Caveats for 12.4(15)T9 through 12.4(20)T

Resolved Caveats—Cisco IOS Release 12.4(20)T

This section describes possibly unexpected behavior by Cisco IOS Release 12.4(20)T. All the caveats listed in this section are resolved in Cisco IOS Release 12.4(20)T. This section describes severity 1 and 2 caveats and select severity 3 caveats.

Miscellaneous

- CSCdy37485

  Symptoms: Multilink PPP (MLP) fragmentation drops may occur on a Layer 2 Tunneling Protocol (L2TP) Network Server (LNS).

  Conditions: This symptom is observed when the maximum transmission unit (MTU) size that is negotiated is any other size than 1500 and Cisco Express Forwarding (CEF) is enabled.

  Workaround: Configure an MTU size of 1500 on both the client device and the LNS.

  Alternate Workaround: Disable CEF on the LNS.

- CSCee21263

  Symptoms:

  Fragmented packets might be dropped by the router.

  Conditions:

  This is observed with non-initial fragments, when a reflexive ACL is configured on the router and the return traffic supposed to be allowed by the reflexive ACL is fragmented

  Workaround:

  There is no workaround. However, normal ACLs are not known to exhibit this behavior.

- CSCeg05149

  Symptoms: After a secondary image is loaded by Standby, "NVRAM Verification Failed" messages show up on Standby console resulting in lost startup and private configuration.

Conditions: The problem is seen only on a Cisco RSP platform that is running Cisco IOS 12.2SB versions.

Workaround: Issue the **write memory** command as soon as slave comes up.

- CSCeg25475

  Symptoms: Filtering BGP routes by means of the **distribute-list prefix MARTIAN in** command applied to address-family IPv4 actually filters out M-BGP routes in address-family VPNv4.

  Conditions: This symptom occurs when MPLS-VPNs are configured.

  Workaround: Use route maps to filter routes inbound.

  Further Problem Description: The **show ip bgp neighbors** command can be used to check whether the prefixes are actually being filtered out from updates for address-family VPNv4, and not for IPv4, as it is configured.

- CSCej49366

  Symptoms: If a default metric and a redistribution metric are configured under EIGRP, the redistributed routes are sometimes removed from the EIGRP topology table. Occurs with the following configuration:

  ```
  router eigrp 1 redistribute ospf 100 metric 1544 10 255 1 1000 network 1.0.0.0 network
  4.0.0.0 default-metric 100 100 100 100 100 auto-summary eigrp event-logging
  ```

  Conditions: Occurs after the default metric statement is removed.

  Workaround: Add the default metric statement back into the configuration, or remove and re-apply the explicit redistribute statement for the donor protocol (OSPF in the above example).

- CSCek24597

  Symptoms: The BGP Support for Next-Hop Address Tracking feature fails.

  Conditions: This symptom is observed when the BGP Event Process is terminated after BGP has been up.

  Workaround: There is no workaround.

- CSCek37011

  Symptoms: A line card may crash when you attempt to remove the child policy from the HQoS parent.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router when the line card has an interface that is configured as follows:

  - The interface faces the MPLS core.

  - The interface has an HQoS policy with a child policy.

  - The HQoS policy has a classification that is based on the MPLS EXP bits.

  Workaround: There is no workaround.

- CSCek63963

  Symptoms: Router crashes with a traceback decode showing a divide by 0 error.

  Conditions: Occurs when a rate-based event is configured for a counter that has a value of 0, such as the following scenario:

  1. The customer must be using a Cisco IOS Embedded Event Manager (EEM) rate-based Interface Event Detector (either applet or Tcl script). Rate-based means use of the "rate" keyword in the event specification statement.

2. The rate calculation is attempted after the counters are cleared and before any samples have been taken.

Workaround: There is no workaround.

- CSCek75558

  Symptoms: When hardware compression is enabled and an MQC policy is used on an FR PVC, the shaper drops all packets after passing a few.

  Conditions: This symptom is observed with normal traffic flow through the interface.

  Workaround: Replace MQC shaping with FRTS and configure the shape rates in the map class. If LLQ is not required on the PVC, another option is to use software compression instead of hardware compression.

- CSCek75931

  Symptoms: A Cisco 10000 series router may experience a CPUHOG condition.

  Conditions: This condition is observed when there is an increase of more than 2000 sessions established.

  Workaround: There is no workaround.

- CSCek76323

  Symptoms: L2TP Ascend Disconnect code 63 is not found on a LAC.

  Conditions: This symptom is observed in a Cisco IOS Release 12.4(17.9)T image.

  Workaround: There is no workaround.

- CSCek77264

  Symptoms: A spurious access error occurs after configuring the **tms-class** command. This command is used when configuring the Threat Information Distribution Protocol (TIDP).

  Conditions: The error is found on the Cisco 7200 router in Cisco IOS Release 12.4(13.13)T4.

  Workaround: Configure with a short name with the **tms-class** command.

- CSCek78237

  Symptoms: A short CPU hog seen in the ATM PA Helper process when an interface flaps and the framing configuration is modified on the interface.

  Conditions: This symptom is observed on a Cisco 7200 with a PA-A3-T3 adapter that is running Cisco IOS Release 12.2(25)S or 12.2(31)SB (and possibly other Cisco IOS releases).

  Workaround: There is no workaround.

  Further Problem Description: The CPU hog is enough to cause OSPF adjacencies (with fast hello) to go down on other unrelated interfaces. The same problem is seen if BFD is configured.

- CSCek79311

  Symptoms: Under stress conditions, an L2TP multihop node may crash.

  Conditions: This symptom is observed when a session is being disconnected.

  Workaround: There is no workaround.

- CSCek79614

  Symptoms: An HTTP client cache entry is not updated.

  Conditions: This symptom is observed when VXML application scripts do not specify the "maxage" attribute. The cached entries in the HTTP client are not refreshed until they expire. If any of the files are modified on the HTTP server, you must perform one of the workarounds below.

Workaround: Choose one of the following options:

1) Change the "maxage" attribute of the VXML application scripts. 2) Reload the router. 3) Use the **audio-prompt load** *url* command on the router console for each file that needs to be refreshed.

- CSCsa65314

  Symptoms: Inbound calls on an MGCP-controlled CAS trunk may experience symptoms where the call does not complete and the calling party hears dead air. When this occurs, it will be experienced at that particular timeslot on the digital trunk until some manual intervention is taken to correct this.

  Conditions: This symptom has been observed at times on Cisco IOS VoIP gateways with CAS trunks configured from MGCP back to Cisco Unified CallManager (CUCM/CCM). An inbound call on a timeslot that is in this state will show the VTSP state in the **show voice call summary** command output as S_DIGIT_COLLECT and will not progress past this point.

  Once source of this issue has been when the status of the timeslot on the CallManager and the gateway is not the same. For example, the CallManager may indicate that the channel is out of service (OOS) while the gateway has the status of this timeslot as in-service (idle). Please refer to CSCef58219, which has seen to lead to this state. If this issue is being seen because of this difference in status between the CallManager and the Cisco IOS gateway, the recommended action is to upgrade the CallManager with a release that contains the fix for CSCef58219.

  Workaround: The only known workaround to prevent this issue from occurring is to use H.323 instead of MGCP with CAS trunks.

  Once in this state, to recover the timeslots you can:

  1. Enter the **shutdown** command and the **no shutdown** command on the voice port. 2. When there are multiple channels stuck, enter the **no mgcp** command and then the **mgcp** command.

- CSCsa73179

  Symptoms: Memory corruption, possibly leading to a crash or other undesired behavior, can occur when the **no default-information originate** command is entered in router RIP configuration mode.

  Conditions: This symptom occurs only if both the RIP routing protocol and the OSPF routing protocol are configured on a router.

  Workaround: There is no workaround.

- CSCsa76212

  Symptoms: Group Manager or Alternate may reload if compactflash is re- inserted into the disk0: slot too quickly after extraction.

  Conditions: This symptom is observed when Group Manager and Alternate are both up and in their respective active states.

  Workaround: After extracting compactflash from the disk0: slot, wait 30 to 60 seconds before re-inserting disk.

- CSCsb84050

  Symptoms: Cisco IOS authentication proxy does not work when both HTTP and HTTPS servers are enabled.

  Conditions: Occurs only when the HTTPS server is enabled in parallel with the HTTP server.

  Workaround: Disable the HTTPS server on the router.

- CSCsb96034

  Symptoms: Routes redistributed from other routing protocols to BGP will be deleted and re-added after an NSF switchover, potentially causing traffic to go down for a long period of time.

Conditions: This symptom may occur when the route is redistributed from other routing protocols (such as OSPF, ISIS, EIGRP) to BGP.

Workaround: There is no workaround.

- CSCsc72722

  Symptoms: TCP connections that are opened through a Cisco IOS Firewall (CBAC) may not timeout.

  Conditions: With Cisco IOS Firewall (CBAC) enabled, the TCP idle timer for a session may be reset even by TCP packets that fail TCP inspection and are subsequently dropped. This could lead to the TCP session not timing out.

  Workaround: There is no workaround.

- CSCsd10762

  Symptoms: The following traceback appears:

  FIB-4-FIBNULLIDB: Missing idb for fibidb Virtual4 (if_number 54).

  Conditions: This symptom is observed when a router is reloaded.

  Workaround: There is no workaround.

- CSCsd73881

  Symptoms: A router may reload.

  Conditions: This symptom is observed if a client uses a very big name for the SVC and uses the **test pasvc** command.

  Workaround: There is no workaround.

- CSCsd82457

  Symptoms: The EapOverUDP protocol cannot detect Cisco IP conference stations and wireless phones, resulting in the policy configured locally on the box for IP phones not being applied.

  Conditions: This symptom is observed with a normal EapOverUDP configuration that is used for applying the NAC policies for IP phones.

  Workaround: There is no workaround.

- CSCse03637

  Symptoms: PIM dense mode interoperability issues are seen with Cisco and third party boxes.

  Condition: This symptom is observed when PIM dense mode is in operation. After the multicast forwarder is decided, based on the assert mechanism, a prune is erroneously sent. Multicast stream ceases to flow.

  Workaround: There is no workaround.

- CSCse61834

  Symptoms: When you modify an ATM PVC by entering the **pvc** *vpi/vci* command, any subsequent modifications in the VC class that is assigned to this PVC do not take effect.

  Conditions: This symptom is observed when the PVC is preconfigured with a VC class when the following events occur:

  1) You make a configuration change in the PVC.

  2) You change the configuration in the VC class.

  The configuration change in the VC class does not take effect.

Workaround: First complete the configuration changes in the VC class. Then, change the configuration in the PVC.

- CSCse85151

  Symptoms: Cisco Catalyst 4500 Supervisors and the Cisco Catalyst 4948 that are running Cisco IOS Release 12.2(31)SG crash.

  Conditions: This symptom occurs when one of the following commands is issued:

  - **show buffers all** - **show buffers assigned** - **show buffers input-interface**

  Workaround: Do not use any of the above commands. For troubleshooting high CPU issues, use the steps indicated in the following tech tip instead:

  http://www.cisco.com/warp/public/473/cat4500_high_cpu.html

- CSCse90294

  Symptoms: In the **connect** command, the ATM option is either coming twice or not coming at all in different platforms.

