600	c7600-sip-200	FPD creation for new pegasus rx (1.6) FPA image for Sip-1 CR
CSCsm32363	c7600	cat6000-acl	Netflow SLB sw-installed entries not aging out
CSCek78066	c7600	cat6000-env	Whitney:CLI & MIB mismatch for aux-1 temperature Sensor SUP32
CSCsi41749	c7600	cs7	ITP-76:%SYS-2-INTSCHED: 'sleep for' at level 2 (Process- "MIP Mailbox")
CSCsq60553	c7600	cwpa2	Create cwslc-rommon3.bin for cwpa2 to accomodate release Rommon (1.8)
CSCsr99933	c7600	loadbal	FWLB: High purge rate causes CPU to increase by 15%
CSCsm87735	c7600	osm-choc-ds0	OSM CHOC12/T1 - t1 shutdown does not disable Serial interface
CSCso78097	c7600	osm-ct3	OSM-ct3 MFR interface is flapping
CSCsq47166	c7600	osm-gigwan	GE-WAN interface stays down with autonegotiation enabled
CSCso59971	c7600	osm-pos	OSM OC3 POS : Wrong traffic counters
CSCsq19159	c7600	snmp	RP crashes in chassismib_add_sub_card_entry after linecard reload
CSCsq19476	c7600	spa-ipsec-2g	DMVPN over POS - wrong spa vlan in cef adj after boot, gre sent in clear
CSCso89823	c7600	spa-pos-oc12	Pos interface "rxload" and "input bytes" counters incorrectly increment
CSCsc69804	c7600	vipmlp	SIP1-ChOC3:Initial packets fail with SW-MLP on SIP-200
CSCsq12119	c7600	vpn-sm	SXF13 Crash on VPNSM OIR due to chunk memory double free.
CSCsi00712	cat6000	c6k-wan-common	Connected ipv4 routes for WAN interfaces missing on reload
CSCsi99875	cat6000	c6k-wan-common	BOOM: spa_eeprom_read_bit on BOOTUP
CSCsg39754	cat6000	cat6000-acl	DHCP snooping redirect ACL permits more than just bootpc and bootps port
CSCso97524	cat6000	cat6000-acl	Packet drop after TCAM exception happened
CSCsf17163	cat6000	cat6000-cm	TCAM mask/entry resource not released after conf/unconf pacl
CSCsm53873	cat6000	cat6000-diag	Module 1/0 failed in health monitoring configuration (error code 23)
CSCsq53822	cat6000	cat6000-env	Monitor session removal may affect traffic through WS-X6148A-RJ-45
CSCsq47140	cat6000	cat6000-fabric	67xx module may not come online
CSCsr54630	cat6000	cat6000-fabric	Patch workaround and s222 build fix for CSCso53756
CSCso87838	cat6000	cat6000-filesys	HSRP: with aggressive timers HSRP peer flaps when "wr mem"
CSCsk93587	cat6000	cat6000-firmware	TestFabricCh0Health test failure with unidir traffic via Ch1on Berytos

Identifier	Product	Component	Description
CSCsl39710	cat6000	cat6000-firmware	cat6000 mac-address-table does not add entries for local fwsm mac . .
CSCsq14259	cat6000	cat6000-firmware	TX Flowcontrol goes on when link negotiation is disabled
CSCsq79253	cat6000	cat6000-firmware	Pinnacle interrupts not re-enabled after memory inconsistency detected
CSCsq85850	cat6000	cat6000-firmware	Opnext GLC-LH-SM :remote port stays up when local RX cable is removed
CSCsq41311	cat6000	cat6000-hw-fwding	I/O memory leak in Medium buffers
CSCsq77464	cat6000	cat6000-hw-fwding	mls rate-limit unicast cef receive value re-written upon TCAM exception
CSCsr28305	cat6000	cat6000-hw-fwding	Packet drops on L2 portchannel on WS-X6708-10G
CSCsl72912	cat6000	cat6000-ipc	VS2: WS-X6708 DFC crash in local_cb1(Segment violation)
CSCsr09554	cat6000	cat6000-ipc	Move SIBYTE SB_RMON_OVRFL messages under debug
CSCsu03772	cat6000	cat6000-l2	Dot1q native vlan tagging is not working with "switchpot nonegotiate"
CSCsq59297	cat6000	cat6000-l2-infra	port-channel IDB gets mixed up
CSCsh16213	cat6000	cat6000-mcast	Disabling MLDsnooping does not clean special MACs 3333.0000.0016, 3333.0
CSCsm59926	cat6000	cat6000-mcast	RP receives 2 copies of each PIM register with MVPN
CSCso44072	cat6000	cat6000-mcast	High CPU due to multicast traffic getting punted to software
CSCso71355	cat6000	cat6000-mcast	PVLAN - 6500 - Multicast flood broken from pvlan port to promiscuous
CSCsg19793	cat6000	cat6000-portsecur	Psecure absolute aging on DFC causes MAC inconsistency w/ Central EARL
CSCsq04355	cat6000	cat6000-span	Fix in CSCso81632 is not complete
CSCso85395	cat6000	cat6000-svc	Unable to add the 256th vlan
CSCso84567	cat6000	cat6000-wccp	6500 with WCCP and CoPP punts non-TCP packets into CoPP policy.
CSCsb60078	cat6000	cat6k-v6-mcast	After SSO switchover, mcast ergess Vlan gets out of sync among DFCs
CSCsj28026	cat6000	cat6k-vs-snmp	WhitneyVS: Unable to mibwalk clcFdbVlanInfoTable . .
CSCsq68529	cat6000	decnet	After reload, there is no mac-address on SVI not running DECnet
CSCso68344	cat6000	dhcp	Switch acting as DHCP server crashes on issuing no service dhcp command.
CSCsq37376	cat6000	elam	Packet Buffer Capture May Crash a 6500 in IOS
CSCsm82958	cat6000	loadbal	radius sticky entry deleted even if the idle timer is not 0
CSCso30038	cat6000	mcast-vpn	A OIL is not registerd properly in mroute table with static igmp group
CSCsl90285	cat6000	pas-pos	POS-APS: CWPA-3-NODISPATCH messages seen when configuring APS
CSCsi74360	cat6000	spa-ipsec-2g	packet loops between icpu and ocpu while sending clear mcast traffic
CSCsq39079	cat6000	spa-ipsec-2g	SPA-IPSEC-2G Crash under load due to IKE session establishment
CSCsq37078	cat6000	vipmlp	Input errors incrementing on Multilink 5 in admin down state
CSCso00793	itp	cwpa2	ITP-76: Flexwan Memory version "VI4DP647228EBK-MD" causes reload

Resolved Caveats in Release 12.2(18)SXF14

Resolved Caveats for Product 'all' and Component 'dns'

- CSCsk25697—Resolved in 12.2(18)SXF14

  Symptom:

  A router with DNS server configured may show CPUHOG tracebacks when it receives repeated crafted udp packets to its port 53.

  Sample for 3800 router:

  %SYS-3-CPUHOG: Task is running for (40004)msecs, more than (2000)msecs (5/0),process = DNS Server Input.

  -Traceback= 0x60D68CDC 0x6033D984 0x6180E58C FFFFFFA0 3F 4E 60 0x708DFD18 06 FFFFFFFE FFFFFF88 FFFFFFA5 FFFFFFA3 FFFFFF92 FFFFFFA7 FFFFFF8B 7A 3A FFFFFFF5 17 FFFFFF9B FFFFFFC9 FFFFFF9B FFFFFFA2

  Conditions:

  Router needs to have dns server configured and listen to udp port 53

  ```
  conf t
  ip dns server
  end
  ```

  Workaround:

  Apply rate limit to port 53 to interfaces facing untrusted networks:

  ```
  access-list 100 permit udp any any eq domain
  access-list 100 deny ip any any
  interface GigabitEthernet0/0
  ip address 10.2.2.2 255.255.255.0
  rate-limit input access-group 100 8000 1500 2000 conform-action transmit exceed-action
  drop
  ```

Resolved Caveats for Product 'cat6000' and Component 'cat6000-sw-fwding'

- CSCek49649—Resolved in 12.2(18)SXF14

  Symptom: Cisco Catalyst 6500 and Cisco 7600 modules are reachable via 127.0.0.x addresses.

  Conditions: Cisco Catalyst 6500 and Cisco 7600 series devices use addresses from the 127.0.0.0/8 (loopback) range in the Ethernet Out-of-Band Channel (EOBC) for internal communication.

  Addresses from this range that are used in the EOBC on Cisco Catalyst 6500 and Cisco 7600 series devices are accessible from outside of the system. The Supervisor module, Multilayer Switch Feature Card (MSFC), or any other intelligent module may receive and process packets that are destined for the 127.0.0.0/8 network. An attacker can exploit this behavior to bypass existing access control lists; however, an exploit will not allow an attacker to bypass authentication or authorization. Valid authentication credentials are still required to access the module in question.

  Per RFC 3330, a packet that is sent to an address anywhere within the 127.0.0.0/8 address range should loop back inside the host and should never reach the physical network. However, some host implementations send packets to addresses in the 127.0.0.0/8 range outside their Network Interface Card (NIC) and to the network. Certain implementations that normally do not send packets to addresses in the 127.0.0.0/8 range may also be configured to do so.

  Destination addresses in the 127.0.0.0/8 range are not routed on the Internet. This factor limits the exposure of this issue.

This issue is applicable to systems that run Hybrid Mode (Catalyst OS (CatOS) software on the Supervisor Engine and IOS Software on the MSFC) and Native Mode (IOS Software on both the Supervisor Engine and the MSFC).

Workaround:

Administrators can apply an access control list that filters packets to the 127.0.0.0/8 address range to interfaces where attacks may be launched.

```
ip access-list extended block_loopback
deny ip any 127.0.0.0 0.255.255.255
permit ip any any

interface Vlan x
ip access-group block_loopback in
```

Control Plane Policing (CoPP) can be used to block traffic with a destination IP address in the 127.0.0.0/8 address range sent to the device. Cisco IOS Software releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP may be configured on a device to protect the management and control planes to minimize the risk and effectiveness of direct infrastructure attacks. CoPP protects the management and control planes by explicitly permitting only authorized traffic that is sent to infrastructure devices in accordance with existing security policies and configurations.

```
!-- Permit all traffic with a destination IP
!-- addresses in the 127.0.0.0/8 address range sent to
!-- the affected device so that it will be policed and
!-- dropped by the CoPP feature
!
access-list 111 permit icmp any 127.0.0.0 0.255.255.255
access-list 111 permit udp any 127.0.0.0 0.255.255.255
access-list 111 permit tcp any 127.0.0.0 0.255.255.255
access-list 111 permit ip any 127.0.0.0 0.255.255.255
!
!-- Permit (Police or Drop)/Deny (Allow) all other Layer3
!-- and Layer4 traffic in accordance with existing security
!-- policies and configurations for traffic that is authorized
!-- to be sent to infrastructure devices
!
!-- Create a Class-Map for traffic to be policed by the
!-- CoPP feature
!
class-map match-all drop-127/8-netblock-class
match access-group 111
!
!-- Create a Policy-Map that will be applied to the
!-- Control-Plane of the device.
!
policy-map drop-127/8-netblock-traffic
class drop-127/8-netblock-class
police 32000 1500 1500 conform-action drop exceed-action drop
!
!-- Apply the Policy-Map to the Control-Plane of the
!-- device
!
control-plane
service-policy input drop-127/8-netblock-traffic
!
```

Additional information on the configuration and use of the CoPP feature is available at the following links:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_paper0900aecd804fa16a.html

Infrastructure Access Control Lists (iACLs) are also considered a network security best practice and should be considered as, long-term additions to effective network security as well as a workaround for this specific issue. The white paper entitled "Protecting Your Core: Infrastructure Protection Access Control Lists" presents guidelines and recommended deployment techniques for infrastructure protection ACLs. The white paper is available at the following link:

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

Further Problem Description:

None

Other Resolved Caveats in Release 12.2(18)SXF14

Identifier	Technology	Description
CSCdu79630	AAA	Username on vty not displayed if accounting is not configured
CSCsl57645	AAA	tacacs-server directed-request fails for enable authentication on 6500
CSCsj88665	Access	Bus error with PA-MC-2T3+ when deleting channel-group
CSCsm12247	Content	WCCP: hash assignment may be lost after service group change
CSCsk70446	Infrastructure	NRT: tracebacks @ data_inconsistency_error - 7200 for HTTP config .
CSCsl06515	Infrastructure	Sup720 Crash with 11 eFlexWan linecards
CSCso99219	Infrastructure	Match ip address with Named ACL not work in route-map
CSCec51750	IPServices	Router reloads do to bus error. and illegal access to low address
CSCsi57927	IPServices	FTP session hangs TCP in closewait after CLI times out . .
CSCsl23788	IPServices	Dlsw+ peer waits in AB_PENDING or WAIT_WR status with modular IOS
CSCsm36306	IPServices	NAT creates overlapping translation entries using the same IG address
CSCsm59037	IPServices	no service dhcp command causes switch to reload
CSCsk94676	LegacyProtocols	dlsw with tbridge, COMMON_FIB-4-FIBIDBMISMATCH
CSCsl78965	MPLS	High CPU in SNMP engine, mplsVpnVrfRouteEntry
CSCso47703	MPLS	Spurious Access error on rsvp_frr_event_lsp_down_psb
CSCek75931	Multicast	LNS: %SYS-3-CPUHOG When sessions have multicast
CSCsk26429	Multicast	Router configured for IGMP Proxy may not send IGMP Join
CSCsm17426	Multicast	RP-bit not cleared on s,g; traffic outage for 4 minutes
CSCsm44620	Multicast	Shutdown interface present in PIM interface list
CSCsm48322	Multicast	IPv6 Multicast RP ignores embedded RP register messages
CSCse40966	PPP	MLP links down after SSO switchover if aaa new-model cfged
CSCsj60595	QoS	SIP-400 : offered rate in sh policy-map int is not accurate
CSCsm29181	QoS	Crash when NBAR applied to sub-interface
CSCsm49062	QoS	cwan2: show queueing interface reports double count for wfq drops
CSCef16315	Routing	default-information originate route-map causes default route aging

Identifier	Technology	Description
CSCek47667	Routing	clear bgp ipv6 unicast * does not work .
CSCsc58258	Routing	OSPFv3: 64-bits long keys for LSDB
CSCsc72090	Routing	EIGRP doesn't honor interface IP MTU when sending packets
CSCsc96014	Routing	EIGRP neighbors from primary add space deleted when sec add removed
CSCse65277	Routing	MU:default isis metric maximum returns parser error
CSCse85383	Routing	OSPFv3: Restructure link-state request list (CSCsd03021)
CSCsj21785	Routing	TE tunnel does not reoptimize after mtu change
CSCsj56281	Routing	BGP inherit peer-policy not working after router reload
CSCsk35985	Routing	OSPFv3: router crashes for "show ipv6 ospf lsdb" after redist of routes
CSCsl06336	Routing	removing 'maximum-paths import 6' causes duplicate paths in VRF table
CSCsl30331	Routing	Prefixes permitted despite the deny action on route-map continue
CSCsl70287	Routing	RIP default-originate not working after a switchover
CSCsm43938	Routing	stby resets when large config/arp table to sync over to it
CSCso60089	Routing	7200: KBOOT image build failed
CSCso64274	Routing	0.0.0.0/0 redistributed entry not removed RIP DB after deleting command
CSCso73076	Routing	can not delete ACE enties in ACL
CSCsc92417	Security	Secure copy feature intreaction issues with Archive command
CSCsg03753	Security	cat6k memory leak in map->peers and peering_info_list_chunk
CSCsl34391	Security	Output of 1st page of "sh crypto ipsec sa" is blank
CSCso03917	Security	Rtr crash on "sh cry ipsec sa" @ crypto_ipsec_manipulate_ident_tree
CSCef71952	Unknown	EzVPN server disconnects all PAT users of same IP address
CSCek74347	Unknown	Router crash after ip address slarp retry
CSCsb81527	Unknown	sup2:Need enhanced FIB fatal error handling
CSCsb97997	Unknown	dot1dTpFdbAddress is broken
CSCsd42319	Unknown	SIP400 crashes during bootup with current pikespeak image
CSCsd58422	Unknown	%IXP_MAP-3-QOS_CONFIG: error detected: Can't download policymap
CSCsd82457	Unknown	EOU Policy can't exempt Cisco 7935 Conference Station & Wireless phones
CSCsg00173	Unknown	v4 Sparse/SSM traffic when src is in PVLAN src port/DFC is not routed
CSCsg16964	Unknown	Sup32 crashes with 23rd image tb@_shmwin_error
CSCsi52715	Unknown	PISA:SIP200 and FW2 reboots on SSO switchover
CSCsi97434	Unknown	A router may crash when ipsec is established
CSCsj25906	Unknown	Configuration changes made after scheduling a reload do not get saved
CSCsj48453	Unknown	AW: CAT6k does not forward multicast traffic to WISM in L3 mode
CSCsk07255	Unknown	Sip-600 crash on SSO
CSCsk09552	Unknown	New varbinds showing real & virtual server info needed in SLB traps
CSCsk44233	Unknown	While raising the interrupt level, bgp_route_map_inform tries to suspend
CSCsk67578	Unknown	Flow End sysUpTime higher value than the Router sysUpTime

Identifier	Technology	Description
CSCsk80552	Unknown	Shut and no shut of interface causes the delay in forming rp mapping
CSCsk82877	Unknown	METROPOLIS #0 cnt=1 reg:[1B0]kic_kic_int 02
CSCsk87262	Unknown	Switch crashes when polling port security MIB for SIP or Flexwan
CSCsk88760	Unknown	122SR:Routers crashes on unconfiguring vlan in the LACP mode
CSCsl02812	Unknown	TCP SYN packet lost for web applications when NAT outside IF is ATM
CSCsl18958	Unknown	IOS-SLB: Multicast packets are droped in SUP22 when FWLB is operational
CSCsl32344	Unknown	Group of 4 ports on 6708 stops passing traffic
CSCsl52748	Unknown	SUP32 crash in tyfib_get_hw_index
CSCsl71339	Unknown	Prevent ssa interrupts from corrupting sfp i2c accesses
CSCsl74456	Unknown	VPN-SPA : TCAM not programmed on POS sub-interface after a reload
CSCsl74976	Unknown	Punted MPLS-tagged traffic causes control plane instabilities
CSCsl80682	Unknown	SPA crashes if crypto acl changed
CSCsl94393	Unknown	OPNEXT / Sup32 uplink port stays up when far-end port down.
CSCsl98238	Unknown	QoS statistics-export only exports to directly-connected destinations
CSCsm11898	Unknown	IOS:SLB: Incorrect NAT Translation when Nat client is enabled
CSCsm18546	Unknown	Root port is not selected with frameraly and bridge domain configs
CSCsm30858	Unknown	PIM register packets upmarked to TOS 6 by PTcam redirection
CSCsm31037	Unknown	URL maps are not properly downloaded to CSG
CSCsm37673	Unknown	Traffic from SSLM service module not going over multi-module etherchanne
CSCsm45453	Unknown	Missing 'lbusDrops' counter for WS-X6516A-GBIC in Native IOS
CSCsm48398	Unknown	mls cef adj leaking
CSCsm48410	Unknown	Vlan-based qos applied to channel when not configured after reload
CSCsm48913	Unknown	Transient SPI aging window is too long
CSCsm59039	Unknown	Message "ME_AR#0 WARNING: Cannot FLUSH Dic#0" seen for WS-X6708A-10 LC
CSCsm69112	Unknown	Multicast output drop w/ IGMP snooping @ near line rate 1Gbps
CSCsm70774	Unknown	Router crashes at cfg_kron_plcy_sbmd_cmd.
CSCsm73173	Unknown	Spurious memory access seen @ slb_lam_cfg_ft_track_interf
CSCsm79163	Unknown	Commit 8.6(0.306)R3V25 C2 FW libraries to the v122_18_sxf_throttle
CSCsm82382	Unknown	7600 standby RP memory leaking cause CEF disable
CSCsm83948	Unknown	CISCO7609 returns sysObjectId as ciscoProducts.402 (which is cisco7606)
CSCsm84257	Unknown	crash in ipflow_periodic context due to watchdog timeout
CSCsm86027	Unknown	B2B failover,ace_tunnel_compare:Invalid address_type, router crashed
CSCsm89251	Unknown	IPSec SA lifetime gets reduced during rekey
CSCsm94421	Unknown	Configuring STP cost in an etherchannel to the defaulthas no effect
CSCsm95456	Unknown	Duplicate L3 packets with 6708 and DEC
CSCsm97669	Unknown	Cat6K with NAT-T through PAT: IKE packets with src_port != 4500 dropped
CSCsm97775	Unknown	fix compile error for earl6

Identifier	Technology	Description
CSCsm99170	Unknown	Memory Leak seen in fw_lcp process
CSCso10819	Unknown	LC not reset after 10 consecutive failures of TestMacNotification
CSCso12903	Unknown	RE MET address check missing while running MET patch on IO bus timeout
CSCso17569	Unknown	VPN-SPA: WAN interface mtu incorrectly programmed on the SPA
CSCso20519	Unknown	Cheronia: Fix SMB drive strength programming.
CSCso31506	Unknown	IPv6 AH Extension Headers Punted to Software on PFC-3B & 3C
CSCso37640	Unknown	DHCP snooping ACL's are not getting programmed after switchover.
CSCso38129	Unknown	Tracebacks seen on standby & switch crash after switchover w/ct3 config
CSCso53741	Unknown	VPNSPA does not handle duplicate IPSec SA correctly in nested tunnel
CSCso81945	Unknown	removing natpool doesn't remove from the slb-policy automatically
CSCso89550	Unknown	cat6k crash due to SP: Supervisor has bad local fabric channel
CSCsq00884	Unknown	"mls qos trust" cmd lost under port-channel interface when upgrading IOS

Resolved Caveats in Release 12.2(18)SXF13

Resolved Infrastructure Caveats

- CSCsk33054—Resolved in 12.2(18)SXF13

  This is the Cisco Product Security Incident Response Team (PSIRT) response to a vulnerability that was reported on the Cisco NSP mailing list on August 17, 2007 regarding the crash and reload of devices running Cisco IOS after executing a command that uses, either directly or indirectly, a regular expression. The original post is available at the following link:

  http://puck.nether.net/pipermail/cisco-nsp/2007-August/043002.html

  The Cisco PSIRT posted a preliminary response on the same day and is available at the following link:

  http://puck.nether.net/pipermail/cisco-nsp/2007-August/043010.html

  Preliminary research pointed to a previously known issue that was documented as Cisco bug ID CSCsb08386 (registered customers only) , and entitled “PRP crash by show ip bgp regexp”, which was already resolved. Further research indicates that the current issue is a different but related vulnerability.