  Condition: When local switching related command is "connect" is configured.

  Workaround: There is no workaround.

- CSCse90710

  Symptoms: A Versatile Interface Processor (VIP) may crash while configuring T1 or E1.

  Conditions: This symptom is observed with a VIP in which a PA-MC-8T1E1 port adapter is installed that is configured with either a T1 or an E1 controller.

  Workaround: There is no workaround.

- CSCse90875

  Symptoms: GRE traffic is not controlled by an [arbitrary-zone]-to-self-zone policy.

  Conditions: A zone-based policy firewall is configured on a router. The zone policy limits connectivity from specific zones to the self zone so only certain GRE traffic is allowed to reach the router's IP addresses.

  Workaround: Apply interface ACLs to limit GRE traffic to and from the router's IP addresses. Remember to append a "permit any any" statement after denying unwanted traffic. If "permit any any" is not added at the end of the interface ACLs, the ACLs may conflict with Zone Policy Firewall configuration.

- CSCsf01190

  Symptoms: The **export destination** command disappears from the running configuration.

  Conditions: This symptom is observed under very specific circumstances. VRFs must be configured for the same destination as that configured for exporting. If these VRFs are deleted, for example with the **no ip vrf** command, the export destination is also deleted, leaving the code in a state in which the export destination will vanish from the running configuration.

  (The fix checks whether any destinations are configured in the deleted VRF, and if yes, the loop that would overwrite this destination is simply exited).

  Workaround: Do not delete VRFs when NetFlow is configured.

  Alternate workaround: If you do delete VRFs, readd NetFlow export configuration via the CLI.

- CSCsf11944

  Symptoms: A router crashes due to the stack for process Exec running low when configuring the **auto qos** command on an ATM subinterface.

Conditions: The symptom has been observed on a Cisco router loaded with Cisco IOS interim Release 12.4(10.5).

Workaround: There is no workaround.

- CSCsf32449

  Symptoms: A Sup720 Multicast-VPN (MVPN) PE router may not advertise its mdt prefix (BGP vpnv4 RD-type 2) after reloading.

  Conditions: This symptom is observed on a Sup720 MVPN PE router.

  Workaround: Use the **clear ip bgp** command after reloading.

- CSCsg04630

  Symptoms: Crash is seen on Standby Route Processor.

  Conditions: The crash is normally seen in case of unnumbered relay, when Standby Relay gets synced from Active Relay. The crash is showing some data inconsistency issue while the Standby Relay gets synced.

  Workaround: There is no workaround.

- CSCsg18894

  Symptoms: When you attempt to change or overwrite the **priority** command for a MQC priority queue, the command is rejected and the following error message is generated:

  priority not allowed in conjunction with queue-limit

  Conditions: This symptom is observed on a Cisco router that has the **queue-limit** command enabled in a MQC priority queue.

  Workaround: Remove the **queue-limit** command, modify the **priority** command, and then re-enter the **queue-limit** command.

- CSCsg25995

  Symptoms: Networks do not show up in the BGP table for multicast address family, as can be seen in the output of the **show ip mbgp** command.

  Conditions: This symptom is observed when BGP is used for multicast address family; it does not affect unicast address family.

  Workaround: Use the **clear ip bgp** *neighbor-address* command.

- CSCsg39295

  Symptoms: Password information may be displayed in a syslog message as follows:

  %SYS-5-CONFIG_I: Configured from scp://userid:password@10.1.1.1/config.txt by console

  Conditions: This symptom is observed when using SNMP to modify a configuration by means of the CISCO-CONFIG-COPY-MIB; selection of ConfigCopyProtocol of SCP or FTP may result in the password being exposed in a syslog message.

  Workaround: When using SNMP to modify a configuration by means of the CISCO-CONFIG-COPY-MIB, use the ConfigCopyProtocol of RCP to avoid exposure of the password.

- CSCsg43751

  Symptoms: A router crashes when HDLC encapsulation is configured on a dialer interface with profile configuration.

  Conditions: This symptom is observed with CEF switching when a dialer interface is configured with HDLC encapsulation.

Workaround: Use PPP encapsulation on the dialer interface so that CEF switching works fine and the router does not crash.

- CSCsg49810

  Symptoms: Power fluctuation causes the Cisco VG224 to go into ROMMON mode.

  Conditions: This symptom occurs while the Cisco VG224 is booting up. If the power is switched off after the initial boot message and then switched back on, the router goes into ROMMON mode.

  The power off/on simulates possible power flaps.

  Workaround: There is no workaround. Avoid cycling the power during bootup.

- CSCsg64163

  Symptoms: Cisco IOS software does not handle packet fragments for port-specific NAT rules such as:

  ```
  ip nat inside source static udp 192.168.21.2 500 interface FastEthernet0/0 500 ip nat
  inside source static udp 192.168.21.2 4500 interface FastEthernet0/0 4500
  ```

  Only the first fragment is being translated; others are not. This symptom remains even if the **ip virtual-reassembly** command is active on interfaces.

  Conditions: This symptom has been observed in Cisco IOS Release 12.4 and Release 12.4T.

  Workaround: There is no workaround.

- CSCsg64586

  Symptoms: A router log contains the following error message and its performance becomes severely degraded:

  %SYS-3-CPUHOG: Task is running for (2004)msecs, more than (2000)msecs (4/3),process = DNS Server.

  Conditions: This symptom is observed on a Cisco router that performs many DNS lookups.

  Trigger: Lots of DNS lookups but may also occur otherwise.

  Impact: Performance impacting bug.

  Workaround: Configure the router in such as way to prevent it from performing many DNS lookups, and do not configure the router as a DNS server for other devices.

  Further Problem Description: Note that CSCsg64586 can produce very similar symptoms, even in the absence of a large number of DNS queries.

- CSCsg91306

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS that can be exploited remotely to trigger a memory leak or to cause a reload of the Cisco IOS device.

  Cisco has released free software updates that address these vulnerabilities. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities addressed 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, if administrators do not require the Cisco IOS device to provide voice over IP services.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080924-sip.shtml.

- CSCsg95896

  Symptoms: A string gets appended to the calling station ID.

Conditions: This symptom is observed when the calling station ID is configured on the RADIUS server.

Workaround: There is no workaround.

- CSCsh12294

  Symptoms: The voice path between already connected secure analog VG224 phones is broken when a new call is made to one of the party.

  Conditions: PhoneA calls PhoneB. PhoneA and PhoneB are connected, and the voice path confirmation is established. PhoneC calls PhoneB. Once PhoneB hears the call-waiting tone, the voice path from PhoneB to PhoneA is lost. But when PhoneA talks, PhoneB can hear it.

  Workaround: The only workaround is to block call-waiting or use non-secure phones.

  Further Problem Description: This symptom occurs only when both the analog phones are secure endpoints. Non-secure phones work fine.

- CSCsh12493

  Symptoms: After addition/deletion/modification of a VRF and the re-addition of associated configuration, it becomes apparent that the RIB is not being updated by BGP after reconvergence, and LDP neighborship is reestablished. As the RIB is not updated, neither is CEF. While BGP VPNv4 has the correct information, the RIB is empty of remote PE VRF subnets, and CEF has a default entry.

  Conditions: This symptom is observed on Cisco 12000 series router.

  Workaround: Clear the BGP session.

- CSCsh22725

  Symptoms: Outbound calls fail on a MGCP-controlled CAS channel on a Cisco VoIP gateway.

  Conditions: This symptom is observed when the following conditions occur:

  - A timeslot on an E&M T1 trunk is taken out of service from the connected switch side, showing as a permanent inbound seizure. In this situation, the output of the **show voice call summary** command indicates that the status for this channel is "EM_PARK".

  - A Cisco CallManager that interworks with the Cisco VoIP gateway checks the status of the trunk via an MGCP AUEP command. The gateway responds with an "ES: rlc" message, which indicates that the trunk is available for calls.

  Because the reported availability and actual availability of the channel are mismatched, all outbound calls on the channel fail.

  Workaround: Attempt to clear the out-of-service state from the connected switch side. If this is not possible, when interworking with the Cisco CallManager, first enter the **shutdown** command followed by the **no shutdown** command on the voice port and then enter the same commands on the T1 controller. Doing so causes the gateway to send an NTFY message that indicates that there is an inbound seizure on the channel.

- CSCsh46433

  Symptoms: Configuring the **ip nbar custom** global configuration command results in irrelevant **show running- config** output. The following **show running- config** output is seen when the **ip nbar custom** command is either configured or unconfigured, and the same output continues to be added to the running config each time the command is executed.

  ```
  no ip port-map gnutella port tcp 6346 6347 6348 6349 description Gnutella Version2
  Traffic - BearShare, S no ip port-map bittorrent port tcp 6881 6882 6883 6884
  description bittorrent no ip port-map bittorrent port tcp 6885 6886 6887 6888
  description bittorrent
  ```

Conditions: This symptom is observed only with protocols that have more than four ports like bittorrent and gnutella.

Workaround: There is no workaround.

Further Problem Description: Other than cluttering the running config, this bug does not have any other side effect.

- CSCsh47251

  Symptoms: A Cisco 3700 or 3800 series router crashes on bootup.

  Conditions: The crash happens only when two conditions are satisfied:

  1) An NM-xDM card is present in the box. 2) An external compact flash is present (inserted) in the box.

  Workaround: Remove the external compact flash before booting the router.

- CSCsh54797

  Symptoms: High CPU utilization occurs.

  Conditions: This issue occurs with PPPoE sessions. When bringing up 24,000 sessions at a rate of 15/sec, the CPU is around 45 percent. When clearing all 24,000 sessions and bringing them up again, the collection process suddenly is manifesting itself by generating a high CPU: it is taking up 50 percent of all the CPU. This issue is seen on the Cisco 10000 platform but may affect other platform also. This will likely happen all the time. This issue may cause operational impact due to high CPU utilization.

  Workaround: There is no workaround. Issue the **show proc cpu** command to see the CPU utilization.

- CSCsh75224

  Symptoms: An RP crashes in IFS code when an SSH or Telnet session is established while the switch is attempting to download a configuration.

  Conditions: This symptom occurs on a Cisco Catalyst 6509.

  Workaround: There is no workaround.

- CSCsh79893

  Symptoms: A Cisco 2800 router running zone-based firewall and URL filtering may reload.

  Conditions: Occurs when URL filtering is unconfigured or reconfigured under the policy map during periods of high traffic.

  Workaround: There is no workaround.

- CSCsh86354

  Symptoms: Cisco MWAM processor reloads when all the VTY lines are used up and command is executed on the Supervisor remotely using the Remote Console and Logging feature of the MWAM. The output of the command is not displayed on the Supervisor console. Instead it is printed on the MWAM processor console and after the display is finished, the MWAM processor reloads.