  There are no workarounds available for this vulnerability. Cisco will update this document in the event of any changes.

  The full text of this response is available at

  http://www.cisco.com/en/US/products/csr/cisco-sr-20070912-regexp.html

Resolved Security Caveats

- CSCsi17158—Resolved in 12.2(18)SXF13

  Symptoms: Devices running Cisco IOS may reload with the error message “System returned to ROM by abort at PC 0x0” when processing SSHv2 sessions. A switch crashes. We have a script running that will continuously ssh-v2 into the 3560 then close the session normally. If the vty line that is being used by SSHv2 sessions to the device is cleared while the SSH session is being processed, the next time an ssh into the device is done, the device will crash.

Conditions: This problem is platform independent, but it has been seen on Cisco Catalyst 3560, Cisco Catalyst 3750 and Cisco Catalyst 4948 series switches. The issue is specific to SSH version 2, and its seen only when the box is under brute force attack. This crash is not seen under normal conditions.

Workaround: There are mitigations to this vulnerability: For Cisco IOS, the SSH server can be disabled by applying the command **crypto key zeroize rsa** while in configuration mode. The SSH server is enabled automatically upon generating an RSA key pair. Zeroing the RSA keys is the only way to completely disable the SSH server.

Access to the SSH server on Cisco IOS may also be disabled via removing SSH as a valid transport protocol. This can be done by reapplying the **transport input** command with 'ssh' removed from the list of permitted transports on VTY lines while in configuration mode. For example: **line vty 0 4 transport input telnet end**

If SSH server functionality is desired, access to the server can be restricted to specific source IP addresses or blocked entirely using Access Control Lists (ACLs) on the VTY lines as shown in the following URL:

http://www.cisco.com/en/US/docs/switches/lan/catalyst2950/software/release/12.1_9_ea1/configuration/guide/swacl.html

More information on configuring ACLs can be found on the Cisco public website: http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00800a5b9a.shtml

Resolved Unknown Caveats

- CSCsg35077—Resolved in 12.2(18)SXF13

  Symptoms: A device that is running Cisco IOS software may crash during processing of an Internet Key Exchange (IKE) message.

  Conditions: The device must have a valid and complete configuration for IPsec. IPsec VPN features in Cisco IOS software that use IKE include Site-to- Site VPN tunnels, EzVPN (server and remote), DMVPN, IPsec over GRE, and GET VPN.

  Workaround: Customers that do not require IPsec functionality on their devices can use the **no crypto isakmp enable** command in global configuration mode to disable the processing of IKE messages and eliminate device exposure.

  If IPsec is configured, this bug may be mitigated by applying access control lists that limit the hosts or IP networks that are allowed to establish IPsec sessions with affected devices. This assumes that IPsec peers are known. This workaround may not be feasible for remote access VPN gateways where the source IP addresses of VPN clients are not known in advance. ISAKMP uses port UDP/500 and can also use UDP/848 (the GDOI port) when GDOI is in use.

  Further Problem Description: This bug is triggered deep into the IKE negotiation, and an exchange of messages between IKE peers is necessary.

  If IPsec is not configured, it is not possible to reach the point in the IKE negotiation where the bug exists.

Other Resolved Caveats in Release 12.2(18)SXF13

Identifier	Technology	Description
CSCee89849	AAA	Router reloaded at vtemplate_build_command_strings
CSCsc98046	AAA	TACACS Accounting isn't sending stop time in the stop packet.

Identifier	Technology	Description
CSCsf30451	AAA	radius-server attrib 32 include-in-access-req/accounting-req not sent
CSCsh46990	AAA	Console hangs with enable/line as aaa fall-back methods
CSCsl33966	AAA	C6509 : attribute 32 nas-Id not sent for Auth (missed by CSCsf30451) .
CSCsm06740	AAA	Memory Leak in AAA accounting and Virtual Exec
CSCsl41784	Access	ION: ARP Input memory leak with "mobile ip arp"
CSCsd84347	ATM	PVC stops sending OAM loopback if AIS/RDI received
CSCse13374	ATM	IMA ports on 7600 always initialized to default clocking on bootup .
CSCsl65335	Content	WCCP: reload following ACL update
CSCsa65031	Infrastructure	show rtr distriution-statistics inactive status
CSCsb66972	Infrastructure	show memory shows negative numbers with 4GB RAM
CSCsh42866	Infrastructure	Static analysis on SNMP code
CSCsi15080	Infrastructure	RP crash when listing files by using the context-sensitive help
CSCsj83966	Infrastructure	Syslog traps cause CPUHOG when lot of interface come up at same time. .
CSCsk06492	Infrastructure	snmp-server drop vrf-traffic implementation in 12.2 SRB train
CSCsk37278	Infrastructure	BFD clients flaps when boot string is removed from "show running" .
CSCsg60447	IPServices	7200: BVI stops receiving CLNS/ISIS packets
CSCsh58099	IPServices	ftp process should call a registry cleanup- Message Could not register..
CSCsj29841	IPServices	Port forwarding breaks NAT-overload on a 6509
CSCsk29013	IPServices	IGMP groups in the vrf not rejoined after executing a cle ip mr vrf
CSCsk39022	IPServices	Modular IOS: ip directed-broadcast not working
CSCsl10348	IPServices	Crash writing to or from ftp/tftp server in modular IOS
CSCsl36293	IPServices	Bus Error crash at standby_arp_add_if while config-change .
CSCsm54171	IPServices	Crash seen with "copy runn tftp" and large hostname in modular IOS
CSCsh34949	LegacyProtocols	DLSW router crash with Bus Error
CSCdy83805	MPLS	%MPLS_TE-3-CONSISTENCY: consider replacing errmsg with buginf
CSCsa70235	MPLS	LDP doesnt withdraw all labels after routes gone
CSCsd55004	MPLS	FRR path gets reoptimized while in Active state
CSCsk30567	MPLS	local label for inter-as vpn not programmed on LC Eng 5 on an ASBR .
CSCsk36276	MPLS	SXF11: on SSO switchover tracebacks are seen at network_redist_ndb_updat
CSCsk55768	MPLS	TAG adj doesn't recover after flap
CSCsl72702	MPLS	MPLS should not allocate labels on standby RP in HA setup
CSCeg85087	Multicast	S,G expire timer set to 3:00 when no downstream pim join
CSCsg95192	Multicast	no ip rp-address <ACL name> causes an address error
CSCsh56720	Multicast	CPUHOG/Watchdog timeout when using igmp static group class-map cmd
CSCsh78277	Multicast	Sierra: mwheel CPUhog on RPF link failure causing crash .
CSCsl20422	platform-76xx	PXF points incorrect adjacency
CSCsl27840	PPP	Router may Crash / Hang, Module Reset @ Shut ATM member + MLPOA

Identifier	Technology	Description
CSCse18146	QoS	SIP1-CT3: SIP1 crashed after switchover @giant_node_process .
CSCsi73132	QoS	Multicast DSCP value not copied to PIM-SM RP-register packet
CSCsk53642	QoS	RSVP PATH msg not forwarded to MCAST receiver .
CSCsk63794	QoS	FlexWAN WS-X6582-2PA + T3+ Serial PA may crash/reload
CSCsk79703	QoS	SIP-200 crashes when moving MFR bundle from OSM to SIP-200
CSCsl70734	QoS	Commiting CSCsk53642 broke build.
CSCee04303	Routing	Spurius Memory access during boot while processing an isis update
CSCeg25475	Routing	Distribute-list configured in ipv4 acts in vpnv4 address-family
CSCsf00171	Routing	summary route not flushed from ospf database
CSCsh82953	Routing	EIGRP pece routes missing extcomm attrs after redistribution to BGP .
CSCsi80057	Routing	RIP default-information originate with route-map not working correctly .
CSCsj78403	Routing	clear ip bgp causes crash to RR client with conditional route injection
CSCsj99269	Routing	BGP: VPNv4 general scanner runtime close to 1 hour at boot time .
CSCsk34344	Routing	Wrong share-count 1:10 via confed-external BGP peers using dmzlink-bw
CSCsk70844	Routing	%SYS-4-REGEXP: new engine: regexp compilation had failed -BGP Router
CSCsl07297	Routing	SXF11: BGP "no neighbor" command caused Address Error exception .
CSCsl47915	Routing	Redistribution of ospf in rip with prefix-list not working properly
CSCsm17391	Routing	ISIS routes are not learned through interfaces
CSCsm27979	Routing	router may crash for "address error exception" doing sh ip route vrf
CSCsg48392	Security	Resuming SSH Session Fails After Disconnecting Another One (Not Console)
CSCsj45031	Security	Cat6k unable to SCP files from Tectia ssh server
CSCsm22805	Security	hsrp crypto map config got removed after reload
CSCsm32840	Security	Router crash in dmvpn-vrf setup after cheronia reset
CSCeb69473	Unknown	connect '/terminal-type' command memory corruption
CSCee13737	Unknown	CSM - sho mod csm # sticky reports invalid # of connections
CSCei28317	Unknown	PIM-6-INVALID_RP_JOIN reports 0.0.0.0 for source of invalid neighbor
CSCei49932	Unknown	Out-Discard counter showing value of zero on WS-X6148-GE-TX
CSCek45036	Unknown	Interuppt throttling to be implemented for Sibyte Modular IOS images.
CSCek55870	Unknown	fabric buffer-reserve queue default issues
CSCek76062	Unknown	Router crashed @ validmem_complete_interrupt .
CSCin67287	Unknown	NxDS0 BERT capability on PA-MC-8TE1+
CSCin89549	Unknown	Router crashes if AAA returns ipv4 address attrib with no xauth
CSCsb36463	Unknown	RF-bit not set in the DBUS hdr for the FS switched+RTD port snooped pkt
CSCsc56179	Unknown	mac-address is not purge when interface is shutdown .
CSCsd18278	Unknown	Host backpressure is not handled by SPA IPC firmware code
CSCsd66406	Unknown	SP error msg is not printed part of syslog levels
CSCsd90173	Unknown	TestIPSecEncrypDecrypPkt HM test config init error reporting is needed

Identifier	Technology	Description
CSCse31973	Unknown	NF double counts packets when span is configured.
CSCsf32441	Unknown	ALIGN-3-CORRECT: messages from process_t1e1s
CSCsg27123	Unknown	Learning not disabled on SPAN dest without learning option
CSCsg29305	Unknown	hw-module subslot reload crashes the router .
CSCsh17328	Unknown	WS-SVC-WISM-1-K9 reports 0.0 in entPhysicalVendorType
CSCsh23961	Unknown	Multicast netflow not working for Vlan interface (SVI)
CSCsh64639	Unknown	VS2: [dead threads] process takes a large chunk of CPU util
CSCsh83109	Unknown	HapiEchoTest fails on SPA-IPSEC-2G when reset.
CSCsh84657	Unknown	STP Loopguard: Ability to disable loopguard for Po270 and higher for FWM
CSCsh85531	Unknown	E1 channels down after PE reload
CSCsh88532	Unknown	Auto-LAG EtherChannel not configurable; doesn't trust QoS. .
CSCsh97395	Unknown	IDSM: Monitor config was removed after RPR switchover
CSCsi00706	Unknown	Sierra: upon fib tcam exception to use ratelimiter and not reload
CSCsi52382	Unknown	radius attribute 5 nas-port not sent in access-request for RA VPN users
CSCsi74194	Unknown	18SXF: Egress SPAN may cause high CPU
CSCsi79991	Unknown	VACL capture not supported for the GE-WAN or GigabitEthernet on SIP-400
CSCsi98587	Unknown	Excessive MET refs and memleak after ipv4 stress, crash follows .
CSCsj00385	Unknown	logging event link-status default negates existing interface config
CSCsj07935	Unknown	%CONST_DIAG-SP-2-HM_MOD_RESET:Failed TestFabricCh0Health .
CSCsj10375	Unknown	802.1X: VLAN Changing on port causes link to go down
CSCsj27352	Unknown	RX Priority q-limit is set to default after reload
CSCsj37078	Unknown	permit missing for internal vlan acl - causing vrf connectivity failure
CSCsj72438	Unknown	Control plane instability and %EARL-DFC3-2-SWITCH_BUS_IDLE: Switching bu
CSCsj83102	Unknown	crash upon card type configuration on WS-X6582-2PA / PA-MC-8TE1+
CSCsk30146	Unknown	Router crashed %DUMPER-3-PROCINFO: pid = 12315: (sbin/ios-base) SIGBUS
CSCsk40931	Unknown	Port Security Inactivity Aging is not working as expected
CSCsk41134	Unknown	ISAKMP SA neg not successful for in tunnel mode w/ RSA-SIG
CSCsk55423	Unknown	7600's SPD implementation allow COS 5 or above in Extended headroom
CSCsk58040	Unknown	WS-X6148A-GE-45AF retains previous modules MACs after OIR
CSCsk77164	Unknown	Connectivity problems to addresses switched based on aggregate label
CSCsk84237	Unknown	SIGSEGV, Segmentation violation in rf_proxy_fatal_error . .
CSCsk84944	Unknown	unidirectional Ethernet UDE is broken on WS-6704 after SW upgrade
CSCsk91267	Unknown	Module fails to come up with (FRU-power failed)
CSCsl00130	Unknown	GRE tunnel not HW accelerated after reboot when source from HSRP address
CSCsl08912	Unknown	Vlan access list not working when have "xconnect vfi #" under the SVI
CSCsl08952	Unknown	rapid link changes causes memory leak on sup32 int with service policy
CSCsl12827	Unknown	Handling Transit IpSec in VRF mode

Identifier	Technology	Description
CSCsl18765	Unknown	6500-7600 : SPAN of EoMPLS port causes packet reflection or loop
CSCsl19708	Unknown	Naxos : Disable Telesto Internal TERMINATION For Reference Clock, PB RAM
CSCsl21106	Unknown	Tunnel destination command crashes MSFC running in hybrid mode .
CSCsl26033	Unknown	Modifying the BFG doesn't re-create the SA's
CSCsl26997	Unknown	Catalyst 6500 may crash when reseting VPNSM module .
CSCsl27236	Unknown	%SYS-3-CPUHOG: Task is running for (126000)msecs, causes RP crash .
CSCsl30750	Unknown	Memory leak after create-apply-remove-delete policies on QM Process RP
CSCsl32122	Unknown	Remote Access for certificate users fails during mode config
CSCsl34647	Unknown	18SXF: RPR RF Keep alive swover not working
CSCsl49734	Unknown	IF_INDEX_ILLEGAL errors and crash due to memory corruption on standby RP
CSCsl51380	Unknown	Sup720 and Sup32 TCAM & SSRAM Consistency Checkers refinement
CSCsl52092	Unknown	DHCP db agent considers port-channel interface (poX) as invalid
CSCsl53494	Unknown	C7600-SSC-400: Error message display incorrect product name
CSCsl59553	Unknown	SIP-400: bursty traffic causes packet drop even in low rates
CSCsl61086	Unknown	urpf global disable even some intf with urpf
CSCsl63311	Unknown	6500 May Experience High CPU due to NAT traffic
CSCsl68327	Unknown	Packet loss during rekey
CSCsl70148	Unknown	PIM enabled p2p Crypto GRE Tunnels not installed in Hardware
CSCsl70634	Unknown	67xx EC tx/rx traffic dependency resulting in low throughput
CSCsl75136	Unknown	Cat6k with Sup32 failed to boot up after power cycle.
CSCsl75719	Unknown	sxf13 show int tunnel with blank display
CSCsl83211	Unknown	Sup32 running ION image fails to bootup after a power-cycle.
CSCsl84317	Unknown	Active crashes on applying acl to EoMPLS subif on SIP-600
CSCsl89069	Unknown	Zamboni crashed at illegal event/state combinationin CfgMonInd, clear sa
CSCsl89176	Unknown	Cat6k may crash when vlanTrunkPortEntry is polled via snmp
CSCsl97653	Unknown	bcm2_5421_isr bcm2_num: 1 messages seen in the log
CSCsm01129	Unknown	Back-out the ubins commit done in CSCse31973
CSCsm01399	Unknown	Bus idle recovery may cause 10GE interface to remain down
CSCsm05486	Unknown	mtu mis probram in adj thru tunnel interface after b2b failover
CSCsm08419	Unknown	debounce timer issue on sup32 10GE uplink and 6708
CSCsm15350	Unknown	vpnspa crashed at assert failure in l2-mcpu.c on line
CSCsm17983	Unknown	Memory corruption by l3_mgr_e7_fmask_init_platform
CSCsm21126	Unknown	C7600-SSC-400: Resync fabric interface on fabric error
CSCsm32493	Unknown	Backout of CSCsh94882
CSCsm35364	Unknown	SPA-IPSEC-2G get reload automatically by RP
CSCsm67778	Unknown	To make CSCsl68327 patch friendly and restore the symbols
CSCsj68446	WAN	NTP will not sync - NTP packets received but ignored by NTP process .

Resolved Caveats in Release 12.2(18)SXF12a

Identifier	Product	Component	Description
CSCsm06740	all	aaa	Memory Leak in AAA accounting and Virtual Exec

Resolved Caveats in Release 12.2(18)SXF12

Resolved Caveats for Product 'all' and Component 'aaa'

- CSCsj91123—Resolved in 12.2(18)SXF12

  Symptom:

  Double freeing of freed memory. Router reloads after authentication attempt fails on vty/console.

  Conditions:

  While performing aaa accounting, the accounting structure was freed twice. Which results in crash. The below CLI is configured **"aaa accounting send stop-record authentication failure"** which sends a stop record for authentication failure.

  Workaround:

  Remove **"aaa accounting send stop-record authentication failure"** , which will disable sending of the stop record at authentication failure.

Resolved Caveats for Product 'all' and Component 'dlsw'

- CSCsk73104—Resolved in 12.2(18)SXF12

  Cisco IOS contains multiple vulnerabilities in the Data-link Switching (DLSw) feature that may result in a reload or memory leaks when processing specially crafted UDP or IP Protocol 91 packets.

  Cisco has released free software updates that address these vulnerabilities. Workarounds are available to mitigate the effects of these vulnerabilities.

  This advisory is posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20080326-dlsw.html

Resolved Caveats for Product 'all' and Component 'ifs'

- CSCsk61790—Resolved in 12.2(18)SXF12

  Symptoms: Syslog displays password when copying the configuration via FTP.

  Conditions: This symptom occurs when copying via FTP. The Syslog message displays the password given by the user as part of syntax of FTP copy.

  Workaround: There is no workaround.

Other Resolved Caveats in Release 12.2(18)SXF12

Identifier	Product	Component	Description
CSCsj89305	all	aaa	RADIUS/NAS-IP address is sent out as 0.0.0.0
CSCse20115	all	ata-filesystem	System hangs when writing to a file, when the disk space is full
CSCek61180	all	atmcommon	crash @ write_to_url, doprintc_core, atm_remove_vc
CSCsc75426	all	bgp	Crash when BGP sends update with bad attribute .
CSCsg16778	all	bgp	router may crash at bgp_update_nbrsoo after deleting BGP neighbor .

Identifier	Product	Component	Description
CSCsg55591	all	bgp	MPLS VPN Local label not allocated/programmed for sourced BGP network
CSCsj56086	all	cat6000-acl	WCCP and VACL cause Cisco router CPU High
CSCsk41374	all	cat6000-acl	device crash seen when auth-proxy enabled on the LPIP vlan .
CSCsh99116	all	cat6000-fib	bits/sec counter is way off in show int vlan
CSCsa79984	all	comm-serv	CTRLC_ENBL should be cleared when line is reset
CSCsi58303	all	eigrp	eigrp resync peer graceful-restart repeatedly after reload .
CSCsj25940	all	eigrp	%SYS-2-NOTQ: unqueue didn't find 6433F698 in queue .
CSCsc38968	all	fr	Frame-relay EEK failure does not keep subinterface down
CSCsj84641	all	install	some patches failed to commit during install commit of 41 patches.
CSCek76776	all	ip	ip interface settings persistent after deleting/adding sub-interface
CSCsk46195	all	ip	Arp entry does not age out with private vlans and no ip sticky-arp
CSCsk26719	all	ip-acl	show ip access crash with per-user acl
CSCsk26973	all	ipsec-dmvpn	Memory leak in nhrp_cache_delete for incomplete cache entries
CSCsk21328	all	ipv6	6504 crashes in IPV6
CSCsk65482	all	loadbal	clear ip slb CLI is defined with wrong privilege level
CSCsf13044	all	mcast-vpn	MVPN: Bidir mroute OIF missing - pim joins not received from MDT tunnel
CSCej00319	all	mpls-ldp	RP Crash for E2 E3 E4 E4P interaction
CSCsk05059	all	mpls-lfib	NRT: traceback tfib_post_table_change_ tfib_ipfib_ ip_fib_table_
CSCsk52331	all	mpls-lfib	Xconnect configuration triggers entire fib table walk
CSCsb67427	all	mpls-vpn	Label not allocated for imported iBGP in ASBR/PE after flap 'mpls ip'
CSCeh56158	all	nat	NAT outside source translation fails for GRE packets .
CSCsd80770	all	netflow-switch	Netflow exports UDP packets with source port 0
CSCir01217	all	neutrino	name_svr.proc[64]: Could not register interest
CSCsj17820	all	nhrp	Hub crashes during unconfiguration due to program counter error
CSCek33384	all	ospf	Tunnels stay down after cutover at MPLS head test cases
CSCsl14632	all	ospf	SXF12:%LDP-5-NBRCHG: LDP Neighbor is down after SSO Switchover .
CSCef54653	all	ppp	Members inactive in a multilink bundle except the first member. .
CSCsd30719	all	ppp	A2A: Stdby sup crashes @ mlp_remove_link .
CSCek78675	all	qos	SIP200 crash at hqf_cwpa_pak_enqueue_local during qos test .
CSCsh91974	all	security	PIM CLI causes RP crash when issued under control-plane subconfig prompt
CSCsg39295	all	snmp	Syslog Displays Password if SCP or FTP Selected in CISCO-COPY-CONFIG-MIB
CSCsk61555	all	socket	Bus Error Exception in sock_tcp_directwakeup . .
CSCsk81396	all	socket	NAM process crash in 12.2SXF .
CSCsj60938	all	ssh	SCP with redirect option locks up console or VTY line .
CSCef52888	all	tcp	PMTUD: MSS is not adjusted which causes the BGP flaping .
CSCeh35980	all	tcp	after unconfig & config of BGP, seeing a crash in TCP .
CSCek68118	all	tcp	window scale option(03030001) occurs in debug ip tcp packet output .

Identifier	Product	Component	Description
CSCsj89544	all	tcp	TCP retransmissions get dropped below IP layer. .
CSCsk80935	all	udp	SXF12, SNMP response being broadcast .
CSCsh31782	all	vpn-sm	Bus error crash - show crypto isakmp sa
CSCsi91658	all	wccp	Wccp stops layer 2 redirection when dscp is present in the redirect acl
CSCsl04908	all	wccp	WCCP: shutdown of appliance i/f leads to c6k reload
CSCsl06110	c7600	c7600-acl	DHCP snooping agent: parse failures when importing the DB
CSCsk89335	c7600	c7600-env	After SSO switchover, see 6K DC power supplies mismatched .
CSCsk06769	c7600	c7600-lcsw-bridge	shut on L2 int cause packets to loop back on T1 int causing traffic loss
CSCsk19652	c7600	c7600-snmp	Failed to assert Physical Port Administrative State Down alarm
CSCsj95291	c7600	cat6000-fib	100% CPU (FIB Control Queue Process) after enabling MPLS .
CSCsj58538	c7600	ha-idb-sync	Lots of prowler/patriot interface go down for few second during sso swov
CSCsk66339	c7600	isis	ISIS fails remove native path from local RIB / del path from global RIB
CSCsk08765	c7600	osm-choc-ds0	Bus error when executing 'encapsulation frame-relay mfr' .
CSCsj76268	c7600	osm-ct3	Autosense LMI stops responding invalid lmi type on OSM-12CT3/T1
CSCsk19333	c7600	osm-gigwan	GE-WAN interface shows incorrect link state with ws-g5483 GBIC
CSCsk82821	c7600	tcp	The UUT not able to receive the Large ICMP message.
CSCsi51649	cat6000	cat6000-acl	RP crashes@fm_send_inband_install_message+21C in many cases with NAT
CSCsj60883	cat6000	cat6000-acl	Error msg. Unable to change flowmask to full-flow because Cx is configur
CSCsk21414	cat6000	cat6000-acl	NAC : Buffer leak in small buffer pool .
CSCsk34237	cat6000	cat6000-acl	Egress multicast replication broken due to wccp .
CSCsj68911	cat6000	cat6000-cm	DFC mem leak in SP Logger Proces when redundancy force-switchover issued
CSCsc98471	cat6000	cat6000-diag	show diagnostic sanity fails to check software modularity boot string .
CSCsk60874	cat6000	cat6000-diag	show tech needs 'show diagnostic results' and 'show diagnostic events' .
CSCsk27835	cat6000	cat6000-env	Disable unsupported service modules in SXF Software Modularity images
CSCsk80934	cat6000	cat6000-env	Add errmsg to clearly indicate if lc reset due to power convertor failur
CSCsk33661	cat6000	cat6000-fabric	show platform hardware capacity should include LTL usage .
CSCsk83646	cat6000	cat6000-firmware	BX10 ports don't link-up after Centaurus resets . .
CSCsh34467	cat6000	cat6000-ha	Standby constanly reset due to RF request with large configuration .
CSCsk80787	cat6000	cat6000-ha	SXF12 CLI: system crash when create Po interfaces . .
CSCsk18206	cat6000	cat6000-hw-fwding	TCAM adjacency hardware programming problem with PBR and NAT .
CSCsk70087	cat6000	cat6000-hw-fwding	Sup720 TLB exception created by fill_earl_vlan_stats_hdr .
CSCsc75381	cat6000	cat6000-l2	Native vlan mismatch is not detected if native not allowed on trunk .
CSCsg50698	cat6000	cat6000-l2	18SXF: set entPhysicalAlias of XENPAK cause stdby-reset .
CSCsk33724	cat6000	cat6000-l2	DOM does not work anymore for cwdm gbic/sfp
CSCsh33518	cat6000	cat6000-l2-infra	STP information is not in sync with Active .
CSCsh97848	cat6000	cat6000-l2-infra	Sierra: LACP pdus should be untagged .
CSCsk83524	cat6000	cat6000-l2-infra	L3 physical interface input drop counter is incorrect .

Identifier	Product	Component	Description
CSCse59209	cat6000	cat6000-lacp	Seeing spurious mem trace back when change etherchannel mode to pagp
CSCek73332	cat6000	cat6000-mcast	Bidir shadow entry is missing some interfaces in oif
CSCsk02962	cat6000	cat6000-mcast	Supervisor Reload after SSO switchover on Multicast MET reconstruction .
CSCsk03679	cat6000	cat6000-netflow	VS2: show mls nde intermittently causes ALIGN-3-SPURIOUS T/B's
CSCsd43185	cat6000	cat6000-qos	Tx queue cos maps for even ports of card WS-X6416-GBIC are incorrect.
CSCsl15604	cat6000	cat6000-qos	Uplink Port becomes untrusted after SSO and shut/no shut of egress port
CSCsl21934	cat6000	cat6000-qos	Port is untrusted after SSO & shut/noshut of any port sharing same asic
CSCsk55012	cat6000	cat6000-snmp	setting portDuplex from 'full' to 'full' may cause standby reset .
CSCsk58810	cat6000	cat6000-snmp	should NOT allow enable port-security on negotiating trunk interface .
CSCsb83142	cat6000	cat6000-span	SPAN / Monitor instances in IOS report ifOperStatus wrongly as down
CSCsg21809	cat6000	cat6000-statistics	Add bridge asic status collection support .
CSCsk24272	cat6000	cat6000-sw-fwding	SUP720-3B RP Crash due to I/O Buffer Leak by NDE w/ NAM 127.0.0.x Addr
CSCsj85485	cat6000	eigrp	EIGRP NSF - MSFC switchover causes hello's to be sent over passive intf
CSCsk88656	cat6000	osm-gigwan	Cat6k: link-flap is observed on OSM-2+4GE-WAN+ after reload .
CSCsd18296	cat6000	osm-qos	Bdwth guarantee not met in cbwfq when cfged with llq in child in MIV .
CSCek39186	cat6000	spa-ipsec-2g	MAC-address for HSRPs VIP not in FVRF vlan if tunnel redirected .
CSCsd92208	cat6000	spa-ipsec-2g	vlan map ocpu is wrong in the active vpnspa after sso+b2b failover .
CSCsk33740	cat6000	spa-ipsec-2g	replay window size of 1024 causes IPSec Policy Check and Replay Failure
CSCsl13477	cat6000	spa-ipsec-2g	SSO not working with crypto maps terminating at same peer address .
CSCsc77148	unknown	novell	Router crash while issuing show ipx cache command. Cleanup SA warnings.

Resolved Caveats in Release 12.2(18)SXF11

Identifier	Technology	Description
CSCsh23142	AAA	aaa local authentication not happening for authproxy .
CSCsh59019	AAA	Avoiding AAA client hangs, if a protocol subsystem is not present.
CSCsj97165	AAA	%AAA-3-BADMETHODERROR: Router crash @ aaa_get_new_acct_reg_type .
CSCsc57207	Access	itevent flooding: code 10 arg0 0 arg1 0 arg2 0 error messages on 7200
CSCsi00099	Access	Spurious Memory Access Error @ ct3sw_check_freedm_fifo
CSCsj37071	Access	PA-MC-E3 will not recover after workload stress
CSCed17607	ATM	Reapplying oam-pvc manage does not send oam cells until shut/no shut
CSCsj57084	ATM	Voice packets in LLQ experience latency
CSCsj78525	ATM	%ALIGN-3-CORRECT, %ALIGN-3-TRACE on the 7500 with 123-22
CSCeg88630	Infrastructure	E3 GE:Linkdown trap via snmp not properly raised
CSCei79855	Infrastructure	IOS resilience fails to work properly with secure boot command .
CSCek56630	Infrastructure	race condition in process_sleep_on_timer code

Identifier	Technology	Description
CSCsb95806	Infrastructure	Incorrect 64bit counter on 1Gb MPLS interface via SNMP .
CSCsg15939	Infrastructure	Switches crash after remove/plug in compact flash
CSCsg43466	Infrastructure	%IPC-5-INVALID: Invalid Dest Port w/ TB @ ipc_xmt_account after SSO
CSCsg71381	Infrastructure	Disabling cisco-specific lsa and tty, removea all ospf trapa from conf
CSCsh28948	Infrastructure	High CPU for sh run/wr mem with PTA sessions up
CSCsh48919	Infrastructure	Embedded spaces in DOSFS dirs/file names cause crash in some platforms
CSCsj58223	Infrastructure	Bus Error after 'show memory' .
CSCsj92874	Infrastructure	Catalyst 6500 May Not Send linkup/linkdown SNMP Traps and may reload
CSCsk10335	Infrastructure	Traceback @ ipc_send_message_blocked during bootup .
CSCsk38461	Infrastructure	Show platform hardware command getting rejected .
CSCeb76035	IPServices	Spurious access or crash from snmp_trap_for_tty
CSCeh65511	IPServices	Connected int IP may not be reachable with a static NAT trans
CSCsg97662	IPServices	Cant disable skinny (tcp 2000) .
CSCsi10974	IPServices	Error configuring dhcp option 67
CSCse13882	LegacyProtocols	Show dlsw peer caused router to crash
CSCsj98895	LegacyProtocols	v2-single-tcp peer connection is established on a non confg/prom peer
CSCsg88433	Management	IP Telephone issues seen with Dhcp snooping and NAC posture validation
CSCsk09197	MPLS	RSVP hello instance remains at shut-down interfaces
CSCek26940	Multicast	Need to unhide interval for send-rp-discovery
CSCsg24505	Multicast	PIM-DM Assert winner does not always send prune
CSCsi03359	Multicast	Sending extra PIM hello if the first one does not go through
CSCsj64230	Multicast	bidir DF election should not be restarted on a downstream interface
CSCsi98355	platform-76xx	LOP does not bring the line protocol down on OSM-1OC48-POS
CSCsj64023	platform-76xx	MPLS: Sup2 OSM sending TTL=0 packets on MPLS VPN
CSCsj93609	platform-76xx	Missing DS3-MIB table entries for OSM-1CHOC12/T3
CSCsj93636	platform-76xx	Incorrect value returned for dsx3TotalUASs
CSCse28421	PPP	%AAAA-3-BADSTR error when Multilink interface goes down .
CSCsd17641	QoS	SIP-400 QOS: after changing hier. policy, the policy no longer attaches
CSCee04271	Routing	eigrp does not send update of poisoned route to stub router
CSCee19119	Routing	IP installs route for PPP interfaces that did not complete IPCP
CSCee73221	Routing	Split Horizon is in effect on redistributed static routes .
CSCei93768	Routing	check heaps CHUNKBADMAGIC crash at BGP Router when remove dmzlink ba .
CSCek62005	Routing	ip prefix list deletes lists before sending notif (causing rtr crash
CSCsc73725	Routing	EIGRP packet pacing should have lower minimum value
CSCsc83742	Routing	BGP MAXPFX Sylog message does not include VRF tableid info
CSCsc98835	Routing	CPUHOG when access-list is modified causes OSPF and BGP session drops .
CSCsd11019	Routing	Rainier:After RPR-Plus switchover standby RP crashes

Identifier	Technology	Description
CSCsd74189	Routing	show ip bgp vpnv4 vrf NAME community-list NAME gives error mesg.
CSCsf05579	Routing	ISIS passive-interface default problem in IOS 12.2(18)SXF
CSCsg21418	Routing	Bus error related to CLNS fast switching
CSCsg40507	Routing	SIERRA:ISIS/BFD session doesnt come up after changing ip-addr of interf
CSCsg71797	Routing	bgp bestpath as-path multipath-relax - command crashes Supervisor card
CSCsg95101	Routing	ALIGN-3-SPURIOUS: Spurious memory access
CSCsh57509	Routing	RIPv2 does not delete redundant paths with different next hops .
CSCsh88825	Routing	bgp: advertisement-interval not nvgened for peer-groups
CSCsi11438	Routing	OSPF does not remove maxage LSAs and age goes to bigger than 16 bit
CSCsi14346	Routing	EIGRP: neighbor command missing in VRF.
CSCsi20281	Routing	Static route redistribution into RIP fails on ACL change
CSCsi25729	Routing	ISIS doesn't enable BFD except after micro reload
CSCsi57971	Routing	ISIS does not advertise prefix of passive interface
CSCsi58867	Routing	CPUHOG After show ip route static or show ip route connected
CSCsj06265	Routing	Switch crashes when doing clear ip ospf process
CSCsj17950	Routing	ISIS redistributed static routes might not be advertised
CSCsj72039	Routing	Prefix not in ISIS database if serial interface and passive
CSCsj77819	Routing	After SSO traffic is punted to the CPU for 20 seconds
CSCsk27685	Routing	FIB-DFC2-4-FIBMSG: Invalid message received On bootup .
CSCdz55178	Unknown	QoS profile name of more then 32 chars will crash the router .
CSCef82084	Unknown	Spurious memory access in pot1e1_tx_interrupt
CSCei76590	Unknown	Different wattage WS-CAC-4000W-US caused PSREDUNDANTMISMATCH output
CSCej02181	Unknown	SLB: cannot configure weight 0
CSCek66590	Unknown	C7600-SSC-400: Crash in show hw-m subslot x status volt
CSCek67701	Unknown	SPA-IPSEC-2G: Crashdump not getting saved on NMI .
CSCek68218	Unknown	sip-600 crashing with diagnostics error online_wan_diag_rp_request
CSCek72777	Unknown	%CWAN_HA-STDBY-4-IFCFG_PLAYBACK_ERROR for 7600 SIP card .
CSCin67370	Unknown	Changing ACL or the crypto map leaves it empty ident tree .
CSCsb29131	Unknown	show crypto ipsec sa identity detail causes system to reload
CSCsb62762	Unknown	Crash no vlan access-map test .
CSCsc28731	Unknown	chassisFanStatus is minorFault when one fan is present on WS-C6509-NEB-A
CSCsd13448	Unknown	IOS SLB custom udp probes don't support faildetect
CSCsd66276	Unknown	IDSM: monitor session dest config removed after two sso switchovers .
CSCsd77622	Unknown	show policy-map interface doesn't show drop counters .
CSCsd88768	Unknown	%SYS-2-BADSHARE: Bad refcount in datagram_done fix for PA-MCX-8TE1
CSCse17175	Unknown	Line down on some serilal interfaces for Chann STM-1 SMI PA
CSCse32876	Unknown	dot1x:cli missing for Ten Gig Ports for dot1x initialize/ reauthenticate

Identifier	Technology	Description
CSCse33420	Unknown	LACP: config for some other port-channel gets removed on bundling ports
CSCsf03730	Unknown	interface remains down even after E1 level local loopback on STM1
CSCsf17739	Unknown	Sup720 SVI does not show multicast traffic rate
CSCsf98341	Unknown	UDLD failed to receive PDU when linked to L3 port.
CSCsg09423	Unknown	IPSEC SAs dont recover after rekey with 3000 IKE SAs and PKI (RSA-Sig) .
CSCsg11616	Unknown	iprouting restart crashes Sup due to Block overrun at 5E64940 (red zone
CSCsg52355	Unknown	RHI Injected routes lost after SUP switchover
CSCsg52740	Unknown	OC48 OSM replicates same packet at line rate
CSCsg55315	Unknown	Packets duplicated out of Gig1/1 when SPAN Monitor session enabled
CSCsg72976	Unknown	CSM - need to add standby state to mib object slbRealServerState
CSCsg99914	Unknown	sip-200 power-cycles after BGP flap (not responding to keepalive)
CSCsh18773	Unknown	Incorrect link behavior with Xenpak
CSCsh33770	Unknown	contrl vlan not set; zamboni remains in initializing state .
CSCsh48983	Unknown	Sup720 GE uplink SFP port ->err-disable on reload of adj switch
CSCsh52941	Unknown	AUTHPROXY:CLI to increase the number of HTTP Proxy process
CSCsh53141	Unknown	IKE SA not getting deleted after clear crypto session
CSCsh80130	Unknown	Add warning/comments to interfaces when Auto Lag is used for interface
CSCsh92031	Unknown	Sierra: Standby RP crashed at auth_proxy_posture_clear_nacl
CSCsi09388	Unknown	VPNSM SA deleted by idle timeout
CSCsi10945	Unknown	Http Auth-proxy with OTP does not display token/SNK challange
CSCsi11874	Unknown	Sup720 DFC forwarding some packets to MSFC instead of hw switching
CSCsi22243	Unknown	Memory leak in *Dead* process due to HTTP Proxy Server
CSCsi24069	Unknown	Collect additional debug info for Modular IOS kernel crashes
CSCsi32655	Unknown	MOD CSG <#> config mode command applied to a running CSM clears config
CSCsi65363	Unknown	Not able to run to t1 loopback when using a PA-MC-T3 with flexwan
CSCsi76115	Unknown	r3:WiSM hw-module reset causes traceback. Cannot decode data descriptor
CSCsi87837	Unknown	IF-MIB does not support gig interfaces on SPA-IPSEC-2G
CSCsi90816	Unknown	show policy-map interface caused sup32 crash . .
CSCsi91324	Unknown	MCAST packet drop when other interface goes down on DFC
CSCsi93273	Unknown	Leak in Big buffer pool on SIP card with NetFlow-export version 9
CSCsi94863	Unknown	New xenpak background task .
CSCsi99234	Unknown	RP crash at validblock with %SYS-6-BLKINFO: Corrupted redzone blk
CSCsi99991	Unknown	When CMM is rebooted, FE goes into ErrDisabled state
CSCsj03722	Unknown	exit command is subject to authorization
CSCsj10744	Unknown	Input queue wedged with Inband Edit Packets on SIP-400
CSCsj11561	Unknown	Inconsistent MTU for Adj. entries used by MLS Netflow and MLS CEF
CSCsj14847	Unknown	crypto connect command dropped after reload on unchannelized 2CT3+ .

Identifier	Technology	Description
CSCsj18014	Unknown	Caller ID string received with extra characters
CSCsj18494	Unknown	Leak +MN to pfc to avoid flooding due to tx span .
CSCsj29583	Unknown	Add warning message to 12.2SXF when configuring PACL
CSCsj30109	Unknown	Cat6k with FlexWan & IPSEC AM making as unreachable BGP neighbors
CSCsj33042	Unknown	Cat6k crashes when unconfiguring vserver (CSM)
CSCsj34552	Unknown	ip address of vlan interface not programmed into spa-ipsec-2g
CSCsj35776	Unknown	Some of the VCs are INACTIVE after SPA OIR
CSCsj40286	Unknown	Interface counters stop working under heavy load
CSCsj42303	Unknown	6K installs ffff.ffff.ffff in CAM table under very specific conditions
CSCsj45951	Unknown	DOM Polling May Cause Link Flaps on Some Xenpak Transceivers .
CSCsj52192	Unknown	FE stays up when remote 'inline powered' is shutdown w/ 100Mbps/Full
CSCsj53663	Unknown	EEM: RP crashed at fh_fd_syslog_event_match
CSCsj56102	Unknown	Upgrade of DFC rommon fails in 12.2SX train IOS
CSCsj56703	Unknown	SSO failover causes RSTP forwarding and physical interfaces blocking .
CSCsj58287	Unknown	7600-SSC-400 crashes on reload
CSCsj61101	Unknown	FRR goes down after few mints when Explicit-null is enabled .
CSCsj64453	Unknown	HSRP support in protocol policing
CSCsj66829	Unknown	Switch crash with clear ip igmp snoop stat and show ip igmp snoop st
CSCsj67096	Unknown	Issue w/NATed traffic on PortChannel (WS-X6408 and WS-X6516) on Sup720
CSCsj68774	Unknown	SIP-600 SXF bus error in const_mpls_collect_imp_te_stats .
CSCsj72251	Unknown	BOOTP replies dropped if DHCP snooping is enabled
CSCsj73669	Unknown	Disable DOM hardware periodic updates (xenpaks/x2s)
CSCsj81067	Unknown	IPSec VPN SPA: OLD-CISCO-CHASSIS-MIB does not return cardType
CSCsj81502	Unknown	show pagp clis are not displaying the correct information .
CSCsj82051	Unknown	Cachelines not invalidated on ICPU in error case .
CSCsk09302	Unknown	CDP packets not received on WS-6704-10GE/CFC links with MLS QoS enabled
CSCsk12525	Unknown	Disabling 67xx line cards with DFC3C/DFC3CXL except WS-X6708-10GE
CSCsk16974	Unknown	Sup2 - Bus Asic #0 out of sync error .
CSCsk17205	Unknown	OSM:MFR LMI packets are not send out through the MFR i/f
CSCsk19590	Unknown	Mem Leak in IKE NODE causes router crash . .
CSCsk20887	Unknown	Packets are route cached on multilink bundle .
CSCsk28585	Unknown	stats is wrong for TE tunnel, right for physical interface for ip2tag .
CSCei22295	WAN	Traceback is seen at fr_svc_teardown_calls
CSCsb87686	WAN	Spurious Access when attempting to configure a connection on MFR bundle

Resolved Caveats in Release 12.2(18)SXF10a

- CSCsj92874—Catalyst 6500 May Not Send linkup/linkdown SNMP Traps and may reload

Resolved Caveats in Release 12.2(18)SXF10

Resolved IPServices Caveats

- CSCsh04686—Resolved in 12.2(18)SXF10

  Symptoms: With X.25 over TCP (XOT) enabled on a router or Catalyst switch, malformed traffic that is sent to TCP port 1998 causes the device to reload. This symptom was first observed in Cisco IOS Release 12.2(31)SB2.