  Conditions: This problem happens when all the VTY lines are in use. If only a few are in use, then the Remote Console and Logging feature works fine and the output is displayed on the Supervisor console as expected.

  Workaround: Currently there is no workaround for this problem. If there are enough VTY lines supported, the chance of encountering this issue is low.

- CSCsh91974

  Symptoms: The Route Processor (RP) crashes.

Conditions: Some of the Protocol Independent Multicast (PIM) CLI commands are causing the active RP to crash. The crash happens *only* when these commands are configured while in control-plane policing subconfiguration mode. Normally, any global relevant configuration should automatically exit the subconfiguration prompt and also accept the command. In this case, the PIM command is rejected and the RP crashes. The same PIM commands work fine when entered under global configuration mode (where they belong) or under other subconfiguration modes.

Workaround: Use the **exit** command to exit the main configuration prompt before configuring PIM-related commands.

- CSCsi07822

  Symptoms: When using the IPv6 VPN over MPLS (6VPE) capability and eBGP multihop, where loadsharing is being done on the VRF, if one of the loadsharing paths on the PE is flapped, loadsharing across the appropriate paths may no longer occur. This is because the RIB is unable to resolve the route to the next-hop via the flapped interface.

  Conditions: Assuming that we have the topology below and that eBGP multihop loadsharing is being done by PE1:

  a1/0.1 a3/0/0.1 +----------+ CE1----------PE1----- 4000:B::/60 a2/1.1 VPN1050 a3/0/1.1

  332:332:332::332/128 444:444:444::444/128

  eBGP Multihop session between PE1 & CE1 via loopback addresses 444:444:444::444/128 & 332:332:332.332/128 respectively

  ################################## Loadsharing before the interface flap ################################## PE1#sh bgp vpnv6 unicast vrf VPN1050 4000:B:0:270::/60 BGP routing table entry for [1050:1]4000:B:0:270::/60, version 3760 Paths: (1 available, best #1, table VPN1050) Advertised to update-groups: 1 3510 102 332:332:332::332 (FE80::217:95FF:FEE4:1A90) from 332:332:332::332 (10.1.1.32) Origin IGP, localpref 100, valid, external, best Extended Community: RT:1050:1 mpls labels in/out 13509/nolabel PE1# PE1#sh ipv6 route vrf VPN1050 4000:B:0:270::/60 Routing entry for 4000:B:0:270::/60 Known via "bgp 6777", distance 20, metric 0, type external Route count is 1/1, share count 0 Routing paths: 332:332:332::332 Last updated 02:17:03 ago

  PE1#

  Let's look at RIB for the next-hop; we should see both paths. ################################## PE1#show ipv6 route vrf VPN1050 332:332:332::332 Routing entry for 332:332:332::332/128 Known via "static", distance 1, metric 0 Redistributing via bgp 6777 Route count is 2/2, share count 0 Routing paths: 2004:1000:9250:A910::2 Last updated 00:48:21 ago 2006:106:106:2006::2 Last updated 00:00:20 ago

  ############################### CEF looks good as shown below ############################### PE1#show ipv6 cef vrf VPN1050 4000:B:0:270::/60 detail 4000:B:0:270::/60, epoch 24 local label info: other/13509 recursive via 332:332:332::332 recursive via 2004:1000:9250:A910::2 recursive via 2004:1000:9250:A910::/64 attached to ATM3/0/0.1 recursive via 2006:106:106:2006::2 recursive via 2006:106:106:2006::/64 attached to ATM3/0/1.1 PE1#

  Now shut down one of the interfaces on PE1.

  PE1(config)#int a3/0/1 PE1(config-if)#sh PE1(config-if)#end PE1#

CEF now has only one recursive output chain to the destination after the interface is shut down. Good. ## PE1#show ipv6 cef vrf VPN1050 4000:B:0:270::/60 detail 4000:B:0:270::/60, epoch 24 local label info: other/13509 recursive via 332:332:332::332 recursive via 2004:1000:9250:A910::2 recursive via 2004:1000:9250:A910::/64 attached to ATM3/0/0.1 PE1#

Now bring back up the a3/0/1 interface and observe CEF. ## PE1#conf t Enter configuration commands, one per line. End with CNTL/Z. PE2(config)#int a3/0/1 PE2(config-if)#no sh PE2(config-if)#end PE1#

Let's see if RIB and CEF have resolved the next-hop via this interface. They have not as demonstrated below. ## PE1#show ipv6 route vrf VPN1050 332:332:332::332 Routing entry for 332:332:332::332/128 Known via "static", distance 1, metric 0 Redistributing via bgp 6777 Route count is 1/1, share count 0 Routing paths: 2004:1000:9250:A910::2 Last updated 00:56:35 ago

PE1#show ipv6 cef vrf VPN1050 332:332:332::332/128 detail 332:332:332::332/128, epoch 24 local label info: other/3305 1 IPL source [no flags] Dependent covered prefix type inherit cover NULL recursive via 2004:1000:9250:A910::2 recursive via 2004:1000:9250:A910::/64 attached to ATM3/0/0.1 PE1#

Workaround: Toggle the associated CE interface a few times.

- CSCsi09549

  Symptoms: CPU HOG messages are displayed, and phones are deregistered.

  Conditions: This symptom is observed very rarely when MoH is configured to be played from flash. Specifically, this symptom is observed under either of the following two conditions:

  1. When polling ciscoFlashMIB. 2. When playing MoH for more than 30 minutes and also *once* during a h/w conference.

  Workaround: The system will recover by itself after some time. Formatting flash: will also solve the issue temporarily.

- CSCsi17020

  A series of segmented Skinny Call Control Protocol (SCCP) messages may cause a Cisco IOS device that is configured with the Network Address Translation (NAT) SCCP Fragmentation Support feature to reload.

  Cisco has released free software updates that address this vulnerability. A workaround that mitigates this vulnerability is available.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080924-sccp.shtml.

- CSCsi21389

  Symptoms: Routers that have the ability to use the optional 802.11 b/g card, such as the Cisco ISR series routers, do not pass multicast traffic across the wireless interface.

  Conditions: Cisco routers that have the 802.11 b/g HWIC card do not pass multicast traffic across the wireless interface, even though multicast routing is enabled and is otherwise configured normally. Wireless hosts cannot pass multicast traffic between each other, and multicast traffic from the wired network will not be transmitted out the wireless interface.

  Workaround: There is no workaround.

- CSCsi33626

Symptoms: One may intermittently see a traceback from the Transport Port Agent because of timing of subsystem initialization in the router. The traceback is nonimpacting to the actual functional performance of the router.

Conditions: This symptom is observed at bootup.

Workaround: There is no workaround.

- CSCsi44914

  Symptoms: Configuring IDS monitoring on a router that terminates a Frame Relay TCP header compression link will block all TCP traffic over the TCP header-compressed link that does not terminate on the router.

  Also, configuring IDS monitoring on a next-hop link for TCP traffic that passes through the TCP header-compressed link will cause all TCP connections that pass through the header-compressed link and the next-hop interface to be dropped.

  Conditions: In a topology in which you want to run Frame Relay with header compression on a serial link, you cannot pass Telnet traffic through a router on one end of that link if it has an IDS sensor running in inline monitoring mode. Using inline mode will limit you to establishing a Telnet connection only as far as that router; any hops beyond that will fail and cause the IDS sensor to start denying all traffic that is passing through it, which you can only fix by reloading the router. This problem occurs regardless of the interface on which the IDS sensor is attached and the direction of the traffic. However, this functionality affects only inline monitoring mode; switching to promiscuous mode will allow you to successfully establish Telnet connections beyond the router on which the IDS module is installed.

  Workaround: Do not configure TCP header compression with the AIM-IPS-K9 installed.

- CSCsi46897

  Symptoms: PPP may crash when an **snmpwalk** command is executed on the cbQosSetStatsTable object.

  Conditions: This symptom is observed when a service policy with a child policy that contains marking ("set") actions is applied to an interface before the **snmpwalk** command is executed on the cbQosSetStatsTable object of the CISCO-CLASS-BASED-QOS-MIB.

  Workaround: There is no workaround.

- CSCsi51014

  Symptoms: Disk access causes router to crash.

  Conditions: Occurs after **fsck** execution.

  Workaround: Format disk, which causes the data loss on the affected disk.

- CSCsi53469

  Symptoms: A router may hang for approximately 7 minutes.

  Conditions: This symptom is observed when you attempt to configure the **range pvc** command in a manner that exceeds the interface limit.

  Workaround: There is no workaround.

- CSCsi57927

  Symptoms: A Cisco router that is running Cisco IOS Release 12.2, Release 12.3, or Release 12.4 will show TCP connections that are hung in CLOSEWAIT state. These connections will not time out, and if enough accumulate, the router will become unresponsive and need to be reloaded.

Conditions: This symptom occurs on a Cisco router that is running Cisco IOS Release 12.2, Release 12.3, or Release 12.4 when a **copy** *source-url* **ftp:** command is executed and the FTP server fails to initiate the FTP layer (no banner) but does set up a TCP connection. This may occur when the FTP server is misconfigured or overloaded.

The CLI command will time out, but will not close the TCP connection or clean up associated resources. The FTP server will eventually answer and time itself out, and close the TCP connection, but the router will not clean up the TCP resources at this time.

Workaround: Manually clear TCP resources using the **clear tcp** command, referencing the **show tcp brief** command output.

- CSCsi61711

  Symptoms: A router experiences tracebacks when a client attempts to send e-mail.

  Conditions: This symptom is observed on a Cisco 1800 router that is running Cisco IOS Release 12.4(11)T2 and that is configured as an Enterprise Class Teleworker (ECT) spoke.

  Workaround: Enable "Inspect TCP" instead of SMTP.

- CSCsi63470

  Symptoms: Device crashes.

  Conditions: Occurs following online insertion and removal (OIR) of PA-POS-1OC3.

  Workaround: Power down the router before removing the card.

- CSCsi68963

  Symptoms: A Cisco 7200P router crashes while removing an IPv6 Protocol Independent Multicast (PIM) bootstrap router (BSR) candidate from the configuration.

  Conditions: This symptom is observed when the IPv6 PIM BSR candidate is unconfigured.

  Workaround: There is no workaround.

  Further Problem Description: After RP information is learned on all of the routers, delete the ACL first and then the BSR candidate.

- CSCsi69938

  Symptoms: The serial interface line protocol on HWIC-2AS, HWIC-1T, and HWIC-2T is flapping in sync mode (and generating the CRC errors).

  Conditions: This symptom is observed when any of the above cards is connected and a transition happens from async mode to sync mode.

  Workaround: There is no workaround.