  Conditions: This symptom is observed only when X.25 routing is enabled on the device.

  Workaround: Use IPsec or other tunneling mechanisms to protect XOT traffic. Also, apply ACLs on affected devices so that traffic is accepted only from trusted tunnel endpoints.

- CSCsi39674—Resolved in 12.2(18)SXF10

  Symptom: Devices may reload upon receiving multiple short lived TCP sessions to the telnet port.

  Conditions: Devices that run IOS and support IOS Software Modularity are affected. Images that support IOS Software Modularity will have "-vz" in their image name.

Resolved Security Caveats

- CSCsg40567—Resolved in 12.2(18)SXF10

  Symptoms: Malformed SSL packets may cause a router to leak multiple memory blocks.

  Conditions: This symptom is observed on a Cisco router that has the **ip http secure server** command enabled.

  Workaround: Disable the **ip http secure server** command.

Resolved Unknown Caveats

- CSCsi01470—Resolved in 12.2(18)SXF10

  A vulnerability in the Cisco implementation of Multicast Virtual Private Network (MVPN) is subject to exploitation that can allow a malicious user to create extra multicast states on the core routers or receive multicast traffic from other Multiprotocol Label Switching (MPLS) based Virtual Private Networks (VPN) by sending specially crafted messages.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available.

  This advisory is posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20080326-mvpn.html.

- CSCsi86396—Resolved in 12.2(18)SXF10

  Symptoms: Two subinterfaces may have the same CEF interface index.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router when the following configuration sequence occurs:

  1) Create subinterface 1, 2, and 3.

  2) Delete subinterface 1.

  3) Create subinterface 4.

  4) Enable subinterface 1.

  In this situation, subinterface 1 and 4 may have the same CEF IDB.

  Workaround: There is no workaround. You must reload the platform to clear the symptoms.

- CSCsi99869—Resolved in 12.2(18)SXF10

  Symptom: Bus error crash (signal 10) seen after the following error message:

  ```
  %MCAST-SP-6-GC_LIMIT_EXCEEDED: MLD snooping was trying to allocate more Layer 2
  entries than what allowed (7744)
  ```

  Conditions: This has been observed on a Catalyst6500 running IOS version 12.2(18)SXF1.

  Workaround: A workaround exist to disable ipv6 mld snooping via the command **no ipv6 mld snooping**.

  There is no negative impact of implementing the workaround as long as there is no IPV6 multicast traffic in the network.

- CSCsj16969—Resolved in 12.2(18)SXF10

  Symptom: A Cisco IOS device supporting IPv6 MLD may crash with a data bus error exception and stack trace PC = 0xA0000100

  Conditions: Device is running normal production traffic. Presence of malformed MLD packet in this network caused the issue.

  Workaround: Disabling MLD snooping on the VLAN or globally on the box will stop the crash.

- CSCsg70474—Resolved in 12.2(18)SXF10

  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)SXF10

Identifier	Technology	Description
CSCse69002	AAA	Accounting of auth failure doesn't work with some switches
CSCsb23106	Access	7206vxr with NPE-G1 bus error crash when OIR PA-2T3+
CSCdv70135	ATM	ATM QoS classes can not be configured.
CSCek39364	ATM	CLI: HA Standby router reloads while unconfiguring atm bundle .
CSCsb26631	ATM	Memory leak - ATM_PVCTRAP process
CSCsb54857	ATM	ATM shaping parameters removed from ATM vc-class for IMA upon bootup

Identifier	Technology	Description
CSCsg30875	Content	wccp blocking telnet to router
CSCsh98343	Content	WCCP redirect-list and mask-acl merge results in wrong redirect info
CSCsi05906	Content	WCCP:appliance failover does not update TCAM adjacency
CSCef66939	Infrastructure	VRF aware SNMP may generate trap with incorrect address
CSCeh65692	Infrastructure	Align Spurious memory access errors .
CSCeh74715	Infrastructure	SNMPv1 should not send traps with counter64
CSCsd13491	Infrastructure	show memory statistics history displays wrong values in processor pool
CSCsd46517	Infrastructure	Huge Memory allocation on c1721 during snmpwalk .
CSCse98807	Infrastructure	Traceback, Process=SNMP Timers, %SCHED-3-STUCKMTMR during regression .
CSCsi22502	Infrastructure	installer imf.tar file not being zipped creates uninstallable image
CSCsi99930	Infrastructure	%Error opening slavedisk0:/<filename> (Cluster chain broken on file)
CSCek66164	IPServices	show command pipeline redirect into rcp crashes the router
CSCsd43344	IPServices	isis-nsf info doesnt sync with standby in SSO mode .
CSCsd87810	IPServices	IOS tftp server should not differentiate between / and backslash in path
CSCsh31939	IPServices	c2w1:ciscoFtpClientMIB:Get & Set opration cause process deadlock & crash
CSCsi29875	IPServices	3/27: SP: oir_rf_reload_self: icc_req_imm failed, node not booting
CSCsi45840	IPServices	ARP requests for HSRP virtual IP may fail after switchport cmd is used .
CSCsi77774	IPServices	On modular IOS,Telnet on VRF int is allowed irrespective of vrf-also key
CSCsi78162	LegacyProtocols	SNASw %DATACORRUPTION-1-DATAINCONSISTENCY messages
CSCsg05873	Management	Buffer leak with SNA Focalpoint PU consuming middle buffers with NMVTs
CSCse22161	QoS	RP pool Memory corruption SXF4 - checkheaps_process/validblock crash
CSCsi05251	QoS	bus error crash at get_rateinterval_from_service_policy at subint delete
CSCef34800	Routing	BGP changes to accept max value for MED attribute
CSCeg43753	Routing	Router crashes at bgp_vpnv4_revise_route_update - corrupt PC & Sig10 .
CSCeg58039	Routing	BGP: changing the max-paths value may cause a crash .
CSCsb63652	Routing	bgp aggregate-address results in high BGP Router process utilization .
CSCsb96034	Routing	Traffic down for too long after SSO switchover .
CSCsd41237	Routing	vrf import map is not working .
CSCsd52225	Routing	BGP soft-reconfiguration keeps the old next-hop
CSCsd72747	Routing	nssa summary to null0 disappears after 'clear ip ro *'
CSCse91962	Routing	prefix stays in BGP table with RD 0:0 even after vrf's RD is configured
CSCsf32449	Routing	Sup720 MVPN PE - Tunnel does not come back up after reload .
CSCsg14026	Routing	Routers/Switches forward traffic destined to Class E Addresses
CSCsg52336	Routing	Crash at ospf_flush_area_summary_lsa after 'no ip vrf' of unassigned vrf
CSCsh61119	Routing	High CPU due to ARP refresh triggered by Serial interface flap
CSCsh80008	Routing	BGP: soft reconfiguration inbound and neighbor weight has no effect
CSCsi45422	Routing	iprouting.iosproc process reloads when making changes to static routes

Identifier	Technology	Description
CSCsi62559	Routing	SPD classifies OSPF IP Precedence 0 as priority .
CSCsj23579	Routing	Invalid memory action (malloc) @ SSO Switchover .
CSCei07548	Security	ocsp response timestamps are mishandled
CSCei85164	Security	OCSP fails when timezone is configured
CSCsh37957	Security	IPsec MIB entries not populated, IKE entries seem OK
CSCei52830	Unknown	Banner command sync is broken by CSCin86483 .
CSCej32124	Unknown	no mls verify commands doesnt take effect on standby supervisor
CSCek37222	Unknown	FR-flat:classification is broken in class-default with random-detect .
CSCek54572	Unknown	crash at ace_create_cm_head_node .
CSCek57760	Unknown	IP MTU of GRE tunnel not used by SPA-IPSEC
CSCek68265	Unknown	Major alarm on active caused syst. shutdn instead of swover to stdby
CSCek75394	Unknown	High CPU after enabling MPLS on interface .
CSCek77954	Unknown	test platform firm get cu-sfp-phy print-reg <port> <reg-no> .
CSCsa75285	Unknown	WS-X6582-2PA crashing cisco7600 when booting up with PA-MC-STM-1SMI
CSCsb13358	Unknown	failaction gtp purge doesnt delete some gtp stickies when probe fail
CSCsb14543	Unknown	t/b pm_port_counters_lock on module reset of active supervisor
CSCsb57042	Unknown	%SYS-SP-3-OVERRUN at test_hm_diag_scratch_regs
CSCsc11689	Unknown	Configure/Unconfigure PACL may cause memory leak.
CSCsc33080	Unknown	%PFINIT-SP-1-CONFIG_SYNC_FAIL_RETRY: Sync'ing the private configuration
CSCsc83961	Unknown	Both APS protect & working ports forwarding traffic
CSCsd33992	Unknown	%PM-SP-STDBY-3-INTERNALERROR: when boot up
CSCsd77207	Unknown	Bidir traffic changed from HW to SW switch after add 200 sub-inf quickly
CSCsd79536	Unknown	Standby RP crashes once at reload after installing set of patches .
CSCse54191	Unknown	CSM fails over when incorrect HSRP group fails
CSCse98369	Unknown	class-default bandwidth percent 100% - SPA ATM fails
CSCse98795	Unknown	bus error while printing access-list
CSCsf18752	Unknown	mls ip slb search wildcard rp breaks gtp slb if 2 sfarms are confgd
CSCsf23115	Unknown	SUP720 does not recognize FAN2 after one of fans failed. .
CSCsg06577	Unknown	'Desc ordr internal vlan allocation' brings up sup with major diag error
CSCsg07870	Unknown	crash seen on switchover at pf_redun_sync_port_asic_on_swover .
CSCsg16272	Unknown	Catalyst6500 LinkDown snmp trap does not generate while performing OIR .
CSCsg30355	Unknown	OIR of redundant sup w/ CatOS crash the Cat6500 System running IOS
CSCsg38231	Unknown	'crypto eng gre vpnblade' cmd does make the tunnels to be accelerated by
CSCsg55237	Unknown	L2 flooding stops when new MAC address entries are learnt
CSCsg92670	Unknown	7600 : MLS FIB frozen, Sanity Check of MLS FIB s/w structures failed
CSCsh20211	Unknown	'Complete' diags fail TestNetflowInlineRewrite test on Service Modules
CSCsh33128	Unknown	MMLS/MVPN: Partial SC internal vlan not included in (*,G)

Identifier	Technology	Description
CSCsh34872	Unknown	With mls mpls recirc configd primary internal vlan has vpn-num .
CSCsh36377	Unknown	crypto connect cmd not updated in standby RP for ATM subif .
CSCsh38728	Unknown	Show int displays half even if port is hard coded to full
CSCsh39318	Unknown	10K / PRE-2 crashes at %MROUTE-4-ROUTELIMIT
CSCsh49239	Unknown	After redundancy failover Mcast packets drop for 60-90sec on SUP uplink
CSCsh54951	Unknown	PBR: TCAM incorectly programmed when match statement is NOT used
CSCsh61061	Unknown	VPM-SM:ISAKMP Lifetimes do not replicate correctly in interchassis setup
CSCsh62565	Unknown	SSH keys regenerated every hour cause route flaps due to high CPU load
CSCsh68976	Unknown	memory leak at xcvr_idprom when executing show hw-module all tranceiver
CSCsh77220	Unknown	SSO failover causes certain configs being removed .
CSCsh94882	Unknown	Unity client not initiating mode config should be rejected
CSCsh98909	Unknown	VRRP traffic not hardware switched on Sup2/MSFC2
CSCsh99351	Unknown	Packet reflection on EoMPLS links
CSCsi00173	Unknown	Bus error at crypto_ipsec_unlock_peer .
CSCsi02885	Unknown	OSM-1CHOC12/T1-SI incrementing abort, interface administrativel
CSCsi12289	Unknown	FWSM Does Not Display Correct Timezone for DST
CSCsi15191	Unknown	BOM messages observed while activation of rollback on stndby supervisor
CSCsi16904	Unknown	VPN-SPA does not send ISAKMP packet with notification payload included
CSCsi40628	Unknown	Dual RSPAN session causes loop between 2 6500 chassis .
CSCsi41791	Unknown	Leak: SPA-IPSEC-2G crash-> No More Free Buffers ; SPA_IPSEC-3-PWRCYCLE .
CSCsi42270	Unknown	IOS-SLB Radius Server LB may not mark a real as failed
CSCsi42517	Unknown	SRB Crashes when upgrading from SXF to SRB with SLB stateful config
CSCsi52209	Unknown	7600-sip-600 crash at PXF-DFC1-2-FAULT: T0 OHB Exception: SLIP FIFO full
CSCsi60125	Unknown	Hosts receive TCP RST due to incorrect NAT translation on cat6k .
CSCsi64204	Unknown	SXF:SIP400:ATMSPA Noticeable delay in output of show int atm command
CSCsi69350	Unknown	Newly active crashed on upgrading rp rommon @ emt_call .
CSCsi76192	Unknown	r3:show wism status not populated until standby up after SSO
CSCsi90011	Unknown	User Auth after Machine Auth causes dot1x security violation
CSCsi91875	Unknown	Cat6k crashes when unconfiguring vserver during snmp poll
CSCsi97192	Unknown	Vrf Agg label is not programmed in vpn-cam, SP thinks it as Ipv6 Agg lab
CSCsi98993	Unknown	Block FPD for Intel SPROM based ATM SPAs
CSCsj01891	Unknown	%SYS-SP-3-OVERRUN at test_hm_diag_scratch_regs
CSCsj04905	Unknown	IOS-SLB: FWLB sticky config not get removed
CSCsj16292	Unknown	DATACORRUPTION-1-DATAINCONSISTENCY: copy error
CSCsj23211	Unknown	'Complete' diags fail TestNetflowInlineRewrite test on Service Modules
CSCsj27811	Unknown	EOBC buffer leak caused by CMM module .
CSCsj28277	Unknown	Sup720 ignores IGMPv3 report if first group in Exclude list is 224.0.0.x

Identifier	Technology	Description
CSCsj30444	Unknown	SUP-2 Router crashes after boot UP
CSCsj40706	Unknown	incorrect ifIndex from multi HC OID Get to various cards
CSCsj47546	Unknown	POS: RDI-P must not be sent when the interface detects PLM-P
CSCsj60722	Unknown	TestNetflowInlineRewrite: diag failure on bootup
CSCsi33554	WAN	Connected net for virtual-template is not created in vrf routing table

Resolved Caveats in Release 12.2(18)SXF9

Resolved Caveats for Product 'all' and Component 'pim'

- CSCsd95616—Resolved in Release 12.2(18)SXF9

  Two crafted Protocol Independent Multicast (PIM) packet vulnerabilities exist in Cisco IOS software that may lead to a denial of service (DoS) condition. Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

  This advisory is posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20080924-multicast.html.

Resolved Caveats for Product 'all' and Component 'socket'

- CSCse56501—Resolved in 12.2(18)SXF9

  A device running Cisco IOS software that has Internet Protocol version 6 (IPv6) enabled may be subject to a denial of service (DoS) attack. For the device to be affected by this vulnerability the device also has to have certain Internet Protocol version 4 (IPv4) User Datagram Protocol (UDP) services enabled. To exploit this vulnerability an offending IPv6 packet must be targeted to the device. Packets that are routed throughout the router can not trigger this vulnerability. Successful exploitation will prevent the interface from receiving any additional traffic. The only exception is Resource Reservation Protocol (RSVP) service, which if exploited, will cause the device to crash. Only the interface on which the vulnerability was exploited will be affected.

  Cisco is providing fixed software to address this issue. There are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080326-IPv4IPv6

Resolved Caveats for Product 'all' and Component 'ssh'

- CSCsc19259—Resolved in 12.2(18)SXF9

  The server side of the Secure Copy (SCP) implementation in Cisco Internetwork Operating System (IOS) contains a vulnerability that allows any valid user, regardless of privilege level, to transfer files to and from an IOS device that is configured to be a Secure Copy server. This vulnerability

could allow valid users to retrieve or write to any file on the device's filesystem, including the device's saved configuration. This configuration file may include passwords or other sensitive information.

The IOS Secure Copy Server is an optional service that is disabled by default. Devices that are not specifically configured to enable the IOS Secure Copy Server service are not affected by this vulnerability.

This vulnerability does not apply to the IOS Secure Copy Client feature.

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

- CSCse24889—Resolved in 12.2(18)SXF9

  Symptoms: Malformed SSH version 2 packets may cause a memory leak, causing the platform to operate under a degraded condition. Under rare circumstances, the platform may reload to recover itself.

  Conditions: This symptom is observed on a Cisco platform that is configured for SSH version 2 after it has received malformed SSHv2 packets.

  Workaround: As an interim solution until the affected platform can be upgraded to a Cisco IOS software image that contains the fix for caveat CSCse24889, configure SSH version 1 from the global configuration mode, as in the following example:

  ```
  config t
  ip ssh version 1
  end
  ```

  Alternate Workaround: Permit only known trusted hosts and/or networks to connect to the router by creating a vty access list, as in the following example:

  ```
  !10.1.1.0/24 is a trusted network that
  !is permitted access to the router, all
  !other access is denied

  access-list 99 permit 10.1.1.0 0.0.0.255
  access-list 99 deny any

  line vty 0 4
  access-class 99 in
  end
  ```

  Further Problem Description:

  For information about configuring vty access lists, see the Controlling Access to a Virtual Terminal Line document:

  http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_cntrl_acc_vtl.html

  For information about SSH, see the Configuring Secure Shell on Routers and Switches Running Cisco IOS document:

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

Resolved Caveats for Product 'c2800' and Component 'voice-xgcp'

- CSCsd81407—Resolved in 12.2(18)SXF9

  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.

Resolved Caveats for Product 'c3600' and Component 'voice-sip'

- CSCeb21064—Resolved in 12.2(18)SXF9

  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)SXF9

Identifier	Product	Component	Description
CSCsh82746	all	7x00-t1e1	Input Errors Counter not incrementing properly with Runt Errors
CSCsb45696	all	802.1x	Crafted EAP Response Identity packet may cause device to reload
CSCef27578	all	aaa	The router crashes when test aaa stop CLI is issued
CSCsh74025	all	atmcommon	clns packets not being punted by an enhanced flexwan .

Identifier	Product	Component	Description
CSCsd32373	all	bgp	BGP does not flag multipath correctly, causing loadbalancing issues .
CSCse04220	all	bgp	Clearing IPv6 BGP sessions can cause crash .
CSCsi06948	all	bgp	Bus error when issuing BGP dampening related commands .
CSCsi58259	all	c7600-atom	EARL7 PFC EoMPLS: CE to CE connectivity is broken with ATM as core
CSCsb19159	all	cat6000-filesys	Command copy const_nvram:vlan.dat startup-config might crash switch .
CSCsh94940	all	cat6000-hw-fwding	Supervisor crash by memory corruption (BADFREEMAGIC) in free block .
CSCsg52887	all	clns	SegV at ctunnel_oqueue when 'no ctunnel destination' on one side
CSCsd25653	all	comm-serv	vrf-also in named ACL for VTY line not saved in running configuration
CSCsi34572	all	dot1x-ios	PC does not get a new DHCP address for machine authentication dot1x
CSCeh78345	all	eventmgr	Ensure EEM policies close tty session properly upon exit.
CSCea53765	all	fib	Facility to periodically validate adjacency prefix against RIB
CSCsh76592	all	fib	Crash in mtrie_longest_match when VRF is removed from config
CSCsa72748	all	fr	router crash due to watchdog timeout on frame relay broadcast
CSCek55001	all	ifs	Dir /recursively with many directories crashes the router
CSCsf04921	all	ifs	18SXF6: getnext loop condition detected on ciscoFlashFileTable .
CSCsg40016	all	ifs	show tech causes various system problems
CSCsi42143	all	ifs	Image installation fails with error msg 'Failed to create output file' .
CSCsh74322	all	install	rp fails bootup when reload installed image with 42 patch in 1 tar ball
CSCsh35311	all	ios-authproxy	Proxyacl downloaded from the ACS cause spurious memory access
CSCek39048	all	ip	Modular IOS: default distribute-list route-map crash router .
CSCse44079	all	ipmulticast	Multicast UDL - High CPU in IGMP Input when UDL interface down .
CSCsd50828	all	ip-pbr	AS-path based redistribution fails
CSCsg42246	all	ip-rip	CPUHOG in IP Background, and router reload .
CSCsh57795	all	ip-rip	Removing 1 RIP neighbor removes all neighbors
CSCsh85355	all	ipsec-core	Address Error exception at crypto_ipsec_clear_peer_sas
CSCsg99872	all	ipsec-isakmp	VPNSM: IPSEC accounting (start/stop) not sent under some conditions
CSCsg47462	all	ip-tunnels	Address error crash at tunnel_ep_addr_compare
CSCsb07279	all	isis	Adding new on route-map which is redistributed by ISIS, is not seen
CSCsi41944	all	isis	Virtual Exec CPUHOG
CSCsd32192	all	mcast-switching	GRE Tunnel With Checksum Enabled Does Not Transmit Multicast Packets
CSCsd40153	all	mpls-ldp	Rainier: label is not advertise to downstream ldp neighbor after reload
CSCsf98345	all	mpls-ldp	vrf-interface down cause LDP peer reset
CSCsh83034	all	mpls-lfib	High CPU on Supervisor caused by FIB Control Task process
CSCsh82993	all	mpls-vpn	Aggregate label missing if static route exists for same network
CSCsc93633	all	nbar	Software bus error crash on 7206VXR w/12.3(14)T3 w/ NBAR configured
CSCsd59610	all	os	%SYS-4-REGEXP: new engine: regexp compilation had failed.

Identifier	Product	Component	Description
CSCsg42072	all	os	Virtual Exec sessions not freeing memory
CSCsi62514	all	os	SXF9: ION image not bootable ROCKIES3_INTEG_070423
CSCek70058	all	osm-qos	OSMs may crash due to memory corruption on applying certain qos config.
CSCse60482	all	osm-qos	OSM QoS per VLAN shaping not configurable for EoMPLS with TE Tunn
CSCsc52057	all	ospf	OSPF passive-interface default bleeds to OSPF VRF subinterfaces
CSCse64565	all	ospf	OSPF passive-interface default pb when converting switchport to L3
CSCsg92954	all	pas-chstm1	Poor Voice Quality over congested Links
CSCef89952	all	pim	Router crashes when state-refresh message is rcvd for non-dense grp .
CSCsd16043	all	pim	Auto-RP for multicast may prematurely expire the group to RP mappings .
CSCeg38418	all	pki	Router crash when OCSP server use key hash as id
CSCsd09892	all	qos	no fair-queue causing VIP crash .
CSCse94388	all	qos	SIP200 crash at dlfi_do_fragment on HQF with priority .
CSCsi01422	all	qos	Hierarchical Frame-Relay QoS does not work .
CSCse51263	all	rcp	RP side console Exec process hangs deadly sometimes
CSCsf08419	all	remote-registry	EIGRP memory leak in registry_ion.c when neighbor flaps.
CSCsh83559	all	remote-registry	Modular IOS: memory leak in xdr_reference
CSCse80032	all	snmp	Mediation Device cannot resync SNMP engine time after 7600 reload .
CSCse95758	all	snmp	Access Lists support for all CONFIG-COPY-MIB protocols under snmp-server
CSCsh79371	all	snmp	SNMP memory leak for Modular IOS on 12.2(18)SXF6 .
CSCsi08777	all	spa-ipsec-2g	Memory Leak seen in Chunk Manager process .
CSCsi42769	all	spa-ipsec-2g	VPNSPA crashes with large certificates (PKI) .
CSCsf32211	all	spa-pos-oc3-12	Input bytes counter continues incrementing when a line protocol is down
CSCsb74409	all	ssh	IOS ssh client blocks Virtual Exec / SSH Process
CSCse79611	all	ssh	SSH source-interface command not working
CSCse53090	all	tcl-bleeding	After console timeout, access can be done to standby console.
CSCed95187	all	tcp	IP ID field is predictable for connectionless RST packets .
CSCef13860	all	tcp	Invalid TCB pointer traceback on exiting from a CPU session
CSCsg00846	all	tcp	Crash of RP blob due to a missed inetd_service_mutex unlock
CSCsg19598	all	tcp	SSH session hangs intermittently
CSCsg56926	all	tcp	no logging console not working in ION for tcp debugs
CSCsi51178	all	tcp	Switch crashes due to ssh session at pak_client_set_pid .
CSCsb86257	all	telnet	Named ACL configured on VTY in with VRF
CSCsd42600	all	telnet	%SYS-3-BAD_RESET alongwith SegV exception crash
CSCsh56081	all	trans-bridging	Spanning tree of vlan-bridge is operated incorrectly
CSCsg99600	all	udp	Modular IOS : ip helper address 1.1.1.255 not work
CSCsh21505	all	udp	ip helper address on vrf interface in ION, dhcp routed with global table
CSCsh75069	all	udp	Input Queue Wedge with UDP Echo packets .

Identifier	Product	Component	Description
CSCsi23203	all	vipmlp	Remove service policy from T1 prior to adding it to the multilink bundle
CSCuk61773	all	wccp	WCCP: ignore redirect assignment messages with identical content
CSCsd76528	c10000	qos	Queues not released after deletion of mtch vlan for HQoS policies .
CSCsa46154	c12000	ip-pbr	12.0(27)S03.1118 Deleting 100 Route-Maps at a time forces failover to RP
CSCsd84497	c2800	ios-authproxy	auth-proxy requests stuck in init state
CSCeg51185	c6venus-slb	laminar	New varbinds reqd in slbRealStateChange & slbVirtualStateChange trap
CSCek31610	c6venus-slb	laminar	IOS changes to support sticky replication in CSM
CSCsb84087	c6venus-slb	laminar	CSM: config-sync cmd not able to remove vlan from standby csm port-chann
CSCsd24461	c6venus-slb	laminar	Configuring CSM with SSL stickyness shows as src-ip stickyness.
CSCsh74881	c6venus-slb	laminar	CSM with a pair of bridged vlans can cause a variable to not function
CSCsg79810	c7600	c7600-sip-400	The MPLS MTU is overruled by the ip mtu on ATM interface
CSCsi10231	c7600	c7600-sip-600-vpls	VPLS: VC types 4 and 5 can not co-exist within same VFI on 7600-SIP-600
CSCsi22379	c7600	c7600-sip-600-vpls	SIP600 vpls drops packets from VC Type 4 neigh when control word present
CSCek25660	c7600	cat6000-hw-fwding	tarceback found at l2_modify_one_entry(0x207b9614)+0x48 .
CSCse61387	c7600	cat6000-qos	After LC is removed, show policy-map control-plane still show LC counter
CSCse89548	c7600	cat6000-routing	SYS-DFC4-3-CPUHOG::FIB Control Queue Task
CSCsh23192	c7600	loadbal	DNS probe does not recover after failure when configured with VRF
CSCsi77083	c7600	osm-ucode	Fix for CSCsh21998 in v122_18_sxf_throttle is erroneous
CSCsh46565	c7600	qos	PWAN2 HQoS(LLQ): shape ave rate is not applied .
CSCsi48550	c7600	vipmlp	dMLP: account lost_frags& rx discards as bundle intf input error
CSCsd08468	cat6000	c7600-mpls	SP crash at %EARL_L2_ASIC-SP-4-L2L3_SEQ_ERR due to invalid packets
CSCsg91545	cat6000	cat6000-acl	ACL TCAM inconsistency seen if ipv6 acl with 2k mask is used .
CSCsh76923	cat6000	cat6000-acl	Memory Corruption or bus error crash on cat6k running NAT .
CSCsf29400	cat6000	cat6000-cmm-voice	Native IOS Sup discards or filters ARP replies from CMM for ACT module
CSCsh49043	cat6000	cat6000-firmware	Output drops in Queue3 after changes in cos-map config on 6148A-GETX .
CSCsh89589	cat6000	cat6000-firmware	ARP fails on FWSM with SFM or SFM2 and S2/MSFC2
CSCsc77287	cat6000	cat6000-ha	SIERRA: Telnet/console: freeze by remote command module slot
CSCsh45258	cat6000	cat6000-ha	delay execution of redundancy force switchover in case stdby nrd .
CSCek68281	cat6000	cat6000-hw-fwding	Syslog instead of crashing on correctable FIB SSRAM ECC errors
CSCsd95877	cat6000	cat6000-hw-fwding	%MLS_ACL_COMMON-SP-4-MLS_ACL_CONSIST appears on active SP on sso.
CSCse90572	cat6000	cat6000-hw-fwding	FIB TCAM exception related enhancements
CSCsb85030	cat6000	cat6000-l2	lost connectivity after port security disabled/removed - packets drop
CSCsf20751	cat6000	cat6000-l2	FlowControl inconsistency between Po and gig interfaces after SW upgrade

Identifier	Product	Component	Description
CSCsh38443	cat6000	cat6000-l2	Removing associated vlan would trigger the mac-add to get purge every 5m
CSCsh98208	cat6000	cat6000-mcast	PIM Snooping strips out Prune List in a (*,g) Join (s,g) RPT prune msg .
CSCsi57912	cat6000	cat6000-mpls	6PE: router mac not programmed for the IPV6 MPLS reserved vlan after SSO
CSCse10113	cat6000	cat6000-netflow	Missing hwidb for fibhwidb netflow_vlan1038 (ifindex 216) : .
CSCsg47044	cat6000	cat6000-netflow	NDE is not exporting packets
CSCsf11787	cat6000	cat6000-oir	EARL bus idle error occurs when the switching bus stall occurs
CSCsg72678	cat6000	cat6000-oir	TCAM entries not displayed for DFC card after OIR .
CSCsh93083	cat6000	cat6000-routing	Hadware uRFP with ACL stops after reboot
CSCsg49395	cat6000	cat6k-vs-infra	%BIT-SP-4-OUTOFRANGE: bit is not in the expected range
CSCsb44267	cat6000	cwpa	bus error crash when forwarding IPX over GRE
CSCsg09757	cat6000	ios-infra	MP(Maintenance Pack) information missing in the MIB .
CSCsh96773	cat6000	laminar	CSM FT : unable to track port-channel interfaces
CSCsi73534	cat6000	laminar	CSM: CSCsb84087 breaks config-Sync feature
CSCse34615	cat6000	loadbal	Radius Acct on-off messages are dropped by Vserver
CSCse56921	cat6000	loadbal	GTP SLB Reloads at the time of session/sticky creation in multiple vserv
CSCsb01373	cat6000	msfc-filesys	MSFC3: Free NVRAM space reduces every time config is written to memory
CSCsg45480	cat6000	osm-ucode	Prevent Invalid IP Packets from OSM causing L2/L3 errors and SP crash
CSCsh21998	cat6000	osm-ucode	MPLS: Sup2 OSM sending TTL=0 packets with aggregate summary-only
CSCsf25728	cat6000	sr-bridging	Unable to session to FWSM when source-bridge ring-group is configured
CSCsg38618	wism	wlc-infra	Session to a 24 bit address fails on WiSM

Resolved Caveats in Release 12.2(18)SXF8

Resolved Caveats for Product 'all' and Component 'dlsw'

- CSCsf28840—Resolved in 12.2(18)SXF8

  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 Caveats for Product 'all' and Component 'ftp'

- CSCsg16908—Resolved in 12.2(18)SXF8

  Multiple vulnerabilities exist in the Cisco IOS File Transfer Protocol (FTP) Server feature. These vulnerabilities include Denial of Service, improper verification of user credentials and the ability to read or write any file in the device's filesystem, including the device's saved configuration, which may include passwords or other sensitive information.

  The IOS FTP Server is an optional service that is disabled by default. Devices that are not specifically configured to enable the IOS FTP Server service are unaffected by these vulnerabilities.

  This vulnerability does not apply to the IOS FTP Client feature.

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070509-iosftp.

Resolved Caveats for Product 'all' and Component 'pki'

- CSCsd85587—Resolved in 12.2(18)SXF8

  A vulnerability has been discovered in a third party cryptographic library which is used by a number of Cisco products. This vulnerability may be triggered when a malformed Abstract Syntax Notation One (ASN.1) object is parsed. Due to the nature of the vulnerability it may be possible, in some cases, to trigger this vulnerability without a valid certificate or valid application-layer credentials (such as a valid username or password).

  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.

  The vulnerable cryptographic library is used in the following Cisco products:

  - Cisco IOS, documented as Cisco bug ID CSCsd85587
  - Cisco IOS XR, documented as Cisco bug ID CSCsg41084
  - Cisco PIX and ASA Security Appliances, documented as Cisco bug ID CSCse91999
  - Cisco Unified CallManager, documented as Cisco bug ID CSCsg44348
  - Cisco Firewall Service Module (FWSM) CSCsi97695

  This vulnerability is also being tracked by CERT/CC as VU#754281.

  Cisco has made free software available to address this vulnerability for affected customers. There are no workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20070522-crypto.html .

  Note: Another related advisory is posted together with this Advisory. It also describes vulnerabilities related to cryptography that affect Cisco IOS. A combined software table for Cisco IOS only is available at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-crypto and can be used to choose a software release which fixes all security vulnerabilities published as of May 22, 2007. The related advisory is published at http://www.cisco.com/en/US/products/csa/cisco-sa-20070522-SSL.html

Resolved Caveats for Product 'all' and Component 'ssl'

- CSCsb12598—Resolved in 12.2(18)SXF8

  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/en/US/products/csa/cisco-sa-20070522-SSL.html

  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.

Resolved Caveats for Product 'cat6000' and Component 'osm-ucode'

- CSCsg40425—Resolved in 12.2(18)SXF8

  Symptoms: An Optical Services Module (OSM) may reset unexpectedly and generate the following error messages:

  %POSLC-3-SOP: TxSOP-0 SOP. (source=0x18, halt_minor0=0x4000)
  %CWANLC-3-FATAL: Fatal Management interrupt, gen_mgmt_intr_status 0x0, line_mgmt_intr_status 0x1, reloading

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series and Cisco 7600 series.

  Workaround: There is no workaround.

Other Caveats Resolved in 12.2(18)SXF8

Identifier	Technology	Description
CSCsd49317	AAA	no tacacs-server administration causes router hang .
CSCsg43322	AAA	AAA: No free authorization/accounting lists for network
CSCsa91863	Access	PA-E3 may reports LOF on reload
CSCse06752	Access	LAM /32 cef entry shows unresolved
CSCdy11156	ATM	13E:12E:RP crashed while applying config on ATM-PA,mgd_timer_stop .

Identifier	Technology	Description
CSCea82222	Infrastructure	timeout login response is broken on TTY and VTY lines with no AAA
CSCek42751	Infrastructure	%Error opening system:/running-config (No such file or directory)
CSCek58966	Infrastructure	Remove IPSLA Feature CLI From Modular IOS
CSCek64188	Infrastructure	Fragmentation fix of CSCek64051 is incomplete
CSCek65370	Infrastructure	Disable IP SLA CLI/SNMP from modular ios image in SXF
CSCsc04397	Infrastructure	Spurious memory access made at Fcheck_interface_state
CSCsc09336	Infrastructure	fix memory leak in display_posix_memory_info ion_lib_show_memory.c .
CSCse56676	Infrastructure	Some SNMP notifications go to the wrong host
CSCsg22769	Infrastructure	CPU utilization goes beyond 99% due to dfs_disk1.proc. .
CSCsh23981	Infrastructure	IPC ISSU: First message to seat 0x2070000 not found .
CSCee30364	IPServices	ip ftp username not used after username was previously used in URI .
CSCek12203	IPServices	File system issues after unsuccessful FTP operation. .
CSCsb27868	IPServices	DHCP Relay should unicast offer/ack on unnum ethernet sub- int
CSCsc12899	IPServices	SSM Mapping configuration inside a VRF broken
CSCse05736	IPServices	A router running RCP can be reloaded with a specific packet .
CSCsg49987	IPServices	HSRP learned groups appear in SNMP MIB
CSCsh29830	IPServices	NAT: Clear IP NAT translation * creates hardware entry for RSHELL.
CSCsc68540	MPLS	mplsTeNotifyPrefix trap emitted instead of correct TE trap name
CSCsg44555	MPLS	7600 MPLS TE mid-point stuck at up/down and Juniper headend up/up
CSCsg86806	MPLS	Client over MPLS unable to ping interfaces
CSCsh58729	MPLS	crash while configuring multiple back up path tunnels
CSCsc25557	platform-76xx	PORT3: Router crashed in CWAN OIR Handler in attempt to lock a semaphore
CSCsg21429	platform-76xx	STM-16 interface in OSM line card flaps endlessly upon SUP switchover .
CSCsg40425	platform-76xx	OSM-1OC48-POS-SI+ keeping reset due to POSLC-3-SOP .
CSCsg87037	platform-76xx	ATM OSM has compatibility issue with 3rd vendor device
CSCsh41006	platform-76xx	change earl reset patch-limit crash disable test cmd to a config cmd
CSCse91675	PPP	SWMLP: all intf are going down w/46 byte pkt size 8links/bundles@LR trfc
CSCeh82893	QoS	PP:R3:SIP400:QOS: LLQ+police drop rate counters are broken
CSCek34117	QoS	SIP1+ATM(OC3 SPA): Crashed at hqf_walk_and_police_inline() .
CSCsd56696	QoS	A2A: FR Adaptive shaping is not accurate .
CSCef15420	Routing	router reload at ed_get_reuseintervals Part II
CSCef84062	Routing	Bus error in bpath_unlock due to null path .
CSCeg03019	Routing	cef not working between different tunnels .
CSCek48274	Routing	clear ip bgp soft in may not delete all the BGP prefix
CSCsa49922	Routing	EIGRP internal route remains in RT but not in topology table
CSCsb34032	Routing	ISIS: router exception at mgd_timer when un-config isis cmds
CSCsc46337	Routing	BGP peer doesnt have an Index, session will not establish .

Identifier	Technology	Description
CSCsc83821	Routing	ISIS: TLV 237 not found in database when isis metric is configured
CSCsd59023	Routing	RP Arping for adjacent next-hop bringing up PTA sessions with AAA .
CSCse24873	Routing	Default-information originate in BGP shouldnt be tied to peer group
CSCse34050	Routing	ISIS keep advertizing passive interface, even after doing shutdown
CSCsf20947	Routing	BGP 'neighbor default-originate' advertisement ignored after link flap.
CSCsf26043	Routing	Cat6k Selective Packet Discard not classify ISIS at high-priority
CSCsg11830	Routing	12.2(18)SX Default-information originate does not generate default route
CSCsg26492	Routing	Error: can not find acl. Abort - msg when removing permit entry in ACL .
CSCsg43140	Routing	Switch may crash due to bgp over vpn .
CSCsg46638	Routing	BGP does not send withdraw when distribute-list is configured
CSCsg55209	Routing	BGP paths increase, with same prefix and next-hop under soft-reconfig .
CSCsg65298	Routing	OSPF: connected network learnt via ospf after interface shutdown #2
CSCsb54378	Security	watchdog timeout crash when starting ssh session from the router .
CSCsd76601	Security	Resuming SSH Session Fails After Other Session Has Been Disconnected .
CSCsd92405	Security	router crashed by repeated SSL connection with malformed finished messag
CSCse40423	Security	With ATM, tunnel interfaces do not ping until a shut-noshut is done .
CSCec76468	Unknown	crash in show route-map when delete route-map during concurrent conf
CSCef56327	Unknown	PA-MC-STM1: Cannot set/keep clock source line in config
CSCeg02918	Unknown	Bus Error at auth_proxy_proc_profile
CSCeh54725	Unknown	MIB object go into loop during snmp query
CSCei09247	Unknown	Local serial link goes up/down when remote link is admin down
CSCei12353	Unknown	Flow End sysUpTime higher value than the Router sysUpTime
CSCek55639	Unknown	Failed to assert Physical Port Administrative State Down alarm
CSCek65022	Unknown	7600-SSC-400: SPA-IPSEC-2g EFC clock hardware issue .
CSCek66277	Unknown	Diagnostics test 18 TestAclDeny should be marked Disruptive .
CSCsa97042	Unknown	Secured port dropping traffic after applying & removing mac-filter
CSCsb64767	Unknown	Unconf/confg port of L2 Eth chnl stop Mcast Traffic fwding out the port
CSCsc08947	Unknown	6k IOS Autostate: L3 int up/up if last L2 port disabled while L3 is shut
CSCsc69076	Unknown	SIP1-ChOC3: Spurious access at swsb_delete on unconfig of T1 chnl group
CSCsc73699	Unknown	Bus error at ipflow_get_template_id with NetFlow v9 .
CSCsd19181	Unknown	Crypto connect command is dropped from serial interface after reload .
CSCsd74091	Unknown	Misc. fixes for GCE handling for standby as DFC
CSCsd98852	Unknown	EEM does not allow read from stdin
CSCse37364	Unknown	traceback @ hal_get_dist_job on toggling mmls
CSCse39956	Unknown	VPLS:UCODE:Replication broken when CW followed by NO_CW VC
CSCse49388	Unknown	Tunnel int fails to receive traffic when links of a diff tunnel shut .
CSCse65726	Unknown	command no tacacs-server admin resets router

Identifier	Technology	Description
CSCse66269	Unknown	ION free memory dropping during mcast failovers but no process leaking
CSCse84602	Unknown	Error messages from Standby Sup when configuring OSM card channelization
CSCse84695	Unknown	Standby supervisor may crash when configuring osm card past FREEDM limit
CSCse88708	Unknown	Early stop of Bert test on OSM-1CHOC12/T1-SI produces error
CSCse97422	Unknown	crash on sup720, when executing 'sh tech' with long regexpr .
CSCsf10605	Unknown	crypto session count incorrect after ungraceful disconnect
CSCsf31458	Unknown	R3Vail: SupW image - entPhysicalTable is not SSO aware. .
CSCsg01366	Unknown	CSM config sync cause stacks to run low and crash router
CSCsg02241	Unknown	SUP720/SUP32 NAT translates incorrectly
CSCsg02391	Unknown	PORT_SECURITY-SP-2-INELIGIBLE error after module reset
CSCsg03739	Unknown	cat6k with vpnsm several possible crypto ikmp leaks .
CSCsg07525	Unknown	Periodic (30sec) traffic loss/dup over dis port-cha due to wrong RBH
CSCsg08200	Unknown	JQL: Bootup diagn for LC detect major failure after RPR swover .
CSCsg08304	Unknown	JQL: UDLD failure detected on neighbor switch after RPR switchover .
CSCsg16425	Unknown	show ip slb reals command displays huge connections value
CSCsg24609	Unknown	Whitney: snmp CISCO-L2-CONTROL-MIB getmany errors .
CSCsg34141	Unknown	Secure mac learnt on non secure port creates a static entry
CSCsg35506	Unknown	JQL: port-channel member in suspend due to flowcontrol mismatch .
CSCsg37435	Unknown	ifIndex missing for 802.1Q vLAN subif after GigEth card OIR .
CSCsg40391	Unknown	Dot1x: Port config on authenticated port changed after linecard reset
CSCsg51230	Unknown	VS2: MLS multicast operating state is IDLE, after SSO switch over
CSCsg51724	Unknown	cbQosCMDropPkt stays at 0 while CLI counters shows positive values
CSCsg61773	Unknown	MMLS: Egress mode, OIF inconsistent between SP/RP, traffic blackholed
CSCsg62119	Unknown	Cat6K Spurious Memory access
CSCsg64170	Unknown	SSO switchover causes service module to appear down for 10-30 secs .
CSCsg64306	Unknown	%MCAST-SP-6-L2_HASH_BUCKET_COLLISION
CSCsg69489	Unknown	Reroute of LSP between two link with label constitutes to traffic loss .
CSCsg72398	Unknown	SLB:Packets getting process switched w/ multiple UDP Vservers
CSCsg73179	Unknown	bi-dir mls rp doesnt get updated after a change in topology .
CSCsg76239	Unknown	Fast Path mcast pkts hit RP cpu if ACL configured on OIF .
CSCsg77142	Unknown	Memory leak in Cat6k SNMP Trap process
CSCsg80948	Unknown	Uneven load-sharing for 4-path ECMP case
CSCsg90190	Unknown	Software does not limit 96 Ports LC inline Power based on HW Limitation
CSCsg97079	Unknown	18SXF7 ION image should also bundle FlexWan1
CSCsh01749	Unknown	mls qos marking ignore port-trust has no effect with EoMPLS configurat .
CSCsh05800	Unknown	Mcast egress replication - VDB is not updated on L3 PO subinterfaces
CSCsh07037	Unknown	OSM may crash with CHUNKBADMAGIC error, when WRED threshold is conf > 2k