  Further Problem Description:

  Setup:

  Serial -2A/S (0/2/1)==========Serial 2A/S (0/0/1)

  Steps:

  1) Two serial 2A/S cards are connected back to back using a V.35 cable as shown in the setup above. 2) The HWIC cards are in SYNC mode, and the encapsulation is HDLC. 3) The basic configuration of IP address and clockrate is done. 4) Both interface protocols are up and can ping each other. 5) The configuration is saved on both routers, and the Cisco 3825 is reloaded. 6) After reloading, the protocol is down at interface 0/0/1 of the Cisco 3825, and the protocol is up/down (flapping) continuously on interface 0/2/1 of the Cisco 2811.

```
*Apr 27 06:59:45.467: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/1,
changed state to down *Apr 27 06:59:55.467: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Serial0/2/1, changed state to up
```

Errors are increasing on the Cisco 3825. Please find details in the errors attachment:

148 input errors, 148 CRC, 105 frame, 56 overrun, 0 ignored, 96 abort

- CSCsi70787

  Symptoms: A router may reset and generate a crashinfo file when memory that was allocated by a dead process is freed by another process.

  Conditions: This symptom is observed on an RPM-XF-512 that runs Cisco IOS Release 12.4T but is not platform-specific.

  Workaround: There is no workaround.

- CSCsi72045

  Symptoms: A bus error crash occurs on a Cisco router.

  Conditions: This symptom is seen when AAA and PPPoE are configured.

  Workaround: There is no workaround.

- CSCsi77147

  Symptoms: DTMF path confirmation is not received for a SIP call.

  Conditions: This problem is due to an issue with the SIP state machine, which may result in an error along the lines of the following:

  ```
  00:05:10: //-1/xxxxxxxxxxxx/SIP/Error/sipSPISipIncomingMsg: Invalid method for
  (STATE_IDLE): ACK
  ```

  The call state should not be IDLE.

  Workaround: There is no workaround.

- CSCsi78783

  Symptoms: Router crashes when **auto qos voip** is configured on ATM-PVCs. It does not crash when **auto qos voip trust** or **auto qos voip** are configured on any interface.

  Conditions: Occurs when **auto qos voip** is configured the first time on any ATM-PVC.

  Workaround: Configure **auto qos voip** on any interface, such as a serial interface, and then configure **auto qos voip** on the ATM-PVC. Use **auto qos voip trust** if it is suitable for the network.

  Further Problem Description: If **auto qos** exists in the startup configuration then the issue is not seen. It is seen only when it is configured on a ATM interface of a router which is up and running.

- CSCsi80057

  Symptoms: Conditional default origination into RIPv2 does not work correctly in the following scenarios:

  1. When the watched network is not present, the default route is not deleted from the local RIP database. This causes the router to still send the default route.

  2. When the watched network is present, the default route is not added to the local RIP database. This causes the router to not send the default route.

  The default behavior can be seen at the following link:

  http://www.cisco.com/en/US/docs/ios/iproute/command/reference/irp_rip.html#wp1011008

  Conditions: This symptom is observed if the **default-information originate route-map** *map-name* router RIP configuration command is used in order to generate a default route only when the watched network is present.

Workaround: There is no workaround.

- CSCsi81891

  Symptoms: RTP packets get transmitted when the mode is recvOnly and inactive.

  Conditions: This problem is observed on both the Cisco 2800 and the Cisco 3800 platforms that are running Cisco IOS interim Release 12.4(13.9).

  Workaround: There is no workaround.

- CSCsi83952

  Symptoms: The **show isdn service** command shows b_channels of interface configured for primary ss7-nfas as out of service.

  Conditions: This symptom is observed on Cisco 5400 or 5850 platforms for a controller configured for ss7-nfas.

  Workaround: There is no workaround.

- CSCsi86823

  Symptoms: An incorrect NAS port ID is found while testing IDBless VLAN for PPPoE.

  Conditions: The symptom is observed on a Cisco 7200 router.

  Workaround: There is no workaround.

- CSCsi89511

  Symptoms: With IKE accounting enabled, memory leaks are found when IKE sessions are terminated abnormally.

  Conditions: This symptom is observed only when IKE sessions are terminated abnormally (for example, by removing a crypto map from the interface).

  Workaround: There is no workaround.

  Further Problem Description: The leak is caused by "uncommon" termination of IKE sessions. Basically, there are two code paths to clean up the (IKE) accounting data structure. One (1) does a good job of freeing everything and can be taken most of the time in a normal call's setup/teardown sequence (for example, IPsec tunnel and IKE are both brought down in sequence). The second one (2) is taken due to a racing condition of termination causes which the IKE peer gets notified first and cleans its accounting structure (partially). It might be said that the leak is "slow" as the second path is not regularly taken. It does not affect the actual functionality.

- CSCsi93916

  Symptoms: An alignment error (i.e., spurious memory access) that causes tracebacks such as "ipnat_nbss_is_special_packet" may be observed on a Cisco router.

  Conditions: The symptoms are observed with a certain packet format, not yet identified. It is specific to the NetBios Session Service (NBSS) protocol.

  Workaround: There is no workaround.

- CSCsi95862

  Symptoms: Router crashes when the **mobile router-service roam priority** command is entered.

  Conditions: Crash is observed during unconfiguration after verifying for generic routing encapsulation.

  Workaround: There is no workaround.

- CSCsi97649

Symptoms: A Cisco 7200 LAC and a Cisco 7300 LNS router crash when approximately 2100 sessions have connected.

Conditions: This symptom is observed when bulk PPPoE sessions are sent on the router.

Workaround: There is no workaround.

- CSCsi98120

  Symptoms: A router may crash because of a bus error. Spurious accesses may be observed.

  Conditions: This symptom is observed on a Cisco 7200 series router that has an NPE-G1. The router is configured as a PE router and uses MQC hierarchical policies for some subinterfaces and the legacy **rate-limit** command for other subinterfaces.

  Workaround: There is no workaround.

- CSCsi98730

  Symptoms: The MPLS labels for packets that are forwarded via CEF and MPLS over a BGP route may not match the labels in the BGP table, which may lead to traffic loss.

  Conditions: This problem occurs under certain circumstances and timing conditions.

  Workaround: When the symptom occurs, enter the **clear ip route** command for the prefix in the VRF.

- CSCsj07189

  Symptoms: Entering the **snmpget** of an object identifier (OID) using the interface index (ifIndex) value of an interface for its index will result in an error:

  ```
  snmpget -c <community> -v1 <device> IF-MIB::ifDescr.92
  Error in packet Reason: (noSuchName) There is no such variable name in this MIB.
  Failed object: IF-MIB::ifDescr.92
  ```

  Conditions: This can occur after port adapters (PA) have been swapped, such as replacing a 4-port PA with an 8-port PA.

  Workaround: Use the **snmpwalk** to retrieve the IF-MIB values.

- CSCsj07297

  Symptoms: Config sync is seen with Cisco 7600 HA routers.

  Conditions: This symptom is observed when the **no vrrp 1 preempt** interface configuration command is configured and when a switchover is done from primary to secondary.

  Workaround: There is no workaround.

- CSCsj09838

  Symptoms: When the BGP session between a Route Reflector (RR) and PE router flaps, the RR may no longer send some routes to the PE router.

  Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software image that integrates the fix for caveat CSCsi85222. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsi85222. Cisco IOS software releases that are not listed in the "First Fixed-in Version" field at this location are not affected.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, enter the **clear ip bgp * all in** command on the PE router to retrieve all routes from the RR.

- CSCsj12867

  Symptoms: The following message can be seen after executing the **write memory** command, even though the version has not been changed.

```
Router# write memory
Warning: Attempting to overwrite an NVRAM configuration previously written by a
different version of the system image. Overwrite the previous NVRAM
configuration?[confirm]
The router then restarts with the following traceback:
-Traceback= 6067F3DC 6067FB38 605E3FE8 60686384 605E3FE8 605188BC 60518830 605444D4
60539164 6054719C 605AB65C 605AB648
```

Conditions: This symptom is observed on a Cisco 7206 VXR (NPE-400) with C7200-IO-FE-MII/RJ45= or C7200-I/O=.

Workaround: There is no workaround.

- CSCsj13347

  Symptoms: Executing the **clear crypto sa** command.

  Conditions: The problem is that the **clear crypto sa** and the **clear crypto isakmp** commands are usually used, but these commands do not trigger the reregistration.

  Workaround: Use the **clear crypto gdoi** command.

- CSCsj21785

  Symptoms: A Traffic Engineering (TE) tunnel does not re-optimize to explicit path after an MTU change.

  Conditions: The TE tunnel is operating via explicit path. The MTU on outgoing interface is changed. OSPF is flapped, and it does not come up as there is MTU mismatch (MTU is not changed on peer router). Meanwhile the TE re- optimizes to a dynamic path-option as expected. Now the MTU is reverted back to the previous value, and the OSPF adjacency comes up. The TE tunnel does not re-optimize to explicit path. Manual re-optimization of the TE tunnel fails as well, and the TE tunnel sticks to the dynamic path.

  Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the particular interface.

- CSCsj22472

  Symptoms: When an IXIA-simulated BGP neighbor is not up, BGP is forced to delete the ARP entry for the IXIA host for a while. During that period, the router has to send ARP, and traffic is lost for a while.

  Conditions: While observed with other protocols, this symptom was noticed with a typical BGP configuration in which the peers are nonexistent. This would cause the SYN to be retransmitted multiple times, and after some threshold, the ARP entry would be purged.

  The ARP entries gets flushed out when the TCP retransmission timer expires. This causes the CEF adjacency to be lost, and performance can drop for packets going to that destination until the ARP is resolved again. This problem is *not* specific to BGP and is applicable to anything that rides over TCP.

  Workaround: There is no workaround.

- CSCsj25056

  Symptoms: Crash occurs with the following error message:

  ```
  %SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header, chunk 173E112C data 173EEFC8
  chunkmagic 15A3C78B chunk_freemagic 185993E4 -Process= "Check heaps", ipl= 0, pid= 5,
  - Traceback= 0x15653E8 0x311CC 0x31440 0x2ED80 0x7D855C chunk_diagnose, code = 2 chunk
  name is L2TP CC
  ```

  Conditions: Occurs when Cisco NPE-G2 is configured with L2TP running Cisco IOS Release 12.4(11)T1.

  Workaround: There is no workaround.

- CSCsj27183

  Symptoms: H323-->SIP interworking fails for a Fast start call when transcoding is enabled on an IPIPGW. Transcoding is done between G711ulaw and G729r8 codecs.

  Conditions: This failure is seen for H323--SIP--SIP--SIP and H323--SIP--SIP-- H323 call flows when transcoding is enabled on IPIPGW1. It is also seen on H323--H323--H323--SIP call flow for transcoding on IPIPGW2. This is seen only with a Fast Start call (both with H245 Tunnel enabled and disabled), and the call passes with a slow start call.

  Workaround: There is no workaround.

- CSCsj28498

  Symptoms: A router may eventually experience depletion in the small buffer pool, leading to MALLOCs and Cisco IOS software crashing.

  Conditions: This symptom is observed on a router running STUN SDLC with local- ack and having multiple SDLC primary stations connected and regularly polling (SNRM) router while the remote STUN peers are disconnected (no IP connectivity to the remote STUN peers).

  Workaround: There is no workaround.

- CSCsj30558

  Symptoms: High-availability agent sends keepalive messages to UDP port 0, which causes the keepalive mechanism to fail.

  Conditions: Occurs on a mobile router configured to use UDP for keepalive messages.