Identifier	Technology	Description
CSCsh17979	Unknown	Ports PWR_DENY not enough system PWR/chassis BackPlane PWR (Not Real)
CSCsh20950	Unknown	18SXF8: PRBS support needs to be disabled on the Malabar8 module
CSCsh22835	Unknown	Major Error is seen with module 6 after swithover in rpr mode. .
CSCsh25976	Unknown	C2W1: SSO sync issue with PSFANINCOMPAT & PSFANFAIL sensor .
CSCsh29863	Unknown	New active crashes after switchover in rpr mode .
CSCsh31306	Unknown	T1 serial o/p drops / no QOS drops - flexwan - T1 multichannel PA.
CSCsh32199	Unknown	Input queue drop counter incrementing even when interface disconnected
CSCsh37008	Unknown	Need to enable Malabar8 in WS-C6509-NEB-A chassis with one fan .
CSCsh41192	Unknown	Memory leak in IPSEC key engine process .
CSCsh42914	Unknown	Cat6500 Netflow does not export all flows with sampled netflow
CSCsh44288	Unknown	Hybrid: Remove uRPF check w/ACL knob from hybrid IOS images
CSCsh48947	Unknown	PWR_DENY Port 47/48 on each LC max PWR support Backplane per LC or VDB
CSCsh54325	Unknown	SIP600/ES20 PXF punt path broken when sup slot is 1 or 2
CSCsh61396	Unknown	R3.8: Hydra module resets during to excessive LCP_FW_ERR Qchip msgs
CSCsh66367	Unknown	Wrong Ubin Images committed to v122_18_sxf_throttle on CSCsh61396
CSCsh85155	Unknown	mls adjacency has extra punt entry after FRR cutover .
CSCsb46223	Voice	Bus error crash at Tcl_DStringAppend

Resolved Caveats in Release 12.2(18)SXF7

Resolved LegacyProtocols Caveats

- CSCsf28840—Resolved in 12.2(18)SXF7

  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)SXF7

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

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

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

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

Other Caveats Resolved in 12.2(18)SXF7

Identifier	Technology	Description
CSCsa93523	Access	7200 PA-E3 incrementing carrier transitions and packet drops
CSCea26450	ATM	PVC may stay down when interface cable is pulled out/put back rapidly
CSCsd20327	Content	WCCP going up/down
CSCeh85133	Infrastructure	Memory leak in Syslog Traps process
CSCsd29469	Infrastructure	Cat6000 SNMP stops responding while polling from ciscoEnhancedMemPoolMIB
CSCsd49133	Infrastructure	Alarms are not pouplated in ceAlarmTable - ceAlarmList is empty.
CSCsg32222	Infrastructure	Need the support for 64 bit bit/second OID on Cat6k/7600
CSCsg70355	Infrastructure	adopt new default summer-time rules from Energy Policy Act of 2005.
CSCei93982	IPServices	Modified ALG classification base on src & dst port
CSCsc78813	IPServices	DNS reply payload does not get translated in the NAT router.
CSCsd51530	IPServices	autocommand-options nohangup is removed on line vty 0-4
CSCse04560	IPServices	tftp-server allows for information disclosure .
CSCdz80245	LAN	SNMP: Need ifDescr output without description
CSCsg01823	LegacyProtocols	DECnet mac-address (aa00.0400.###) missing from interface after reload
CSCsb52900	MPLS	mpls forwarding table label inconsistency after switchover
CSCse92050	Multicast	With mis-configuration, router may reload at twheel_running
CSCse11678	PPP	SIP: Ping fails after removal of primary link from multilink bundle.
CSCsg02881	PPP	MLP: Bandwidth of down MLP group should be sum of member bandwidths
CSCsd37025	QoS	CPUHOG and crash when removing nbar policy-map
CSCse25833	QoS	%SYS-2-CHUNKBADMAGIC every 10 sec with 12.2(18)SXF4
CSCsf11353	QoS	Autobahn:FW2 kept crash at hqf_dp_set_blt_quantum and dlfi_inform_config
CSCei29944	Routing	RP crashes at bgp_get_msg_count while sho ip bgp summ
CSCei32930	Routing	EBGP+label : soft-reconfig inbound broken
CSCsb50606	Routing	Leak in dead process due to TCBs from BGP active connections
CSCsc43989	Routing	CEF adjacency inconsistent with NHRP cache entry
CSCsd03383	Routing	OSPF:TE Tunnel route not installed if parallel path eq max-path
CSCsd53402	Routing	ABR delets OSPF summary route for 5sec after DR is changed
CSCsd74396	Routing	eigrp authenticaion fails with md5 enabled
CSCsd81600	Routing	OSPF Stub-links should advertise LSInfinity when max-metric configured
CSCse41484	Routing	DMVPN / VPN-SPA / few GRE packets not encrypted when negotiating the SAs
CSCse51804	Routing	DMVPN tunnels not stable; keeps flapping
CSCse89119	Routing	OSPF discard route (Null0) is disappeared from RIB when AD is changed
CSCsf99057	Routing	JQL: OSPF Stub-router should work with SSO/RPR-Plus if NSF is disabled
CSCsg16748	Routing	ABR deletes OSPF type 3 LSA after it received max-aged type 2 LSA
CSCsb47257	Security	bus error crash @ pki_add_to_obj_list
CSCsf05479	Security	Address error at gre_ipip_fastsend

Identifier	Technology	Description
CSCsg10671	Security	No message when CA re-enrollment fails
CSCdy47789	Unknown	Non-directed LDP neighbors showing up under targetted discovery list
CSCeg41330	Unknown	crypto isakmp client config max-logins is case sensitive
CSCeh95801	Unknown	IPSec Accounting: DN not sent in group-id with EzVPN + CERT
CSCei58681	Unknown	port channel does not form after minlinks added and removed
CSCej78221	Unknown	CSG Refund policy with more than 10 entries causes cat6K to crash
CSCej83614	Unknown	Multicast packets punted with deny acl on outgoing interface
CSCej86174	Unknown	Need a command to disable EOBC JAM recovery
CSCek54981	Unknown	Incorrect ICMP MTU proposal for outgoing ESP packets
CSCsc55951	Unknown	SPA-4XOC3-ATM has compatibility issue with 3rd vendor device
CSCsc64718	Unknown	persistent-store command not available on SUP32 Images
CSCsc69851	Unknown	Port Security does not show offending MAC address in syslog
CSCsd69480	Unknown	%HYPERION-4-HYP_RESET on flexwan2 chSTM1 card
CSCse00115	Unknown	mcast egress replication -- Wrong output interface index for msc
CSCse37587	Unknown	DHCP snooping in conjunction with VRF breaks DHCP
CSCse43709	Unknown	supw nmi support
CSCse63054	Unknown	Remove VLAN IDB from VRF if_list when releasing a rserved VLAN
CSCse75904	Unknown	VPNSM: periodic accounting is still sent for disconnected vpn users
CSCse87210	Unknown	Enable service cards to operate in crossbar mode with Dist Etherchannels
CSCse87618	Unknown	cRTP and Interleave doesnt work together on Virtual-Template Interface.
CSCse98692	Unknown	12.2SX code not showing int trust state in sh mls qos cmd
CSCsf03986	Unknown	spurious at fm_wccp_format_adj_entry after upgrade
CSCsf07232	Unknown	tclsh stdio operations do not output to current terminal
CSCsf08368	Unknown	Prevent NBAR configuration on non-FlexWAN interfaces
CSCsf10116	Unknown	Reflexive ACL not getting Sw Installed.
CSCsf11639	Unknown	WS-X6148-FE-SFP interface counter increments even if the link is down
CSCsf14994	Unknown	SIP1-ChOC3:Some of the MLP links wont ping, if deleted & configred again
CSCsf23326	Unknown	IOS SLB does not on 7600 with SXF4 if Client is behind MPLS cloud
CSCsg00845	Unknown	'no logging event link-status' is lost after reload
CSCsg02605	Unknown	Rapid reboot does not work
CSCsg03503	Unknown	NAt Netflow entries need to be purged on routing change
CSCsg07765	Unknown	Sierra: scp_fpoe_req: memory allocation error, subopcode=10, count=9
CSCsg17923	Unknown	IKE Notifiies (DPD, Deletes,...) not processed -- dropped
CSCsg23979	Unknown	Crashes in iprouting.iosproc produce no tracebacks
CSCsg25416	Unknown	flash information is missing from show hardware output in ION
CSCsg26450	Unknown	move enum value at the end of the list
CSCsg28959	Unknown	rwindex = 0xFFFF on the non PI causing all mcast traffic to be dropped

Identifier	Technology	Description
CSCsg36726	Unknown	Bonham parity errors may cause packet loss on a 7600-SIP-400 module.
CSCsg38092	Unknown	Pre-Pilot:EEPROM (feature_bits) needs to upate to no floating capable
CSCsg38930	Unknown	7600 SPA-IPSEC-2G - Multicast data is not forwarded through GRE Tunnel
CSCsg40401	Unknown	SUP32 unstable to communicate with all neighbors after reload.
CSCsg41552	Unknown	Module fails to come online first time after reset
CSCsg58917	Unknown	mls ip cef load-sharing and mls ip cef rate-limit missing in Sup22
CSCsg62154	Unknown	18SXF7: ltl_alloc_index_at: T/Bs are seen after multiple switchover
CSCuk57037	Unknown	IGMP: crash at at ../ipmulticast/igmp.c:3162
CSCsc50986	WAN	NTP unsynchronizes when packets out of order at STEP
CSCsd19880	WAN	ATM pvc does not come up with new style legacy command
CSCse55004	WAN	NTP clients wont associate

Resolved Caveats in Release 12.2(18)SXF6

Resolved Caveats for Product 'all' and Component 'cat6000-mpls'

- CSCsf12082—Resolved in Release 12.2(18)SXF6

  Certain Cisco Catalyst 6500 Series and Cisco 7600 Router devices that run branches of Cisco IOS based on 12.2 can be vulnerable to a denial of service vulnerability that can prevent any traffic from entering an affected interface. For a device to be vulnerable, it must be configured for Open Shortest Path First (OSPF) Sham-Link and Multi Protocol Label Switching (MPLS) Virtual Private Networking (VPN). This vulnerability only affects Cisco Catalyst 6500 Series or Catalyst 7600 Series devices with the Supervisor Engine 32 (Sup32), Supervisor Engine 720 (Sup720) or Route Switch Processor 720 (RSP720) modules. The Supervisor 32, Supervisor 720, Supervisor 720-3B, Supervisor 720-3BXL, Route Switch Processor 720, Route Switch Processor 720-3C, and Route Switch Processor 720-3CXL are all potentially vulnerable.

  OSPF and MPLS VPNs are not enabled by default.

  This advisory is posted at
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080326-queue

Resolved Caveats for Product `all' and Component `snmp'

- CSCsf04754—Resolved in Release 12.2(18)SXF6

  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

Other Resolved Caveats in Release 12.2(18)SXF6

Identifier	Technology	Description
CSCsd71301	AAA	Depending on Attriubut order send from aaa server priv level assigned.
CSCsd95752	AAA	6500 TACACS message sent to wrong server .
CSCse45735	AAA	%AAAA-3-NOREG: authentication method 5 has no registry! T/B
CSCdw26914	ATM	show atm vc truncating outputs
CSCei39688	ATM	ATM subinterface fails to pass traffic due to CEF initialization failure
CSCse64269	ATM	show ip int br shows member link state down for PA-A3-8T1/8E1IMA
CSCse29465	Content	CASA traceback routing agent in process causing CPUHOG
CSCse45427	Content	debug ip casa packet displays incorrect values
CSCse76405	Content	CASA wildcard updates dropped
CSCdy11174	Infrastructure	ciscoFlashCopyTable/ciscoFlashMiscOpTable obj unreadable @ creation
CSCeb56615	Infrastructure	ATA_Status time out waiting for 1
CSCee23195	Infrastructure	Spurious memory access in show ipc queue .
CSCef49904	Infrastructure	No option in snmp to source the interface for Informs
CSCek51851	Infrastructure	Standby does not come up during switchover with slavenvram in access
CSCin97208	Infrastructure	Standby does not come up during switchover with slavenvram in access
CSCsc14034	Infrastructure	Master RSP crashes on bootup w/ snmp mib notification-log default
CSCee32814	IPServices	Source port selection is predictable, should be harder to guess
CSCeg51303	IPServices	VRRP responds with int MAC instead of VMAC afetr shut/no shut
CSCsd23056	IPServices	reverse telnet (tty daemon) broken by TCL feature
CSCsd33013	IPServices	FHRPs fail to clear ARP entry after Duplicate IP event
CSCsd69052	IPServices	Netbios/NAT optimization
CSCse23548	IPServices	modular ios (ION) : logging source-interface command ignored
CSCsf16715	IPServices	TCP will leak TCBs if app closes in notification callback context
CSCsf33034	IPServices	T/B tcb_isvalid+7C during bootup and when EOMPLS vc is configured.
CSCek46996	LAN	Cwan FA-PA port need to be in promiscous mode if IP address not conf
CSCsc95736	Management	cns config partial command causes cpu up 25%
CSCef32748	MPLS	tfib_ipfib_post_table_change needs to check for recursive routes
CSCek31478	Multicast	ip multicast boundry cmd does not take effect after modify ACL
CSCek42421	Multicast	One prune not processed on receiving batched join/prune message
CSCsd49955	Multicast	RPF info created by (S,G) RPT-bit prune does not change by (S,G) join
CSCse09435	Multicast	PGM router assist on GRE causes small pool buffer leak
CSCse20714	Multicast	MSDP doesnt send triggered SA for non-directly connected PIM-DM source
CSCee93983	platform-76xx	osm : egress CE router is missing in traceroute in MPLS/VPN

Identifier	Technology	Description
CSCeh32595	platform-76xx	Ping fails across atm interface after configuring routing protocols
CSCsd25766	platform-76xx	OSM-1OC48-POS: APS Protect-Inactive port is receiving and fwding packets
CSCsd80632	platform-76xx	12.2(18)SXE2 ifHCInOctetssub interface traffic is not close to the main
CSCsd88401	platform-76xx	input packet drop w/ gt48520 mac_rx_error at port2 on OSM-2+4GE-WAN+
CSCse26606	platform-76xx	packet drop occur when issuing shut/no shut on other sub-if /w OSPF
CSCeg26728	QoS	BGP fails to establish a peer with policy bw 199K
CSCek44025	QoS	Hierarchy is not collapsed when FRF.12 is configured
CSCsc00993	QoS	Lower tx-ring-limit for ATM VCs with higher SCR when QoS is enabled
CSCse02510	QoS	Crash with ALIGN-1-FATAL at hqf_process_wfq_command
CSCse54611	QoS	WS-X6582-2PA bus error crash on hqf_cwpa_pak_enqueue_local
CSCee71850	Routing	Router crashes while unconfiguring IPX GRE
CSCee77180	Routing	Static routes with space in name not recognized after reload
CSCei26931	Routing	fragment option is not in access-list command
CSCej42121	Routing	clear adj hangs router
CSCin85894	Routing	Reflexive acl when used as ext. acl gives T/bks & crashes with std.
CSCsc37212	Routing	ISIS: Redistributed routes might not be advertised if interface flaps
CSCse52184	Routing	unrelated MPLS TE tunnel flapping cause unnecessary fib/lfib updates
CSCse61025	Routing	ip http auth aaa is not needed for Authproxy to work
CSCsb62045	Security	scp connection fails with error: unexpected filename:
CSCse29545	Security	Crypto pki trustpoint loses ip-address command upon reload
CSCec42435	Unknown	crypto map local-addr command may disappear on E1and T1 interfaces
CSCeh52424	Unknown	OC3 ATM/SPA: Input CRC errors caused SIP200_SPIRX-3-SPI4_LINKERROR
CSCej08637	Unknown	Inline power sensors needed on standby to support entity mib SSO.
CSCek22782	Unknown	CSM: Configuration sync check does not work in all cases
CSCek28561	Unknown	SIP1/ChOC3: T1/E1 BERT unusable after first run
CSCek36288	Unknown	EoMPLS VC down with SIP1 as core facing interface
CSCek50720	Unknown	Improve error handling for DLL centering algorithm
CSCsa77785	Unknown	Router crashes when L2 redirection is configured with HTTP traffic
CSCsa95306	Unknown	SNMPWALK does not get all CSG user group information
CSCsa96972	Unknown	Dbus header err int be triggered when recovery procedure on DFC3
CSCsb41923	Unknown	isakmp key ending in backslash will be lost after device reboot
CSCsb80468	Unknown	Hvpls: MAC Addresses May Not Be Flushed When VC Goes Down
CSCsb82048	Unknown	%ALIGN-3-CORRECT: Alignment correction made at 0x402B4BA4
CSCsc20064	Unknown	Ping fails on changing removing and reconfiguring controller for ChSTM1.
CSCsc25952	Unknown	Need to print out error message for unsupported marking on OSM
CSCsc56766	Unknown	Slow convergence of DEC for mac-address moving from one FE to another FE
CSCsc59025	Unknown	UDLD config on 2nd uplinki of act/sby sup change after switchover

Identifier	Technology	Description
CSCsc75397	Unknown	sup32 enables fix for CSCeb49514 with cross-module etherchannel
CSCsc81300	Unknown	uRPF check ACL programming spikes RP CPU
CSCsd46882	Unknown	OSM-CT3 Port in Unchannelized mode stays UP/UP when looped towards line
CSCsd47475	Unknown	cat6k unable to resolve arp request when using flexwan, pa-fe-tx and vpn
CSCsd53513	Unknown	%ALIGN-3-SPURIOUS_SO: Spurious memory access seen with tracebacks
CSCsd64103	Unknown	'mls qos trust dscp' not working for traffic coming from FWSM
CSCsd80745	Unknown	bus error or alignment err at crypto_isakmp_profile_contain_xauth_info.
CSCsd94439	Unknown	I/O mem corruption on SP with mld snooping report-suppression enabled
CSCsd95575	Unknown	RP-Crash @ draco2_pa_eobc_intr
CSCsd96121	Unknown	Mac's don't get purged when the port is blocking during topology change
CSCse09460	Unknown	Agg ram is not programmed properly after switch over
CSCse15906	Unknown	CAT6500/7600 Sup2 show int counters output drops double the qos drops
CSCse16512	Unknown	Egress Queuing on WS-6148-21AF broken
CSCse19732	Unknown	Not able to apply policy on a port -which is earlier part of l3 port-cha
CSCse29001	Unknown	ISIS did not update when encap frame-relay on POS SPA of SIP-400
CSCse29419	Unknown	Need SNMP support for traffic counters given by 'show vlan counters'
CSCse33257	Unknown	Intf Flap causes memory Hog in mls-msc on DFC installed Sup720 system
CSCse33395	Unknown	HSRP track interface in down state in ITASCA though active on SUP
CSCse33488	Unknown	DS1: Back to back connectivity not successful between T1/E1 SPA-PA
CSCse35278	Unknown	VPNSM drops transit NAT-T packets
CSCse47430	Unknown	Need boundry check in heartbeat_create_recv_info
CSCse47811	Unknown	Guard output does not reach GRE tunnels on SUP-720
CSCse50503	Unknown	Hybrid fix for CSCed74512
CSCse50607	Unknown	SPA-8XCHT1E1 IPC failure causes latency and MLPPP lockups
CSCse51577	Unknown	Sup2/MSFC2: Memory leak at Dead/FM VMR chunk when pasting in NAT config
CSCse54768	Unknown	CASA traffic not CEF switched
CSCse59777	Unknown	WLSM: CPUHOG on L3mm process
CSCse61121	Unknown	Memory leak in FIB Control Task
CSCse61252	Unknown	ION : reset reason displayed incorrectly in show version
CSCse62117	Unknown	cbQosCMDropByte reset after clear counters
CSCse63856	Unknown	Sup720 Doesn't Terminate GRE Properly - Packet Recieved on Wrong Int.
CSCse67650	Unknown	SIP600 WRED fails to forward ARP packets
CSCse69713	Unknown	Redirect traffic punted to software when all CEs in the group are lost
CSCse69748	Unknown	CLI for IMAP retcode in CSG refunding is broken
CSCse73539	Unknown	c7600 - crash of active sup720 after inserting a second one
CSCse85399	Unknown	traffic does not go over crypto tunnel after a no shut.
CSCse86602	Unknown	Cat6500 IOS does not set correct portAdminSpeed

Identifier	Technology	Description
CSCse87417	Unknown	FlexLink : ARP frames w/ known opcodes cause interop issues.
CSCse88171	Unknown	PA-MC-8TE1+: cRTP compression failure
CSCse98354	Unknown	SIP-200: SYNC FAILED not initialized. Interfaces up/down.
CSCsf00089	Unknown	Packets not HW switched after test crash invoked
CSCsf03566	Unknown	Memory corruption crash trying to free unassigned block
CSCsf04301	Unknown	Multicast on ATM SPA with P2MP sub-interfaces does not work
CSCsf13325	Unknown	Commit of CSCse95804 broke v122_18_sxf_throttle s3223-adventerprisek9_wa
CSCsf15527	Unknown	ION: Reset Reason Does Not Change on Normal Reload
CSCsf31504	Unknown	TestFabricFlowControlStatus: Monitor interval is to be reduced to 100ms
CSCef01547	WAN	7200 tx-ring resets to default after OIR
CSCek27504	WAN	NTP crash during show runn after deletion of NTP ref-peer
CSCse95146	WAN	Sup720 with cross module etherchannel duplicates all packets

Resolved Caveats in Release 12.2(18)SXF5

Resolved Infrastructure Caveats

- CSCsc64976—Resolved in 12.2(18)SXF5

  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 LAN Caveats

- CSCsd34759—Resolved in 12.2(18)SXF5

  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)SXF5

  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)SXF5

  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.

- CSCsd75273—Resolved in 12.2(18)SXF5

  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

- CSCsd37415—Resolved in 12.2(18)SXF5

  Cisco Catalyst 6500 series systems that are running certain versions of Cisco Internetwork Operating System (IOS) are vulnerable to an attack from a Multi Protocol Label Switching (MPLS) packet. Only the systems that are running in Hybrid Mode (Catalyst OS (CatOS) software on the Supervisor Engine and IOS Software on the Multilayer Switch Feature Card (MSFC)) or running with Cisco IOS Software Modularity are affected.

  MPLS packets can only be sent from the local network segment.

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

- CSCse52951—Resolved in 12.2(18)SXF5

  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)SXF5

  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)SXF5

Identifier	Technology	Description
CSCsb11698	AAA	Input Queue Wedge with TACACs
CSCei71142	ATM	autovc handling stopped
CSCse35684	ATM	OSPF adjacency does not recover from OIR active supervisor
CSCsc94191	Content	WCCP does not GRE Redirect TCP FIN packet that would fragment
CSCed21186	Infrastructure	Incorrect GE output IFMIB counters when CAR is configured
CSCee24395	Infrastructure	SYS-3-BADMAGIC after GetNextObjectInstance clogHistoryEntry_get
CSCei85359	Infrastructure	%SCHED-3-SEMLOCKED: IP RTR Probe MaxName attempted to lock a semapho
CSCek24385	Infrastructure	ION config checkpoint for process restart must handle SNMP, HTTP
CSCin62031	Infrastructure	Crash when SNMPset rttMonCtrlAdminStatus to 1 (IP SLA Probe activation)

Identifier	Technology	Description
CSCsa61284	Infrastructure	snmpset rttMonCtrlOperState to 7 (restart) cause rttMonCtrlAdminStatus 2
CSCsb08386	Infrastructure	PRP crash by show ip bgp regexp
CSCsb16702	Infrastructure	Configuring using http forced sw-crash on standby supervisor
CSCsb34180	Infrastructure	Rockies 3 SNMP: PS in entPhysicalChildIndex not in incremental order
CSCsc06891	Infrastructure	no traps are sent when CF is inserted or removed.
CSCsc85922	Infrastructure	IOS changes its implementation of what is an unknown community tring
CSCsc97279	Infrastructure	Takes long time (more than 2 minutes) on wr mem
CSCsd32923	Infrastructure	Bus Error in Exec attempting command completion in a full command buffer
CSCsd77751	Infrastructure	IOS - SUP720 - sends empty/blank syslog messages
CSCec10091	IPServices	DHCP relay agent forwards requests with src. 0.0.0.0
CSCed93425	IPServices	DHCP Database fails to write to local flash.
CSCeh35083	IPServices	NAT-PPTP change Call ID wrongly
CSCsd80754	IPServices	HSRP Active-Router not respond to ARP request about VIP
CSCec87736	LAN	SNMP counters on FE subif not updated for dcef
CSCsc69537	LAN	GigE sub-interfaces not registered with SNMP after LC reload
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
CSCsd55300	LegacyProtocols	DLSw ER LLC session fails to connect with SUP720 or SUP32
CSCse17611	LegacyProtocols	DLSw Circuits Connect outside of DLSW ER to switch with passive mapping
CSCef78565	Management	cdp not advertising ifName
CSCek35484	MPLS	FRR: MP tears down protected lsp if local protection des flag rese
CSCsc94359	MPLS	BGP table and CEF forwarding table have mismatched labels
CSCsd41981	MPLS	TFIB on SUP720 PFC is broken when an OSM (GE-WAN) card was disabled
CSCsd57678	MPLS	Label inconsistency between BGP and forwarding tables for remote routes
CSCei77227	Multicast	PE router crashes @ igmp_delete_group while unconfiguring vrf
CSCej20707	Multicast	igp and pim neighbor goes down during mcast stress testing
CSCej78303	Multicast	RP crash @ pim_tt_grange_first after CMD: no ipv6 unicast-routing
CSCsb76434	Multicast	PIM: auto-rp group stuck in registering when sparse-mode
CSCsb85290	Multicast	IPv6 BSR: BSM forwarding breaks with ipv6 vrf implementation
CSCsc69155	Multicast	ciscoIpMRouteIfInMcastOctets counts decrease
CSCsc96746	Multicast	PIM-sm chooses wrong RPF interface in equal cost multipath network
CSCsc98828	Multicast	PIMV6: SR flag set on RP acting as first hop
CSCsd64138	Multicast	ip multicast rpf not configurable in 12.2(18)SXF3
CSCsd68993	Multicast	Fluctuation in IPv6 mcast trffic fwdng happns with large numbr of strms
CSCse05960	Multicast	PIM leaking memory used for xdr messages
CSCse64256	Multicast	FHR crashes on starting Embedded RP stream
CSCsb64975	platform-76xx	Rate counters are erratic for a bi-dir traffic more than 2 Gig

Identifier	Technology	Description
CSCse05336	platform-76xx	Packet drop on OSM-2+4GE-WAN+ if sub-if is created or deleted
CSCsc33562	PPP	SNMP ifInOctets shows negative value for MLP interface
CSCsc37902	PPP	Standby MSFC may experience bus error after RP_MLP-4-MISCONFIGLINK.
CSCsd34741	PPP	dMLP: line card might crash with cRTP enabled.
CSCec80902	QoS	Router crashes with Bus Error at 0xFD011147
CSCsa68661	QoS	LC crashes when service-policy is configured on channelized interface
CSCdt69452	Routing	scaling: need ability to do clear ip arp A.B.C.D.
CSCea71711	Routing	Missing cef table for tableid 2829 during Table removal event
CSCee47792	Routing	OSPF Traps does not use IpAddress. Uses type integer at present
CSCee81606	Routing	LSAs not generated when redistributing connected subnets into OSPF
CSCef11304	Routing	MIB walk on OSPF-MIB involving ospfExtLsdbTable crashes switch
CSCef17647	Routing	NPE-G1:tracebacks when high nmbr of RIP neigh/low update timer
CSCeg16631	Routing	CSCee32557 breaks RIP distribute-list w/ VRF interface
CSCeg52659	Routing	BGP route may not get withdrawn under rare condition
CSCeh54086	Routing	ABR fail to update LSA type3 in response to shut interface.
CSCei45669	Routing	OSPF router may fail to flush its self-originated LSA
CSCej89011	Routing	LSA received via Demand Circuit may show aging
CSCek45564	Routing	iprouting crash with corrupted block on mpath config change
CSCsb36755	Routing	BGP does not delete multi-path route when receiving worse metric UPDATE
CSCsc07467	Routing	OSPF route lost after interface flap.
CSCsc10494	Routing	Partial SPF may skip an LSA
CSCsc63871	Routing	Only 1 clns adjacency on ethernet but several neighbors
CSCsd00028	Routing	OSPF: spurious access in ospf_generate_trap
CSCsd03882	Routing	SUP720 RACL Deny ACE not being implemented
CSCsd64173	Routing	Bus error crash IPV6 due to OSPF summary prefix command
CSCsd84489	Routing	Crash in ospf_add_all_stub_routes on topology change
CSCsd99760	Routing	After iprouting.iosproc Process Restart Routing table not updated
CSCuk58462	Routing	Routes are not filtered even when route-map rule sets deny the rule
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)
CSCea24341	Unknown	SLB real to real ICMP traffic broken with FWLB
CSCeb68312	Unknown	IOS SLB HTTP probe uses :0 in host tag
CSCeb77318	Unknown	IOS SLB: Incorrect checksum of forwarded icmp unreachable
CSCed61394	Unknown	Easy VPN(with RSA) does not work with XAuth
CSCef21434	Unknown	isakmp profiles only use one trustpoint.

Identifier	Technology	Description
CSCeg86665	Unknown	Trust state - Tunnel decap side, modify the original packets dscp
CSCeh21210	Unknown	MF: DHCP Snooping crash when server send invalid option 82
CSCeh42489	Unknown	cbQosCMDropByte64 always shows the same value as cbQosCMPrePolicyByte64
CSCeh78411	Unknown	Failed IKE sessions does not get deleted in certain conditions
CSCei37299	Unknown	clear crypto session remote ip may crash router if client reconnect
CSCei93025	Unknown	Etherchannel config changes not synched to inactive member ports
CSCei95384	Unknown	PP:R3:8xT1/E1-SPA MLP: EFC ERROR/inactive after link added to bundle
CSCej86188	Unknown	MLS packet error syslogs should be configurable and no service int
CSCek22536	Unknown	SLB high cpu with second VIP inservice and user->real traffic
CSCek22595	Unknown	SLB vserver access commands break user->real traffic
CSCek24053	Unknown	Sup720_rp: spurious memory accesses in cardifmib_get_card_index
CSCek26155	Unknown	EEM cli ED can enter recursive loop with action cli commands.
CSCek26158	Unknown	IOS TCL leaks memory when EEM policy triggered.
CSCek28863	Unknown	Need to change default SCP keepalive timeout on IOS to CSM module
CSCek30589	Unknown	WS-X6196-RJ-21/ WS-F6K-FE48X2-AF inline power auto detect
CSCek31437	Unknown	6516 with Sup32 should not be powered down as unsupported module
CSCek32555	Unknown	MFR i/f lineprotocol takes too long to come up after RPR+ switch
CSCek35417	Unknown	NVRAM write failed on runtime image for Rommon Upgrade.
CSCek35770	Unknown	Need show module power equivalent in IOS
CSCek35951	Unknown	Priority queue with policing configured doesnt work
CSCek37181	Unknown	Loopback on controller for online diagn of wism card
CSCek42027	Unknown	SPA FPD upgrade fails with sip1-CR
CSCek47714	Unknown	The supervisor crashed after second switchover in rpr-plus mode
CSCin96942	Unknown	BAD_RESET and HARIKARI messages with linewatch_timer and crash
CSCin98448	Unknown	controller shut throws up error msg and remote end is not going down
CSCsa76455	Unknown	Sup32:Pkts switched out with incorrect DA MAC for VRF adjacency
CSCsa98081	Unknown	up/downgrade in SXB code w/ crypto connect, BGP fails
CSCsa99158	Unknown	Unexpected START records triggered by IPSec - unreliable AAA records
CSCsb29028	Unknown	Processor Memory leak in Crypto IKMP process
CSCsb53810	Unknown	sup720 outbound acl not denying traffic, hitting incorrect tcam entry
CSCsb61021	Unknown	IP Spoofed packets from CE are not hw switched with egress WCCP
CSCsb72854	Unknown	CONFIG_FILE ROMMON var and boot config support for c6k
CSCsb79306	Unknown	C2R3: cbeDot1dTpVlanIndex is out of sync w/ CLI causes standby sup reset
CSCsb85024	Unknown	WS-X6148A-GE-TX corrupt counter dot3StatsInternalMacReceiveErrors
CSCsb86198	Unknown	show port-sec int <int-name> add not sync with stdby after SO
CSCsb91644	Unknown	IPv6 MFIB entry is updated on RP and delayed to update MFIB on SP & DFC
CSCsc05015	Unknown	SNA packet is not bridged when VLAN1025 is used on bridged interface

Identifier	Technology	Description
CSCsc08857	Unknown	LPIP:eou_sm_post_event traceback on clear ip device tracking all
CSCsc10914	Unknown	Tracking fails at reload for inteface with switchport enabled
CSCsc18986	Unknown	IOS SLB causes high CPU
CSCsc22552	Unknown	low address access crash upon malloc_fail for tcl script output
CSCsc26237	Unknown	Bus error at hqf_police_update
CSCsc29942	Unknown	Could not retreive/set EEM MIB objects values from snmp workstation
CSCsc30268	Unknown	linecards crash @ free_qos_set_if_sub_structures
CSCsc38892	Unknown	slb http and tcp probes not working with access ints/vrf
CSCsc43862	Unknown	SPA ping failure caused by SIP-200 serial primary channel sync failure
CSCsc46301	Unknown	Crash in GTP SLB imsi sticky
CSCsc51357	Unknown	Unicast Flood Protection causes CSM redundancy to transition
CSCsc54382	Unknown	RE: L3 DEC activates EC purging
CSCsc54552	Unknown	mac-address-table static configuration problem
CSCsc61809	Unknown	Min-links feature doesn't work intermittently even just on shut/no shut
CSCsc62574	Unknown	ifHCInUCastPkts are decremening between 2 polls
CSCsc71245	Unknown	sup720:High CPU and traceback in ipsec_db_get_ipsec_sa_list with VPNSM
CSCsc77703	Unknown	SYS-SP-3-CPUHOG process = FIB Control Task
CSCsc84683	Unknown	crash observed on removal of certain mcast mac address
CSCsc86540	Unknown	SIP-400 Tracebacks occur when upgrading FPD on SIP 400
CSCsc87117	Unknown	slowness in updating DF in HW after doing shut or no shut RPF link
CSCsc89229	Unknown	Traceback & crash at pm_get_standby_vlan on Sup720
CSCsc89979	Unknown	EEM traceback for,action x info cli frequenc; if cli history table empty
CSCsc90782	Unknown	dsx1FarEndInterval not available in 12.2(18)SXF on a c7609
CSCsc94171	Unknown	FIBTCAMSSRAM on Ant24/NikeXL fails if running FIBTCAM in Aph in parallel
CSCsc95631	Unknown	Rapid PVST does not automatically recover from ROOT_Inc (Root Guard)
CSCsd01719	Unknown	SIP-600: SPA OIR with DOT1Q tunnel on port-channel can crash RP
CSCsd03416	Unknown	Active RP Crashed after doing rerouting in PIM SM Stress Test
CSCsd05513	Unknown	7600 CBQOS-MIB is missing info which is present in CLI
CSCsd08411	Unknown	EEM Tcl policy execution delayed relative to config size
CSCsd14307	Unknown	PA-MC-8TE1+ PA shows alarm led red even with all controllers shut down
CSCsd15806	Unknown	r2.5:Tcam is not programmed after shut/no shut on interface
CSCsd16407	Unknown	Ingress service-policy on SPA10X1GE interface fails to police traffic
CSCsd17174	Unknown	SLB Connection states get into loop on snmp query
CSCsd17992	Unknown	After PS fails and powered on, PS fan fail msg. display even if PS on
CSCsd25447	Unknown	bill-of-materials file update failed on rollback activation
CSCsd25532	Unknown	High SP-CPU utili occurs when c7600 recieves IPv6 Multicast traffic
CSCsd25611	Unknown	MPLS VPN forwarding broken for new vrfs on PE 7600 SUP720

Identifier	Technology	Description
CSCsd28870	Unknown	Entries from redirect acl list with log keyword not programmed into tcam
CSCsd28995	Unknown	ip default-network is not installed if it is ip2tag fib
CSCsd29927	Unknown	6500 BIT-SP-4-OUTOFRANGE error with voice vlan dot1p and monitor session
CSCsd31503	Unknown	Cat6k Selective Packet Discard drops OSPF packets
CSCsd35622	Unknown	session timeout TCL causes CPU hog/crash
CSCsd37537	Unknown	ipMRouteInterfaceOutMcastOctets not incrementing, remains zero
CSCsd37634	Unknown	SCCP portion of Skinny packet is not being NATd
CSCsd39189	Unknown	ALIGN-3-CORRECT with DHCP Snooping when using Option 82
CSCsd40211	Unknown	Sup720 : Delay in arp result after interface shut/no shut
CSCsd42247	Unknown	Config rspan, remove rspan and then config span cause unidirect. traffic
CSCsd42850	Unknown	mGRE broadcast issue, invalid checksum seen on IP Header Checksum
CSCsd43185	Unknown	Tx queue cos maps for even ports of card WS-X6416-GBIC are incorrect.
CSCsd43481	Unknown	EoMPLS drops OSPF multicast packets with mls ip verify length minimum
CSCsd45167	Unknown	Memory leak in Crypto IKMP Process
CSCsd49280	Unknown	show idprom should work with non-cisco xenpaks
CSCsd49723	Unknown	Memory leak in Crypto IKMP Process when using certificate authentication
CSCsd49767	Unknown	Memory leak in Crypto IKMP process
CSCsd52633	Unknown	VPN-Spa stop forwarding traffic if any changes on ATM traffic shaping
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
CSCsd59274	Unknown	MLD snooping report-suppression does not work correctly
CSCsd59975	Unknown	WS-X6704-10GE causing CRC errors on WS-X6502-10GE interfaces
CSCsd64158	Unknown	%MLSCEF-SP-2-FREEZE: hw switching disabled due to mls cef sanity failure
CSCsd64741	Unknown	SLB IMSI sticky idle timeout queries fail to reach GGSN when vrf-aware
CSCsd65434	Unknown	igmp snooping fails when leave is processed during igmp general query
CSCsd67341	Unknown	WS-X6148A-45AF compatible issue with 3rd party Video Camera
CSCsd67456	Unknown	VPN-SPA: IPSec SA comes up with wrong lifetime in KB
CSCsd68266	Unknown	input errors increment on 10/half port
CSCsd70494	Unknown	Bidir-Multicast Packets are dropped when using G/m entries
CSCsd70948	Unknown	After SSO switchover all CDP and BPDU are lost if L2 rate limiting is on
CSCsd71047	Unknown	NAT cef entry is not changed after IP address change MAC address
CSCsd74975	Unknown	Clearly indicate customer friendly bus stall log messages.
CSCsd75069	Unknown	IPC RX FIFO FULL err w/ high traffic&LC CPU (IO-FPGA Pat-Mav2.5/Pro1.5)
CSCsd75929	Unknown	Sup32 fails to get DHCP snooping binding table on switchover
CSCsd81263	Unknown	After reload, sup32 system unable to communicate with all neighbors
CSCsd86340	Unknown	After unplugging PC from back of phone into new port - error disable
CSCsd90501	Unknown	Minimum/Maximum WRED thresholds for default DSCP stays at 32/64

Identifier	Technology	Description
CSCsd94127	Unknown	COS aligned to IPP for routed multicast traffic
CSCsd94541	Unknown	Multiple T3 controllers bounce on the SPA
CSCsd95279	Unknown	VPNSM uses incorrect MTU if egress interface is down at boot time
CSCsd96511	Unknown	Interface admin down: egress TCAM default program as bridge
CSCsd98390	Unknown	WS-X6148A-45AF module may not bootup/lose config on switch power-cycle.
CSCsd98421	Unknown	MPLS:VPN:QoS:set mpls exp fail at ingress PE OSM interface
CSCsd98887	Unknown	SP Memory Leak In mls-msc Process
CSCse00284	Unknown	ION Code crashes active sup under heavy stress and show proc cpu cmd
CSCse11333	Unknown	Native IOS does not syslog thermal warnings from IDSM-2 Cat6k card.
CSCse12195	Unknown	6816: Interface 3/4 flapping when interface 3/1 is not connected
CSCse15495	Unknown	sip-600 and 10GE SPA - incorrect cbQosCMPostPolicyByte64
CSCse15728	Unknown	VPNSM does not perform invalid spi recovery in vrf mode
CSCse23889	Unknown	Bus error when configuring xconnect vfi from int vlan
CSCse41480	Unknown	cos vlan priority is not preserved for MPLS traffic over EoMPLS tunnel
CSCse41963	Unknown	RSPAN+VACL is broken when DEC is configured in system
CSCse54041	Unknown	CSM config sync timemout with large configs
CSCse60601	Unknown	Standby Sup crash due to ACLDeny bug in TYCHO
CSCse70423	Unknown	change WS-X6708-10GE default behavior for non-E chassis

Resolved Caveats in Release 12.2(18)SXF4

Resolved LAN Caveats

- CSCsd34759—Resolved in 12.2(18)SXF4

  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 Unknown Caveats

- CSCsd28570—Resolved in 12.2(18)SXF4

  Symptom: A vulnerability exists within the Cisco IOS Authentication, Authorization, and Accounting (AAA) command authorization feature, where command authorization checks are not performed on commands executed from the Tool Command Language (Tcl) exec shell. This may allow authenticated users to bypass command authorization checks in some configurations resulting in unauthorized privilege escalation.

  Conditions: Devices that are not running AAA command authorization feature, or do not support Tcl functionality are not affected by this vulnerability.

  This vulnerability is present in all versions of Cisco IOS that support the **tclsh** command.

  Workaround: This advisory with appropriate workarounds is posted at http://www.cisco.com/en/US/products/csr/cisco-sr-20060125-aaatcl.html

  Further Problem Description: This particular vulnerability only affected Cisco IOS versions 12.3(4)T trains and onwards. (12.3 Mainline is not affected)

  Please refer to the Advisories "Software Versions and Fixes" table for the first fixed release of Cisco IOS software.