  Workaround: There is no workaround.

- CSCsj32013

  Symptoms: A Cisco 12000 series router may crash unexpectedly. Conditions: Occurred only on Cisco IOS Release 12.0(32)SY0f. Workaround: There is no workaround.

- CSCsj33060

  Symptoms: Packet marked with qos-group does not match shaping policy on IPSEC tunnels in DMVPN scenario. In the marking policy, show policy-map interface shows the packets are being marked but on the shaping policy, none of the marked packets matched the class that has "match qos-group".

  Conditions: The problem is seen in IPSec tunnel scenario where The inbound packets are marked with certain qos-group through the policy-map. The outbound packets are matched through the policy-map which is applied to the traffic entering IPSec tunnel and qos pre-classify is configured. Issue is not seen when changed to mark/match base on ip precedence.

  Workaround: There is no know workaround, except to use IP precedence based mark/match.

- CSCsj34456

  Symptoms: The mplsLdpEntityIndex for the following tables is different now:

  mplsLdpPeerTable

  mplsLdpSessionTable

  mplsLdpSesStatsTable

  The value does not match the mplsLdpEntityIndex in these tables:

  mplsLdpEntityConfGenLRTable

  mplsLdpEntityStatsTable

  mplsLdpEntityTable

mplsLdpHelloAdjacencyTable

Conditions: This is due to a bug fix CSCsi69278. Any release with this fix will encounter this disparity.

Workaround: There is no workaround.

Further Problem Description: The change in the mplsLdpEntityIndex will also be seen in the varbinds of LDP traps.

- CSCsj37111

  Symptoms: IPv4 inconsistencies and %FIB-4-FIBXDRINV error message upon reset of line card

  Condition: Problem observed on Cisco 7600 series router.

  Workaround: There is no workaround.

- CSCsj37709

  Symptoms: Memory held by mem_mgr_chunk_t and mem_mgr_mempool_t in dead process is causing an out-of-memory condition on the gateway.

  Conditions: This scenario occurs when SIP phone calls are made using the default application or a TCL IVR application and the **header-passing** command is enabled in voice service VoIP SIP configuration mode.

  The following processes are the cause of the large amount of holding memory in *Dead* process:

  0x61EC066C mem_mgr: mem_mgr_chunk_t 0x61EC091C mem_mgr: mem_mgr_mempool_t

  Workaround: Disable the **header-passing** command.

- CSCsj38829

  Symptoms: When running double authentication crypto configurations (ah encap and esp encap auth together) and passing large packet data that requires fragmentation, errored packets can be observed.

  Conditions: This symptom has been observed only on routers with AIM-VPN-PLUS AIM cards installed. Routers that support this AIM are the Cisco 1800, Cisco 2600, Cisco 2800, Cisco 3700, and Cisco 3800 routers.

  Workaround: Do not use ESP and AH double authentication. You can use the **no crypto engine accel** command in the configuration to run encryption in the SW engine.

- CSCsj39503

  Symptoms: Interface flap on a GET VPN group member (GM) may cause the GM not to re-register immediately to the key server (KS) after the interface is up. It can take up to a maximum of 8 minutes before re-registration happens.

  Conditions: An interface is down long enough, eg. greater than eight minute, the problem will be seen after the interface is back up.

  Workaround: Use EEM and trace the interface state or routing protocol neighbor. As soon as interface is UP or routing protocol neighbor is UP, issue the **clear crypto gdoi** command on the GM to force reregistration.

- CSCsj39538

  Symptoms: Router tracebacks and then crashes during deconfiguration (removal) of VRF. The following message was seen prior to crash:

  ```
  -Process= "IP RIB Update", ipl= 3, pid= 68 -Traceback= 609538D8 60D1B8B4 612B2838
  612588C8 61258CD4 6125E61C 6125ED04 6125EF30 61261CDC 6125A14C 61265A08 6126BE10
  6097CF00 609547D8 609548B8
  Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x609538FC
  ```

  Conditions: No specific conditions are known to cause this fault.

Workaround: There is no workaround.

- CSCsj40156

  Symptoms: Memory is leaking in case of radius-proxy users.

  Conditions: This symptom is seen when a rad-proxy host object is already present in the SSG box, and it receives the access-request. The accounting starts from the proxy client, which is sent to the AAA server and AAA replies with an access-accept.

  Workaround: There is no workaround.

- CSCsj41443

  Symptoms: Line protocol goes down on a Cisco 7200 router.

  Conditions: Occurs while attaching a policy to a packet over SONET (POS) interface configured for frame relay encapsulation.

  Workaround: There is no workaround.

- CSCsj45148

  Symptoms: Display IE contained in connect message is not passing through ISDN- to-H323 interworking at Originating Gateway (OGW).

  Conditions: This happens when call Initiator makes a voice call to Path Terminating Equipment (PTE) (PC simulating remote-device) passing through VGW and OGW having Cisco IOS interim Release 12.4(16.9) images.

  Workaround: There is no workaround.

- CSCsj45211

  Symptoms: Percentage-based traffic shaping fails.

  Conditions: Occurs on a Cisco router that is configured for percentage-based traffic shaping on output policy.

  Workaround: There is no workaround.

- CSCsj46178

  Symptoms: A Cisco AS5850 responds with a 500 Endpoint Unknown to a CRCX for an endpoint on a channelized T3 card. The endpoint otherwise responds normally to AUEP command.

  Conditions: This symptom is observed on a Cisco AS5850 that is controlled via MGCP, and the **endpoint naming t3** command is configured on the router in either global MGCP configuration or MGCP profile.

  Workaround: Do not configure the **endpoint naming t3** command. Use t1 endpoint naming instead.

- CSCsj46859

  Symptoms: Real Time Streaming Protocol (RTSP) inspection does not work with fragmentation.

  Conditions: Occurs only when fragmentation is set. Without fragmentation this problem does not occur.

  Workaround: There is no workaround.

- CSCsj47705

  Symptoms: An accounting record may indicate that the NAS-Port-Id has an adapter number of 1 when the correct adapter number is greater than 1.

  Conditions: This symptom is observed when AAA accounting is configured and a PPP interface that is used as a NAS port has more than two adapters.

Workaround: There is no workaround.

- CSCsj48440

  Symptoms: Packets "returned" from a WCCP appliance (web-cache) for further forwarding are always processed by the RP leading to elevated CPU usage.

  Conditions: This symptom is observed on a Cisco 7600 series router for WCCP redirection and with "L2 return" being used to return traffic from the appliance to the router. Further the router must either be configured for outbound redirection (**ip wccp** <*service*> redirect out) or the appliance must have selected hash assignment.

  Workaround: If the appliance is resident on its own subnet, apply the WCCP command **ip wccp redirect exclude in** to the appliance facing interface. Alternately use mask assignment and input redirection (**ip wccp** <*service*> redirect in).

- CSCsj49293

  Symptoms: The interface output rate (214 Mb/s) is greater than the interface line rate (155 Mb/s).

  Conditions: This symptom is observed with a Cisco 7600/7500/7200-NPE400 and below. That is, PA-POS-2OC3/1OC3 (PULL mode).

  Workaround: There is no workaround.

  Further Problem Description: From the Ixia, packets are transmitted at 320 Mb/s. On the UUT (Cisco 7600), the outgoing interface (POS-Enhanced Flexwan) shows the output rate as 200 Mb/s. But the interface bandwidth is 155 Mb/s.

- CSCsj50412

  Symptoms: This bug is addressing 2 issues: 1. LDP is not installing the outgoing label in LFIB for a directly-connected static route with null next-hop (e.g. pointing to a p2p interface)

  2. MPLS LFIB may not be updated following a quick LDP session flap. This may result in a "No Label" for outgoing label for the affected prefix.

  Conditions: Issue seen only when LDP flaps in a short interval

  Workaround: There is no workaround to prevent the issue. To recover a **clear ip route** <*affected_prefix*> will trigger an install of the outgoing labe.l

  Further problem description: LDP would be having the label from the next-hop neighbor, but doesn't update the LFIB. To confirm this a **show mpls ldp binding** <*prefix*> <*mask*> **detail** should show a label received from the appropriate neighbor.

- CSCsj54606

  Symptoms: Invalid updates to the system clock are allowed on the Cisco IOS command line interface (CLI).

  Conditions: The symptoms are observed when a user attempts to configure the set end of summer-time earlier than the start of summer-time:

  ```
  Router(config)#clock summer-time PDT date 11 mar 2007 2:00 ? <1-31> Date to end MONTH
  Month to end
  Router(config)#$r-time PDT date 11 mar 2007 2:00 11 march 2007 00:00 60
  ```

  Workaround: Do not pass invalid arguments to the **clock summer- time** command on the Cisco IOS CLI.

- CSCsj54837

  Symptoms: A Cisco 7200 that is running Cisco IOS Release 12.4 or 12.4(11)T2 crashes with a TLB (store) exception.

Conditions: This symptom is observed when Rate Based Satellite Control Protocol (RBSCP) tunneling is configured on the device.

Workaround: There is no workaround.

- CSCsj55043

  Symptoms: On certain specific router platforms, if multiple subinterfaces are configured on a Gigabit Ethernet motherboard interface and if these subinterfaces are configured with HSRP and the same VMAC, then whenever the router becomes HSRP standby for at least one of these subinterfaces, the router drops all traffic that is directed to the same VMAC on other subinterfaces.

  The following is a sample configuration that would be exposed to this issue:

  ```
  interface GigabitEthernet0/0.1 encapsulation dot1Q 1 native ip address 10.1.0.100
  255.255.0.0 standby 1 ip 10.1.0.1 standby 1 mac-address 0000.0000.0001 ! interface
  GigabitEthernet0/0.2 encapsulation dot1Q 2 ip address 10.2.0.100 255.255.0.0 standby 2
  ip 10.2.0.1 standby 2 mac-address 0000.0000.0001
  ```

  Conditions: This symptom is observed *only* on Cisco 3800 (both 3825 and 3845), 7200/NPE-G1 and 7301 motherboard Gigabit Ethernet interfaces. It is not observed on Fast Ethernet/WAN modules or on other router platforms.

  Workaround: The problem does not occur if different VMAC addresses are configured on different subinterfaces or if static VMACs are not used.

  If the problem is encountered in a production environment, a quick workaround is to shut down the Gigabit Ethernet interface of the other router in order to make one router HSRP active in all VLANs.

- CSCsj56438

  This Cisco Bug ID identifies a vulnerability in Cisco's implementation of Extensible Authentication Protocol (EAP) that exists when processing a crafted EAP Response Identity packet. This vulnerability affects several Cisco products that have support for wired or wireless EAP implementations.

  This vulnerability is documented in the following Cisco bug IDs:

  * Wireless EAP - CSCsj56438 * Wired EAP - CSCsb45696 and CSCsc55249

  This Cisco Security Response is available at the following link: http://www.cisco.com/warp/public/707/cisco-sr-20071019-eap.shtml.

- CSCsj58796

  Symptoms: No ringback is generated in calls from VoIP to a PBX end using Cisco Multicast Manager (CMM).