Other Resolved Caveats in Release 12.2(18)SXF4

Identifier	Technology	Description
CSCsb12329	ATM	ifAdminStatus of ATM sub-interface is down without shutdown command
CSCsc72066	Content	MNLB - incorrect affinities installed
CSCsb14936	Infrastructure	SNMPv3 EngineID (default value) not established correctly
CSCsb85983	Infrastructure	bootflash corruption seen even with CSCei17174 fix
CSCeg61169	IPServices	Traceback recorded in tcb_isvalid by TCP Remote Shell Process .
CSCsc47919	IPServices	VRRP does not correctly interoperate with Proxy ARP
CSCsd34855	LAN	VTP update with a VLAN name >100 characters causes buffer overflow .
CSCeh67947	Multicast	Auto-RP group 224.0.1.40 Pruned after Assert.
CSCek26627	Multicast	CPUHOG when RPF change affects ~30k mroutes
CSCsc16148	Multicast	Allow (S,G) expiry timer to be configurable
CSCeh62084	PPP	ifStackStatus drops ifIndex when interface is OperStatus down
CSCsb97950	PPP	dLFIoATM: Packets with CLP set, get punted to RP.
CSCee58986	QoS	fair-queue nvgen does not happen
CSCsc98510	QoS	Ehanced Flexwan reloads with VRF/MLPPP/QoS
CSCsd71119	QoS	ALL ATM PVC DOWN IN FLEXWAN WITH PA-A3-OC3 AND OAM
CSCed82273	Routing	IPV6 I-BGP does not reach established state
CSCef35386	Routing	BGP does not inform PIM of the second best VPNv4-MDT
CSCeg77104	Routing	EIGRP neigh over ATM IMA link flaps due to Authentication failure
CSCsa64947	Routing	High CPU seen after clear arp
CSCsa68988	Routing	route-map cache for soft-reconfig is not made when BGP peer comes up
CSCsb78345	Routing	ipv6: Sup720/3b-XL crash when show ipv6 cef after OSVFv3 cost change

Identifier	Technology	Description
CSCsc59089	Routing	BGP: updates missing if route-refresh received while updates on OutQ
CSCsc67367	Routing	set ip next-hop in-vrf not working with import maps
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
CSCsd11631	Routing	7600: Spurious accesses originated by OSPF process
CSCsd12904	Routing	OSPF sham-links do not come up
CSCsa63387	Security	Router may crash when CRL expires
CSCei27448	Unknown	Router crashes while displaying sh ip pim mdt bgp
CSCek26158	Unknown	IOS TCL leaks memory when EEM policy triggered.
CSCek26186	Unknown	ATM SPA: setup vp fails.
CSCek32944	Unknown	GLOBAL,DONTWAIT registries broken
CSCsb12969	Unknown	MQC: Router crashes when a service-policy is added to atm or FR pvc
CSCsb33258	Unknown	RP crash while mvpns come up - MDFS buildup
CSCsb61514	Unknown	Packet drop for size > 1526B between SUP <-> MWAM
CSCsb94412	Unknown	SIP1: RBE: OAM Packets being accounted as input errors
CSCsc22552	Unknown	low address access crash upon malloc_fail for tcl script output
CSCsc46105	Unknown	Not carryover ToS value if enabling mls qos on Native IOS
CSCsc55406	Unknown	Tcl scripts leak memory upon every run
CSCsc57156	Unknown	Hardware fault on FWSM ports not causing FWSM redundancy failover
CSCsc65256	Unknown	Connection Count incorrect after ungraceful disconnect/reconnect
CSCsc68250	Unknown	Packet flow halt on 7600-SIP-400
CSCsc86600	Unknown	SNMP:subinterface aal5 layer: Ifindex counter for ATM SPA not updated
CSCsc91075	Unknown	IPSEC Connection Count incorrect after unsuccesfull connection attempt
CSCsd02881	Unknown	Spanning tree issue with vlan mapping and trunk port
CSCsd10975	Unknown	IOS TCL uses ifs_close to close a tcp socket in tclIosChan.c
CSCsd19203	Unknown	SIP400:ATM:new LLQ traffic stop flowing on dynamic changes to Policy
CSCsd33647	Unknown	ER: Improve C2 MET programming under heavy traffic scenarios
CSCsd44517	Unknown	flow control needs to be toggle off/on to become active after no shut
CSCsd45479	Unknown	Process restarts not guaranteed if installer is in list of processes ...
CSCsd47734	Unknown	Additional memory leak fixes by ActiveState
CSCsd04219	WAN	Add feature support for ACLs in 12.2SXE on virtual templates

Resolved Caveats in Release 12.2(18)SXF3

Resolved Routing Caveats

- CSCec12299—Resolved in 12.2(18)SXF3

  Devices running Cisco IOS versions 12.0S, 12.2, 12.3 or 12.4 and configured for Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) or VPN Routing and Forwarding Lite (VRF Lite) and using Border Gateway Protocol (BGP) between Customer Edge (CE) and Provider Edge (PE) devices may permit information to propagate between VPNs.

  Workarounds are available to help mitigate this vulnerability.

  This issue is triggered by a logic error when processing extended communities on the PE device.

  This issue cannot be deterministically exploited by an attacker.

  Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

  This advisory is posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20080924-vpn.html

Other Resolved Caveats in Release 12.2(18)SXF3

Identifier	Technology	Description
CSCeg62070	Infrastructure	Tracebacks noticed with Radius configs through HTTP Post
CSCsb69614	QoS	data bus error - NBAR match_heuristic_label w/RTP UDP traffic
CSCsc95511	QoS	Bus error crash at hqf_scheduler_info_init
CSCsa81039	Routing	EIGRP PE-CE:routing loop when a prefix has no cost-community
CSCsc24102	Unknown	Fabric sync errors if WS-X6704-10GE is on slot 4 on 7606
CSCsc39902	Unknown	Sup720 SNMPGET of dot1dTpFdbPort returns variable does not exist
CSCsc55949	Unknown	C2 Frequent fabric channel sync errors and rxErrors
CSCsc57156	Unknown	Hardware fault on FWSM ports not causing FWSM redundancy failover
CSCsc68250	Unknown	Packet flow halt on 7600-SIP-400
CSCsc89044	Unknown	IO memory leak with big buffers and EOBC0/0
CSCsd01885	Unknown	Flexwan module, when pvc is down, mac-address are not flushed
CSCsd10156	Unknown	crashinfo missing Additional Subsystem section if core file configured
CSCsd12976	Unknown	Installing image/patch fails on internal compact flash adapter
CSCsd16853	Unknown	X6196-RJ-21 or X6148X2-RJ-45 may fail to boot when running Sup IOS
CSCsd20092	Unknown	Device crashes with fabric error on bootup starting from 28th build
CSCsc86344	WAN	NNI fr intfs with keepalives enabled remain down/down after reload

Resolved Caveats in Release 12.2(18)SXF2

Resolved AAA Caveats

- CSCed09685—Resolved in 12.2(18)SXF2

  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)SXF2

Identifier	Technology	Description
CSCsc33348	AAA	AAA Down: AAA Memory Leak
CSCsb27358	Access	PA-T3+ goes down when seeing two bursts of AIS less than 1 second each
CSCec17185	ATM	PA-A3: VBR traffic shaping inaccurate when PCR=SCR.
CSCsc49134	ATM	Router crashes while creating ATM subinterface - ATM pvc discovery
CSCsc62474	ATM	Some of the PVC might not get deleted through ATM periodic process
CSCsb21972	Content	Tracebacks when both WCCP and Netflow are configured
CSCeb05456	Infrastructure	nvram file locking incorrect for remote file operations
CSCeb62508	Infrastructure	ATA disk corruptions caused by ATA device re-entrant
CSCec75641	Infrastructure	GRP-B: Switchover due to bus error with ip as-path access-list
CSCef11195	Infrastructure	MIPS platforms take Address Error Exception in malloc()
CSCeh44660	Infrastructure	Router crashed while writing the crashinfo to disk
CSCei32102	Infrastructure	Need an option to disable snmp traps for link during switch failover
CSCej08355	Infrastructure	Memory corruption on MSFC with syncnlmTable
CSCej42935	Infrastructure	Incorrect use of directory entry buffer by dfs_next()
CSCsb67916	Infrastructure	SNMP Authentication Failure Trap source ip address 0.0.0.0
CSCsb81704	Infrastructure	SNMP SSO: OID Set on multiple MIBs reset stdby Sup ALIGN-1-FATAL
CSCsb89834	Infrastructure	Config is not saved after write mem from config mode then changing cfg
CSCsb93316	Infrastructure	%CPU_MONITOR-NOT-HEARD causes RP/SP ios-base crash
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
CSCsa51150	IPServices	NAT translation not timing out correctly when a TCP session closes
CSCsb51019	IPServices	TCP session stuck in FINWAIT1 after BGP password changed
CSCsc39357	IPServices	TCP sessions flap under zero window scenario
CSCeh18295	LegacyProtocols	circuit cant get connected via DLSw ER
CSCeh18390	LegacyProtocols	DLSw load-balance doesnt distribute the load evenly with cir count

Identifier	Technology	Description
CSCsa45750	LegacyProtocols	DLSw load-balancing not working as remote mac is not in reachability
CSCeh51720	MPLS	TE LM floods link in wrong area after links area is changed in ospf
CSCsa62908	MPLS	OSPF Opaque LSA not advertised after shut/no shut on MPLS TE interface
CSCsa69210	MPLS	Cannot create VRF in RPR mode
CSCsb16512	MPLS	High CPU in CEF Process and CEF scanner due to prefix reresolve
CSCsc40027	MPLS	corrupted program counter crash - IP-3-LOOPPAK
CSCef65806	Multicast	CISCO-PIM MIB object cpimLastErrorRP truncated when polled
CSCeh93087	Multicast	Need triggered Bidir RP Cache update
CSCei13579	Multicast	consolidation of some post-reload PIM blackhole issues
CSCsb60206	Multicast	TB@bc_odd_src_dst with CPU HOG on SSO sw/o crashes New Active RP
CSCsb61487	Multicast	(*,G) prune not processed on non-DR router
CSCsb64585	Multicast	RP is down but multicast routing continues to work
CSCsc76666	Multicast	PIM Sparses converges at <10K vs 30K+ groups (vs R2.2) on RPF change
CSCsc73288	platform-76xx	OSM asic error:SRIC packet data CRC error
CSCei76630	PPP	PP:R3:FW2+ATM:MLPPPoA+dLFI: I/O Pool MALLOCFAIL after PORT DOWN/UP
CSCsb74603	PPP	Router generated traffic does not match output policy
CSCeg31032	QoS	service-policy stops working on reload
CSCeh88604	QoS	VIP keeps crashing - with PCI DEVSEL timeout @ classify_packet
CSCej77367	QoS	RP crash at hqf_check_vc_layertype during qos testing
CSCsc35609	QoS	Crash in rvsp tail-end while shuting down egress interface on mid
CSCsc98510	QoS	Ehanced Flexwan reloads with VRF/MLPPP/QoS
CSCdv07156	Routing	rip crashes when link up/down.
CSCea34586	Routing	Bus error crash in ip_arp_merge process
CSCed67358	Routing	PIM/OSPF neighbor loss due to improper multicast MAC filter removal
CSCed87897	Routing	sh ip route missed default gateway after ip default-net command
CSCee01688	Routing	NAS crashes at ip2access_add_acl_item() while running stress test
CSCef46230	Routing	per-user ACL not removed upon call termination (regr. CSCee01688)
CSCeg12616	Routing	RIP v2 routes stuck in the RT after interface shut down.
CSCei53226	Routing	BGP: fix updgrps for non private-as peers with remove-private-as
CSCei65553	Routing	OSPF must accept LSID with a mix of 0/1s in the host portion
CSCei77396	Routing	enable ip routing causes error msg %FIB-2-IF_NUMBER_ILLEGAL: Attempt
CSCej08670	Routing	IPFAST-CFC8-2-FASTPORTOPENERR msg after switchover
CSCej21891	Routing	crash in rip_update_dbase when default-information originate used
CSCsa53394	Routing	T/B ospf_generate_trap after Trap enabled on the module
CSCsa79783	Routing	Loosing routes after reload/OIR when ispf enabled
CSCsa99924	Routing	High transient memory usage during EIGRP convergence
CSCsb09852	Routing	BGP: pathless nets not freed when updgrp members are out of sync

Identifier	Technology	Description
CSCsb24535	Routing	clear ip bgp update-group [ip address] clears all the bgp peers
CSCsb37553	Routing	IPv6 : nexthop address inaccesible after clear bgp ipv6 nei soft
CSCsb39749	Routing	router crashes upon isis removal on redundant system
CSCsb40115	Routing	BGP: Failed to find expected # of multipath entries
CSCsb44220	Routing	ipfast needs to retry openning the ipc port in the background
CSCsb59555	Routing	Line Card stuck in request reload
CSCsb74588	Routing	SUP720 crashes when OSPFv3 comes up afer neigh router SSOfailover
CSCsb79759	Routing	External LSAs are not being installed correctly
CSCsb79895	Routing	RIP protocol with MD5 authentication fails
CSCsb80866	Routing	PE global IP address shows up in traceroute VRF
CSCsb83521	Routing	%SCHED-3-STUCKMTMR - Process= IPC LC Port Opener after SSO
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
CSCuk54191	Routing	MP-iBGP routes not installed in VRF RIB
CSCee32606	Security	SSH server crashes when re-generating RSA keys
CSCsa67272	Security	Serial number in certificate subject is incorrect
CSCsc52105	Security	ipsec may leak Crypto IKMP memory blocks
CSCed34190	Unknown	Cannot configure LACP timeout (long or short)
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
CSCeg03733	Unknown	Sprious Alignment and crash with MIB walk in Cisco Class Based QoS
CSCeh17756	Unknown	ASSERT may not function properly with dual PEs and CEs
CSCeh61467	Unknown	Router crashes at pim_reset_updated_nbr on uncfging mdt group
CSCeh78028	Unknown	7600 Port-Sec: traffic fails to recover after reload
CSCei37672	Unknown	chevys/c2lc take ~ 180s before resetting following a mandatory proc exit
CSCei46182	Unknown	c6msfc2a/sup32 DEC MOP packet internally looping
CSCei49919	Unknown	WRR Queue buffer allocation does not work for Q3
CSCei60249	Unknown	VPNSM:default ip mtu sent to VPNSM must be same as IOS
CSCei72033	Unknown	1xcSTM-1 SPA goes OOS upon adding 12 serial links to MFR bundle
CSCei80006	Unknown	Same Proxy, Multiple Peers, both RRI routes deleted
CSCei80699	Unknown	multicast tunnel if_number numbers being duplicated
CSCei86256	Unknown	Crash when typing show lacp neighbors
CSCei86937	Unknown	Sup22 NDE does not export all flows
CSCei88140	Unknown	Sup32:RPR/SSO,standby crashes with exception & goes to rommon.
CSCei92291	Unknown	Message on reload:Error in setting Reload Reason
CSCej00341	Unknown	CSM Configuartion Sync timing out for large configurations
CSCej11090	Unknown	PP:R31:MSC-600/MSC-400: bogus fabric channel error counters

Identifier	Technology	Description
CSCej21515	Unknown	ATM SPA DLL tuning may miss valid lock points
CSCej21520	Unknown	ATM SPA: Removing APS on Protect interface causes locked console
CSCej21698	Unknown	EARL_L2_ASIC- SRCH_ENG_FAIL/ SCHED-DFC9-3-STILLWATCHING
CSCej22954	Unknown	fh_server.proc crash with show ev man hist events max
CSCej29710	Unknown	EEM applet SNMP notifications broken.
CSCej32688	Unknown	CSM: Problem in FT show command with gateway, config sync with more vlan
CSCej37803	Unknown	cT3 SPA:Upgrade to IOFPGA rev2.1
CSCej57810	Unknown	ifOperStatus for Control Plane Interface is always down
CSCej87462	Unknown	SNMP set not-in-service to crcERSpanIFEntry corrupts mem
CSCek03772	Unknown	zamboni: crashes for double fragmentaion
CSCin85363	Unknown	Server crashes while showing peer struct if peer struct is removed
CSCsa58710	Unknown	Supervisor Crashes with hw-module module reset
CSCsa79630	Unknown	Cat6500 Netflow does not export all flows
CSCsa80620	Unknown	ct3 spa: serial interface efc queue stuck on deleting/adding mlp bundle
CSCsa93545	Unknown	UTIL-3-TREE and L3MM-4-MN_IPDB_ADD messages and crashes in wavl and l3mm
CSCsb02848	Unknown	VPNSM does not log messages in datetime format
CSCsb18498	Unknown	SNMP polling broken in cat6k SXE1 image
CSCsb21148	Unknown	Rx SPAN may not work when outbound ACL is applied to source interface
CSCsb21941	Unknown	Supervisor reload with Large sized packet stream
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
CSCsb34983	Unknown	EEM: Trackback and software-forced crash detected
CSCsb43860	Unknown	CSM tracking interface broken when link flapping multiple times quickly
CSCsb48739	Unknown	GTP SLB:Session reassigned even when sticky entry exists
CSCsb49326	Unknown	Cat6K crashes after EPLD upgrade of WS-X6548-GE-TX
CSCsb59010	Unknown	ceExtProcessorRam implementation inconsistent between RP and LC
CSCsb60453	Unknown	Need improved logs for severe fabric errors which triggers fab swover
CSCsb62566	Unknown	Add an option to power-down the LC when fabric error is detected
CSCsb62581	Unknown	const_mpls_prog_vlan_recirc_adj msg on hw-mod reset, pkts hit CPU
CSCsb62773	Unknown	Guaranteed bandwidth not consistent with hier shaping configured
CSCsb66248	Unknown	no logging event link-status does not prevent SP to send link messages
CSCsb66799	Unknown	URL match statement removed from configuration after reload
CSCsb67152	Unknown	MET inconsistent on DFC, multicast traffic is blackholed for an OIF
CSCsb68513	Unknown	Mcast packets not always forwarded through VPNSM on 6500 with SUP720
CSCsb70335	Unknown	Flexwan crash when fragmentation is enabled under MFR interface
CSCsb70973	Unknown	igmp snooping explicit tracking and report suppression issues
CSCsb70996	Unknown	IOS SLB drops trailing fragments in VRF and misroutes SLB msgs to GGSN

Identifier	Technology	Description
CSCsb72291	Unknown	NetflowTCAM Test failed on Sup7203B with an error code 0x1
CSCsb74212	Unknown	Logical & Phy Port run Configs lost on toggling no sw / sw frm VTY
CSCsb76540	Unknown	Missing global label in TCAM if multi-paths to NH for internet access
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
CSCsb79031	Unknown	Clear counter caused the MSFC to reload the SUP due to RPC timeout
CSCsb80141	Unknown	IOS-SLB: no mls ip slb search icmp does not work.
CSCsb80590	Unknown	Enhance IPC buffer usage and IOMEM buffer allocation for Flexwan
CSCsb84405	Unknown	dscp mutation not working after reload
CSCsb84746	Unknown	Memory leak ed at qm_process_enqueue/qm_mqc_mesg_to_process
CSCsb84998	Unknown	MLS-MSC ASSERTION FAILED with T/Bs after hw-module reset
CSCsb85049	Unknown	cwpa2 bridged/routed ATM PDUs lost between Flexwan2 and SUP720
CSCsb85229	Unknown	Hierarchical classification rejected on ATM EGRESS interface
CSCsb85326	Unknown	Error Message SP: MLS-MSC ASSERTION FAILED gce->oif_count in mscdb_gce
CSCsb85589	Unknown	enable explicit-null cause ldp keeps flapping after switchover
CSCsb85748	Unknown	Attempt to open FIB Master failure warning msg occurs after SSO
CSCsb88963	Unknown	WRR queue-limit remains at 0 when WRR bandwidth set to >0 on queues 4-7
CSCsb89241	Unknown	BRE LTL is not populated properly after reload for flexwan2
CSCsb90472	Unknown	Small AToM packets from Flexwan2 dropped if forward by 6548-GE-TX
CSCsb93068	Unknown	WS-x6148-FE-SFP shows incorrect value in CISCO-STACK-MIB::PortTable
CSCsb95563	Unknown	cat6k crashes while releasing mem blocks after unconfig regd. EM Policy
CSCsb95851	Unknown	Cat6K crashing by bus error at msc_sc2vdb_unlink
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
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
CSCsc08498	Unknown	SCHED-3-THRASHING traceback from MWAM_CONSOLE Background Process
CSCsc08602	Unknown	RLB errors with code 50 and access messages without username
CSCsc09557	Unknown	Dot1x authenticated ports loosing states after SSO
CSCsc12302	Unknown	Core MTU change is not reflecting in label HW-ADJ in PE for CSC
CSCsc13720	Unknown	llq functionality with _match input vlan_ broken
CSCsc18551	Unknown	Spurious Access on OSM line card
CSCsc18707	Unknown	No error msg when event manger run nonexist policy

Identifier	Technology	Description
CSCsc18728	Unknown	Sup720 HW PAT (NAT overload) punts frames with valid MTU
CSCsc21581	Unknown	syslogED: value for built-in variable _syslog_msg is incorrect
CSCsc22043	Unknown	Event manager tcl script cannot monitor debug output on vty session
CSCsc24089	Unknown	rspan not working with sup2 and OSM gig ports
CSCsc26048	Unknown	Cat6k: CPUHOG in PIM Snooping Process
CSCsc26490	Unknown	wrong static mac address entry in case of GLBP virtual mac
CSCsc30532	Unknown	PIM snooping not populating mac-address table properly on auto rp group
CSCsc31921	Unknown	Flexwan configured for frame-relay switching causes LMI sequence reset
CSCsc32198	Unknown	IGMP per-port leave with multiple leave nested cases disturbs mcast strm
CSCsc32801	Unknown	Traceback seen after configuring 8 channel-members in etherchannel
CSCsc33110	Unknown	Sip-400 MPB: ST instance not created on SUPW when a PVC is created
CSCsc33990	Unknown	Enhancements and Optimizations to TestSPRP InbandPing
CSCsc38127	Unknown	Standby RP crash in qm_stile_adjust_sb_nbar_flags
CSCsc39939	Unknown	Cat6K : MSTI CAM table not flushed when boundary port generates TC
CSCsc44293	Unknown	Jagger failed on loopback diag.
CSCsc48986	Unknown	WS-X6148-FE-SFP boards may fail to bootup in Supervisor IOS
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
CSCsc59207	Unknown	IKE SAs not replicating to standby chassis
CSCsc59332	Unknown	CPUHOG: WS-X6748-SFP/WS-X6724-SFP with many copper SFPS installed
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.
CSCsc66102	Unknown	JAC:Minor Error on Ant48, show mod faulty, reset come online
CSCsc74828	Unknown	Rockies3.1: need diags coverage after RPR+ swover due to asic issues
CSCsc80822	Unknown	VPN-SPA - Router fails to decrypt certificate payload during IKE negotia
CSCsc85990	Unknown	EEM policy causes switch to go in tight loop and leak memory
CSCsc88725	Unknown	SPRP ping not triggering the recovery action if only one FIBTCAM device
CSCsc92114	Unknown	Port Power Mismapped On 6148-rj21AF
CSCsc93283	Unknown	R2.5: no mls qos mpls trust exp CLI not effective after reload
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
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
CSCsb86675	WAN	Multicast Packets are forwarded out on down PVC on ATM Bundle

Resolved Caveats in Release 12.2(18)SXF1

Identifier	Technology	Description
CSCeb05456	Infrastructure	nvram file locking incorrect for remote file operations
CSCsb64585	Multicast	RP is down but multicast routing continues to work
CSCsc73288	platform-76xx	OSM asic error:SRIC packet data CRC error
CSCeh88604	QoS	VIP keeps crashing - with PCI DEVSEL timeout @ classify_packet
CSCsb85748	Unknown	Attempt to open FIB Master failure warning msg occurs after SSO
CSCsb98702	Unknown	Breakpoint (signal 5 exception) when ltl profiling .
CSCsc38127	Unknown	Standby RP crash in qm_stile_adjust_sb_nbar_flags