  Conditions: This symptom has been observed when a call is made from the VoIP side to the PBX side through an MGCP-controlled CMM.

  PBX <-------GW (CMM or Cisco 2620XM) <----CCM <----IP Phone

  Workaround: Use a Cisco 2620XM router in place of CMM.

- CSCsj58969

  Symptoms: Executing the **show port modem calltracker** command on a Cisco AS5400XM can cause bus error crash.

  Conditions: This symptom occurs on a Cisco AS5400XM with multiple calls being made and terminated when running Cisco IOS Release 12.4(13a).

  Workaround: There is no workaround.

- CSCsj64230

Symptoms: When a bidir PIM, with no directly connected receivers, router has to change its RPF interface to the RP, multicast traffic could be lost for up to 60 seconds.

Conditions: This symptom occurs if the connection to the first RP is lost and the middle router changes its RPF for its bidir upstream interface. The middle router then restarts the election process on all DF interfaces, and purges the interface point in the leaf router out its OI @L. That interface will only get repopulated upon a periodic state refresh from the leaf router because the leaf router does not have an RPF change and therefore has no reason to send a triggered Join.

Workaround: There is no workaround.

- CSCsj64731

  Symptoms: EIGRP neighbor relationship fails to establish between two routers connected directly.

  Condition: Occurs on a Cisco 2800 series router configured for Dynamic Multipoint VPN (DMVPN).

  Workaround: Choose one the following options: 1. Disable CEF. 2. Disable on-board crypto engine and use either software crypto or AIM crypto engine.

- CSCsj65189

  Symptoms: Traffic stops over EOM ckt after SSO and followed by TE FRR cutover.

  Conditions: The issue seen here is that after the SSO switchover at cat5 the local EOM label at cat5 gets changed and the same gets updated at cat2 for the corresponding VC correctly. Now, when the FRR cutover is performed at cat5, the local VC label gets changed for the second time and the same also gets updated at cat2 for the corresponding circuits. However the label push gets messed up at cat2, which results in EOM traffic loss from cat2 to cat5 but the other direction traffic passes fine. If the same FRR cutover is performed before the SSO switchover at cat5 then there will not be any problem. It is only after the SSO when this issue is observed.

  Workaround: There is no workaround.

- CSCsj66282

  Symptoms: Router with VPN Services Adapter (VSA) crashes.

  Conditions: Occurs when Cisco Unified CallManager (CCM) has an access control entry (ACE) defined for the router. When the port number is removed from the crypto interface, the router crashes.

  Workaround: There is no workaround.

- CSCsj66492

  Symptoms: When a service policy is configured under the cable modem interface and matching traffic passed through it, the policy-map counters do not go up.

  Conditions: When a service policy is configured, something like below:

  ```
  interface cable-modem 0/0/0 service-flow primary upstream service-policy output
  ```

  and matching traffic passed, the service policy should take affect for primary service flow packets. However, it does not.

  Workaround: There is no workaround.

- CSCsj71998

  Symptoms: An ATM interface loses its assigned IP address if the interface is gracefully stopped/started.

  Condition: This symptom is observed in Cisco IOS Release 12.4(17).

  Workaround: Reconfigure the interface.

- CSCsj72039

  Symptoms: The prefix of a serial interface that is configured for PPP or HDLC and that functions as a passive interface for IS-IS may not be installed in the local IS-IS database.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(18)SXF6 but is not release-specific.

  Workaround: Remove and reconfigure the **passive-interface** command.

  First Alternate Workaround: Enter the **clear isis *** command.

  Second Alternate Workaround: Enter any command that triggers the generation of the local IS-IS database.

- CSCsj72320

  Symptoms: A Cisco 7613 may crash during an SNMP dump, causing a memory allocation failure.

  Condition: This symptom is observed when you perform an SNMP dump by using an SNMP monitoring tool.

  Trigger: The application queries the IP Tunnel MIB and CISCO-SWITCH-ENGINE-MIB on the router, causing a memory allocation failure

  Impact: This leads to router not completing SSO process and router crashes with crash file on the RP

  Workaround: Remove the IP Tunnel MIB by entering the **remove tunnel mib** command.

- CSCsj72647

  Symptoms: On a Cisco IOS voice gateway, the **show call active voice brief** command output on the IP leg shows rx counters stay at 0 for 46 seconds.

  Conditions: This symptom is observed on a Cisco AS5850 that runs Cisco IOS Release 12.4(7e).

  Workaround: There is no workaround.

- CSCsj74102

  Symptoms: DTMF digits are not recognized by the remote side.

  Conditions: Occurs on a Cisco MGW using MGCP configured for DTMF RFC2833 standard under control of Cisco PGW2200. When the first digit is pressed it contains a wrong synchronization source identifier in an RTP header.

  Workaround: There is no workaround.

- CSCsj75279

  Symptoms: Router may crash in sentInviteResponse200Loopback, when receiving a specially crafted SIP packet.

  Conditions: Router must be configured to accept SIP packets, and have a dial-peer voice peer with a session target configured as loopback:rtp.

  Limited to Cisco IOS releases 12.4(12) Mainline and 12.4(11)T trains and later (and associated trains synced to these branches).

  Workaround: Removed the dial-peer entry which has the session target configured as loopback:rtp

  Further Problem Description: When the router crashes a message "%ALIGN-1-FATAL: Illegal access to a low address" will appear on the console logs.

- CSCsj78403

  Symptoms: A router may crash when the **clear ip bgp** command is entered.

Conditions: Occurs on devices running BGP and configured as a route reflector client with conditional route injection configured.

Workaround: Unconfigure conditional route injection.

- CSCsj81015

  Symptoms: Cisco Multiservice IP-to-IP Gateway (IPIPGW) crashes during a stress scenario.

  Conditions: This symptom occurs in a stress scenario with 100 SIP-H323 calls + 150 SIP-H323 DTMF interworking (rtp-nte to h245-alpha) calls.

  Workaround: There is no workaround.

- CSCsj85065

  A Cisco IOS device may crash while processing an SSL packet. This can happen during the termination of an SSL-based session. The offending packet is not malformed and is normally received as part of the packet exchange.

  Cisco has released free software updates that address this vulnerability.

  Aside from disabling affected services, there are no available workarounds to mitigate an exploit of this vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080924-ssl.shtml.

- CSCsj87522

  Symptoms: RTP and RTCP ports are leaked when a ReleaseComplete (reason=newConnectionNeeded) is received as a response to a FastStart Setup that is sent.

  Conditions: This problem is seen in Cisco IOS Release 12.4(11)T and Release 12.4(15)T images for a normal H323 to H323 gatekeeper routed call with no supplementary services.

  Workaround: There is no workaround.

- CSCsj87744

  Symptoms: Configuring a command with the string "do " in it may not behave correctly. Only commands starting with "do " should be interpreted as exec commands.

  Conditions: Using "do" as shorthand for "domain" for example in **ipe domain** CLI.

  Workaround: Do not use "do" keyword as shorthand in commands.

- CSCsj88665

  Symptoms: A device with a PA-MC-2T3+ may reset because of a bus error if a channel group is removed while the **show interface** command is being used from another telnet session at the same time, and then the telnet session is cleared.

  The device may also display Spurious Memory Accesses.

  Conditions: These symptoms have been observed in the latest Cisco IOS 12.4T and 12.2S releases.

  Workaround: Do not remove a channel group while using the **show interface** command for that interface.

- CSCsj88961

  Symptoms: SNASwitch HPR/IP (Enterprise Extender - EE) receiving retransmissions due to HPR/IP UDP packets being dropped at the UDP socket layer in the SNASw router. This leads to poor throughput across the HPR/IP pipe.

Conditions: This can occur when receiving large bursts of HPR/IP traffic inbound to the SNASwitch router. The UDP socket inbound queue can hold a maximum of 50 packets. If more than 50 HPR/IP packets are received before the SNASwitch process can run and dequeue some, subsequent packets will be dropped.

Workaround: There is no workaround.

Further Problem Description: The output of the **show ip socket detail** command or the **show udp detail** command (depending on your release of IOS) will show the number of drops that have occurred, the maximum queue size(50) and the highwater value.

HPR/IP Uses ports 12000 through 12004. Here is an example of UDP port 12003 showing 190577 dropped inbound packets:

Proto Remote Port Local Port In Out Stat TTY OutputIF 17 --listen-- x.x.x.x 12003 0 0 61 0 Queues: output 0 input 0 (drops 190577, max 50, highwater 50)

Resolution Summary: The resolution of this bug adds a new **qsize** parameter on the **snasw port** configuration command. This allows the specification of a UDP socket queue size value for HPR-IP ports only.

For example:

snasw port EE hpr-ip GigabitEthernet0/1 qsize 500

Note that the default of 50 was not changed by this. In order to increase the size of the UDP socket queue the new parameter must be specified.

Other parameters may need to be adjusted as well:

Global configuration:

ip spd queue max-threshold 512 ip spd queue min-threshold 500

Under each IP interface where HPR/IP packets are flowing in and out of this router add:

hold-queue 500 in

- CSCsj89544

  Symptoms: If a BGP keepalive message fails to be sent to a BGP peer because the transport link is down, the neighbor BGP peer does not accept any further keepalive packets even though TCP retransmits the failed message using a backup path. This eventually causes the BGP peer to go down because of holdtime expiration.

  Conditions: This happens when TCP retransmissions occur on MPLS-enabled network. This is seen only when MPLS is configured on Catalyst 6500 or Cisco 7600.

  Workaround: There is no workaround.

- CSCsj90012

  Symptoms: Some Cisco 2800 and Cisco 3800 platform routers are observed to crash upon startup after the 256MB-v5 has been loaded, and the signature files saved to flash.

  Conditions: This symptom occurs when loading the 256MB-v5.sdf file and saving signature files to flash using the **ip ips config location flash**. The router will then crash when restarted when the files are read out of flash.

  Workaround: The crash has not been observed with the package files, such as IOS-S300-CLI.pkg, nor was it repeatable on a Cisco 3725 or Cisco 2651 router.

- CSCsj90346

Symptoms: Intermittent delays in traffic to/from the GigabitEthernet interface when a WAAS/WAE or NME-CUE module is installed on a Cisco IOS 2800/3800 gateway. This can lead to noticeable impairments to voice quality when using VoIP to and through the gateway.

Conditions: When a WAE or NME-CUE module is installed in 2800/3800 router, it has been found that intermittently the GigabitEthernet interface on the chassis may send out pause frames. These pause frames will cause delays in traffic through the interface.

These pause frames are being generated it appears when the Integrated-Service-Engine interface used to connect to the WAE/NME-CUE module is being reset.

This impact is for Integrated-Service-Engine interfaces and not Service-Engine interfaces.

Use the exec command **show interface** on the GigabitEthernet and Integrated-Service-Engine and look at the pause output frames on the GigaBitEthernet interface and the “interface resets” count incrementing on the Integrated-Service-Engine interface.

One reason found as to why the Integrated-Service-Engine is being reset is when the gateway is configured for **ccm-manager music-on-hold** and the Cisco CallManager is using multicast music-on-hold. When calls through the gateway are placed on hold, the software by default will attempt to listen for the multicast music-on-hold stream on all interfaces. This in turn causes the Integrated-Service-Engine to reset.

Workaround: If **ccm-manager music-on-hold** is configured on the gateway, remove the command and reapply it with the optional bind keyword pointing to an active interface on the gateway. This forces the software to listen for the multicast stream on the interface indicated with the bind keyword. Make sure that the interface indicated in the bind command is the interface in which the multicast stream is coming in from.

Note that this issue is fixed in Cisco IOS Release 12.4(15)T2 via CSCsk58014.

- CSCsj91069

  Symptoms: If the filter within a class-map is changed from DSCP to ACL, classification of packets under any of the class-maps stops working.

  Conditions: This happens right after reload while traffic is running and matching using the DSCP filter.

  Workaround: Reapply the service policy after you make the change and it will start matching properly.

- CSCsj92153

  Symptoms: Prolonged high CPU usage may occur in the "Tag Control" process in steady-state conditions and in the "IP RIB Update" process during route change events.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that function in a network environment with large numbers of BGP routes such as more than 100,000 BGP routes.

  Workaround: There is no workaround. However, if BGP next-hop tracking is enabled, disable it. Doing so helps to alleviate the high CPU usage because there are less route change events.

- CSCsj92911

  Symptoms: A crafted EIGRP packet sent to a device enabled with EIGRP configured may cause the input interface to block (queue wedge).

  Conditions: EIGRP is partially configured.

  Workaround: Disable EIGRP or add a network statement. A reload is not required to clear the blocked interface.

- CSCsj93012

Symptoms: A router may crash when QoS is enabled.

Conditions: Seen with IMA ATM interfaces on 7500 and 7200. Occurs when ATM and serial interfaces have QoS configurations as output/input policy and when peer is reloaded/or write memory is done. This is specific to IMA.

Workaround: There is no workaround.

CSCsj93195

Symptoms: A bus error may occur on an MSFC when ISAKMP is enabled, and the following error message may be generated in the logs:

```
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON Address Error (load or instruction fetch)
exception, CPU signal 10, PC = 0x41579EB0
```

Conditions: This symptom is observed on a Cisco 7600 series that has a Supervisor Engine 720 and that runs Cisco IOS Release 12.2(33)SRA2.

Trigger: Executing **crypto map cm redundancy public** command.

Impact: This crash prevent customer to configure their crypto, as they do not want to have the box crashing again.

Workaround: There is no workaround.

Further Problem Description: Cisco IOS Release 12.2(33)SRAs is developed for and intended to run on Cisco 7600 series routers. We do not encourage you to run this release on Cisco Catalyst 6500 series switches. However, if you do run Cisco IOS Release 12.2(33)SRA2 on a Cisco Catalyst 6500 series switch, the symptom may occur.

- CSCsj94561

  Symptoms: A router may crash because of a bus error when you perform an OIR of a PA-MC-8TE1+ port adapter or when you enter the **hw-module slot** *slot-number* **stop** command for the slot in which the PA-MC-8TE1+ port adapter is installed.

  Conditions: This symptom is observed on a Cisco 7200 series.

  Workaround: There is no workaround.

- CSCsj94818

  Symptoms: Virtual circuit (VC) goes to inactive state due to the fact that peak cell rate (PCR) is higher than physical bandwidth.

  Conditions: Problem occurs on Cisco 877 router with ADSL2+ and with Cisco IOS Release 12.4(11)XJ3 and Cisco IOS Release 12.4(15)T1. Occurs when device is configured for VBR-NRT and PCR rate higher than VC bandwidth.

  Workaround: Reset the VC.

- CSCsj95475

  Symptoms: Multicast replicated packets are dropped when passed through an interface with crypto map attached and VPN Services Adapter (VSA) is active.

  Conditions: Occurs when multicast packets are coming in the fast switching path, and multicast packets get replicated on different interfaces.

  Workaround: use the **no ip mroute-cache** command to disable multicast fast switching.

- CSCsj95534

  Symptoms: High CPU is observed on SNMP Engine while polling dsx1FracIfIndex for DS3s.

  Conditions: This has been observed on a Cisco 7206 VXR platform having NPE-G1 that is running Cisco IOS Release 12.4(14).

Workaround: Applying a view on DS1 MIB prevents such high CPU usage. This prevents the user to monitor those entries.

Further Problem Description: The SNMP Engine comes into a loop and Get-NEXT always reports the same values. This happens while coming to the first interface channelized E3 card. Deleting this interface created the problem on the channelized E3 one.

- CSCsj95947

  Symptoms: The following message is seen on the router:

  ```
  *Aug 6 16:34:47.188: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error, -PC= 0x8005EC50,
  -Traceback= 0x809971F4 0x809B9C2C 0x809DD8A4 0x8005EC50 0x800651E4 0x800652A8
  0x809E42D4 0x809C4A38 0x800652EC 0x809C4BA0 0x809E42D4 0x80A0854C 0x800DB8C0
  0x800DEE48
  ```

  Conditions: The conditions under which this symptom occurs are not known at this time.

  Workaround: There is no workaround.

- CSCsj96002

  Symptoms: Interfaces on CE , WLC and/or SE may flap after an IP address is assigned.

  Conditions: Cisco IOS Release 12.4.11.XJ or higher Possibly CME4.1

  Network statement under OSPF should contain the IP address of the WLC/Service-Engine/Content Engine

  Workaround: Use Redistribute connected instead

- CSCsj96577

  Symptoms: A Cisco AS5400HPX crashes due to a bus error as indicated by show version "System returned to ROM by bus error at PC 0x61728370, address 0xB0D0B45".

  Just before the crash the following error message is seen:

  %SYS-2-NOTQ: unqueue didn’t find 674D6D40 in queue 3C -Process= "MGCP Application", ipl= 0, pid= 170

  Conditions: This symptom is observed on a Cisco AS5400HPX.

  Workaround: There is no workaround.

- CSCsj97045

  Symptoms: While running a Cisco IOS Release 12.4 Mainline release, a Cisco router mAY crash with a bus error. The error displayed will be similar to:

  Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x605AFF94

  Conditions: This symptom has been observed only if gateway is configured for Voice over IP (VoIP).

  Workaround: There is no workaround.

- CSCsj97484

  Symptoms: The router may crash when the linecard is booted.

  Conditions: It’s not easily reproducible. THe problem may be experienced if there are heavy distribution traffic to the linecards.

  Workaround: There is no workaround.

- CSCsj97602

  Symptoms: A Cisco access server may run out of free processor memory. This symptom can be seen in the **show process memory** command. Increased memory utilization will be seen in the Dead pool.

Conditions: This symptom has been observed only in access servers that participate in Cisco Customer Voice Portal (CVP).

When a VXML application is configured with fetchaudio, the fetchaudio playout fails after user disconnect. The fetchaudio should have been removed from the prompt list, but it was not. This causes the session not to be freed when the application is finished.

Workaround: A reload will temporarily free the leaked memory.

- CSCsj99269

  Symptoms: With some VPN configurations, such as configurations with a multipath import or an import map, the CPU usage of the router may be very high for a long time, even after BGP convergence has occurred.

  Conditions: This symptom is observed on a Cisco router that functions in a highly scaled environment involving several hundred VRFs and occurs after the router has been reloaded or after a switchover has occurred.

  Workaround: There is no workaround.

- CSCsk00580

  Symptoms: Cisco 7200 router crashes at stile_classification_ip_input.

  Conditions: Above symptom is seen in Cisco routers loaded with IOS version of 12.4(17.4)T1

  Workaround: There is no workaround.

- CSCsk01615

  Symptoms: Category processing (the time after the user enters category selection to the time the prompt returns) took 8 minutes to complete.

  Conditions: When adding or modifying any signature categories with the following releases: 12.4(11)T2, 12.4(11)T3, 12.4(15)T.

  Workaround: There is no workaround.

  Further Problem Description: Scenarios that this issue will happen:

  1. Configure the following categories first category all retired true category ios_ips basic retired false then load sig pkg on to the router, the router then took ~ 2 minutes to build the engines. Afterwards, removing the "ios_ips basic" or add any other sig categories, then the router will take 8 minutes category processing.

  2. Configure the following categories first category all retired true

  then load sig pkg on to the router, then add "category ios_ips basic" or any other categories, e.g. "web_services", the router then took ~ 8 minutes for category processing. Afterwards, removing the "ios_ips basic" or add any other sig categories, then the router will take 8 minutes for category processing.

- CSCsk04350

  Symptoms: When there are burst L2TP session authentication failures on the LNS and the **vpdn logging** global configuration is enabled, the system takes too many CPU cycles to print the syslog messages to the system console.

  Conditions: Burst L2TP LNS session authentication fails.

  Workaround: Disable system console logging by entering the **no logging console** global configuration command.

- CSCsk04900

  None

Symptoms: Router crashes when tcp logging is enabled and killed in remote receiver, such as a linux server.

Conditions: Kill the syslog server at remote.

Workaround: Do not kill the receiver on remote end.

- CSCsk04970

  Symptoms: There is a memory leak and fragmentation in *Dead* process due to MallocLite. After disabling malloclite, it will be seen as memory allocated to the "Virtual Exec" process in the **show memory allocating-process [total]** command output.

  Conditions: The leak occurs whenever the **show vpdn session [l2tp] [all] username** *username* command is used, and there are many non-matching entries. Memory will be leaked proportional to the number of non-matching usernames (approximately 170 bytes per non-match).

  Workaround: Avoid using the **show vpdn session [l2tp] [all] username** *username* command.

- CSCsk04977

  Symptoms: IPC process may fail to send config messages to the PA.

  Conditions: While doing any configuration changes, PA IPC may fail.

  Workaround:There is no workaround.

- CSCsk05653

  Symptoms: The **aaa group server radius** subcommand **ip radius source-interface** will cause the standby to fail to sync.

  ```
  c10k-6(config)#aaa group server radius RSIM c10k-6(config-sg-radius)#ip radius
  source-interface GigabitEthernet6/0/0
  c10k-6#hw-module standby-cpu reset c10k-6# Aug 13 14:49:31.793 PDT:
  %REDUNDANCY-3-STANDBY_LOST: Standby processor fault (PEER_NOT_PRESENT) Aug 13
  14:49:31.793 PDT: %C10K_ALARM-6-INFO: ASSERT MAJOR RP A Secondary removed Aug 13
  14:49:31.793 PDT: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault (PEER_DOWN) Aug
  13 14:49:31.793 PDT: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault
  (PEER_REDUNDANCY_STATE_CHANGE) Aug 13 14:49:31.793 PDT: %REDUNDANCY-3-STANDBY_LOST:
  Standby processor fault (PEER_NOT_PRESENT) Aug 13 14:49:31.793 PDT:
  %REDUNDANCY-3-STANDBY_LOST: Standby processor fault (PEER_DOWN) Aug 13 14:49:31.813
  PDT: %REDUNDANCY-3-IPC: cannot open standby port no such port Aug 13 14:49:32.117 PDT:
  %RED-5-REDCHANGE: PRE B now Non-participant(0x1C11 => 0x1421) Aug 13 14:49:32.117 PDT:
  %REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a standby insertion
  (raw-event=PEER_REDUNDANCY_STATE_CHANGE(5))
  Aug 13 14:50:52.617 PDT: %RED-5-REDCHANGE: PRE B now Standby(0x1421 => 0x1411) Aug 13
  14:50:54.113 PDT: %C10K_ALARM-6-INFO: CLEAR MAJOR RP A Secondary removed Aug 13
  14:51:33.822 PDT: -Traceback= 415C75D8 4019FB1C 40694770 4069475C Aug 13 14:51:33.822
  PDT: CONFIG SYNC: Images are same and incompatible
  Aug 13 14:51:33.822 PDT: %ISSU-3-INCOMPATIBLE_PEER_UID: Image running on peer uid (2)
  is the same -Traceback= 415CCC2C 415C75FC 4019FB1C 40694770 4069475C Aug 13
  14:51:33.822 PDT: Config Sync: Bulk-sync failure due to Servicing Incompatibility.
  Please check full list of mismatched commands via: show issu config-sync failures mcl
  Aug 13 14:51:33.822 PDT: Config Sync: Starting lines from MCL file: aaa group server
  radius RSIM ! <submode> "sg-radius" - ip radius source-interface GigabitEthernet6/0/0
  ```

  Conditions: This symptom is observed if the **aaa group server radius** subcommand **ip radius source-interface** CLI is configured on a box with dual PREs.

  Workaround: If the customer does not use the **aaa group server radius** subcommand **ip radius source-interface** *interface*, this will not be a problem.

  If they use the **aaa group server radius** subcommand **ip radius source-interface** *interface* on a Cisco 10000 router in simplex mode (a single PRE), this will not be a problem.

If they run with dual PREs, then they will need to remove the **aaa group server radius** subcommand **ip radius source- interface** *interface* from the configuration as a workaround.

Removing the **aaa group server radius** subcommand **ip radius source-interface** *interface* from the configuration could cause problems for the customer. The radius server may be expecting the request to come from a specific source address. The router will now use the address of the interface the packet egresses the router from, which may change over time as routes fluctuate.

- CSCsk06024

  Symptoms: Router crashes when WebVPN client attempts to use Outlook Web Access.

  Conditions: Occurs when PKI trustpoint configuration is incomplete or incorrect.

  Workaround: There is no workaround.

- CSCsk09651

  Symptoms: A router crashes while a service policy is being attached, detached, or modified across a virtual template under traffic.

  Conditions: This symptom is observed on a Cisco 7200 or Cisco 7301 router that is configured with MLPPP over FR on channelized interfaces.

  Workaround: There is no workaround.

- CSCsk09933

  Symptoms: The configured max-threshold/minimum-threshold option on Selective Packet Discard (SPD) is lost after reloading the router.

  Conditions: If the configured minimum threshold value is greater than default maximum threshold value or the maximum threshold value is less than default minimum threshold value, the router will report "min-threshold must be less than default max-threshold" or "max-threshold must be greater than min- threshold" while doing the system reload.

  Workaround: Reconfigure the appropriate **ip spd** threshold command.

- CSCsk10057

  Symptoms:

  Packet fails to reach from initiator to responder with ipsec-gre tunnel

  Conditions:

  Happened when configured for process switching

  Workaround:

  Use CEF switching at the tunnel interfaces

- CSCsk10133

  Symptoms: During a mid-call codec switch from g.711 to g.729 on a gatekeeper- controlled gateway, the gateway may intermittently receive a Bandwidth Confirmation (BCF) message from the gatekeeper and wrongly detect it as a Bandwidth Reject (BRJ) message. This results in a release complete being sent from the gateway with a cause code of 65.

  Conditions: This condition appears to be intermittent, due to the order of the OLC and the ECS (Empty Capability Set) messaging. This issue will be seen only on gatekeeper-controlled gateways that are doing bandwidth control. This issue is currently being seen only when codecs are switched mid-call to a codec with less bandwidth utilization.

  Workaround: Any of the following workarounds should alleviate this issue:

  1. Disable bandwidth requests from the gateway:

voice service voip h323 no ras brq

2. Configure all call legs to use the same codec.

3. Do not use a gatekeeper with this gateway.

Further Problem Description: This issue appears to be a recurrence of CSCee60960 and can be seen by enabling the following debugs:

- debug h225 asn1 - debug ras - debug cch323 all

The following would be seen after the BCF is received:

```
581565: .Aug 15 13:45:06.376: //- 1/xxxxxxxxxxx/H323/cch323_ras_handle_recv_msg:
received msg of type BCF_CHOSEN 581566: .Aug 15 13:45:06.376:
//94506/5A1D2CEFA2CC/H323/cch323_percall_ras_sm: ccb 0xC2A5CA58: received event
CCH323_RAS_EVENT_BCF while at CCH323_RAS_STATE_ACTIVE state 581567: .Aug 15
13:45:06.376: //94506/5A1D2CEFA2CC/H323/cch323_percall_ras_sm: ccb 0xC2A5CA58:
changing to new state CCH323_RAS_STATE_ACTIVE 581568: .Aug 15 13:45:06.376: //-
1/xxxxxxxxxxx/H323/cch323_iev_queue_service: Dispatch 0x1E internal event to H245 IWF
SM 581569: .Aug 15 13:45:06.376: //94506/5A1D2CEFA2CC/H323/run_h245_iwf_sm: received
IWF_EV_BRJ while at state IWF_OLC_OUT_AWAIT_BCF 581570: .Aug 15 13:45:06.376: //-
1/xxxxxxxxxxx/H323/h323_set_release_source_for_peer: ownCallId[94506], src [6]
581571: .Aug 15 13:45:06.376: //94506/5A1D2CEFA2CC/H323/h245_iwf_set_new_state:
changing from IWF_OLC_OUT_AWAIT_BCF state to IWF_OLC_IDLE state 581572: .Aug 15
13:45:06.376: //- 1/xxxxxxxxxxx/H323/cch323_iev_queue_service: Dispatch 0xE internal
event to H245 IWF SM 581573: .Aug 15 13:45:06.376:
//94506/5A1D2CEFA2CC/H323/run_h245_iwf_sm: received IWF_EV_OLC_FAILED while at state
IWF_ACTIVE 581574: .Aug 15 13:45:06.376: //-
1/xxxxxxxxxxx/H323/h323_set_cc_cause_for_spi_err: Categorized cause:65, category:278
```

- CSCsk10985

  Symptoms: IMA group interface does not come up after the reload.

  Conditions: This symptom is observed on a Cisco 2811 router with ATM interface that is using VWIC2-2MFT-T1/E1 connected to MGX AUSUM card.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the IMA interface.

- CSCsk12089

  None

  Symptoms: Cisco 7200 sees a hang with crypto protected multicast packets in GETVPN configuration.

  Conditions: Problem is seen on doing a ping to multicast address from one of the host.

  Workaround: Failure is seen only with specific configuration.

- CSCsk12238

  Symptoms: Calls are torn down within a second after establishment.

  Conditions: This symptom occurs when pinging from the client to the NAS gives "Request drop link from bundle".

  Workaround: Configure the **dialer idle-timeout 0** command under the template. This will never bring down the calls nor bring down the physical link.

  template template1 dialer idle-timeout 0

- CSCsk12739

  Symptoms: Router runs out of free memory after applying service policies.

Conditions: Occurs on a Cisco 7200 router running Cisco IOS Release 12.4(15)T with a large QOS configuration. When service-policy is applied to an interface, the memory consumption becomes too high and the free memory is reduced in 235Mb as each service-policy is applied. The interface can be shutdown, but the behavior is the same.

Workaround: There is no workaround. Downgrade to Cisco IOS Release 12.4(11)T1 or upgrade to Cisco IOS Release 12.4T(15)T2.

- CSCsk13250

  Symptoms: When Cisco's Secure Device Provisioning Registrar (SDP) is configured on a Cisco 7206 router that has a hardware encryption accelerator card enabled (the VSA card), the registrar fails to process incoming requests properly.

  Conditions: Occurs when the SDP Registrar processes registration requests coming from a remote location and when the VSA card is enabled.

  Workaround: Disabling the VSA card makes the registrar operations work in software mode, and then it works properly.

- CSCsk14137

  Symptoms: Cisco 1812J router fails to forward incoming multicast traffic. This problem might be also seen with HWIC-4ESW on other routers.

  Conditions: Occurs when the "ip igmp snooping" feature is used with switch-port and a VLAN interface is used as the incoming interface

  Workaround: Disable "ip igmp snooping" or use a routed-port instead of a switch-port.

- CSCsk14208

  Symptoms: A WAN line card or module that is configured for WCCP Redirection via the **ip wccp web-cache redirect {out | in}** interface configuration command may not redirect packets to the Cache Engine after an OIR has occurred or after the line card or module has been reloaded.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router when WCCP redirection is applied to the interfaces that are configured on the WAN line card or module.

  Workaround: Remove and re-apply the WCCP Redirection configuration to the affected WAN interfaces by entering the **no ip wccp web-cache redirect {out | in}** interface configuration command followed by the **ip wccp web-cache redirect {out | in}** interface configuration command.

  Alternate Workaround: Delete and configure WCCP Redirection globally on the router by entering the **no ip wccp web-cache** router configuration command followed by the **ip wccp web-cache** router configuration command.

- CSCsk16618

  Symptoms: Cisco 870 router is missing **usbflash** commands.

  Conditions: Occurs on a Cisco 870 router running Cisco IOS Release 12.4(16) and Cisco IOS Release 12.4(16)T.

  Workaround: There is no workaround.

- CSCsk16821

  Symptoms: A Cisco router acting as a DHCP server may experience the following problem when Secure ARP is also configured, and the Secure ARP keepalive time is less than the DHCP lease time. If a client device goes into sleep mode for a period of time less than the DHCP server's configured lease time but more than the Secure ARP time, the DHCP lease will be cancelled at the server. If the client awakes, it will have a valid DHCP lease, for the remainder of the last lease time it was granted. When the device awakes and attempts to renew its IP address, it sends a unicast DHCPREQUEST

to the DHCP server. Because the lease has been removed from the DHCP server, and there is no ARP entry for the client, the DHCP Server does not send any reply to the device. The Secure ARP feature will, however, prevent the device from communicating until its lease has expired.

Conditions: This symptom has been observed with a Cisco router acting as a DHCP server when Secure ARP is also configured.

Workaround: Disable Secure ARP on the DHCP server or change the Secure ARP keepalive time to correspond to the lease time.

- CSCsk16904

  Symptoms: A NAT router fails a H323 connection by ARP resolution failure, which ARP request is triggered by H225/H245 packet. When the problem occurs, the NAT router creates an incomplete entry and sends an unexpected ARP request for the destination IP address instead of the next-hop IP address, whereas the destination prefix is not a directly connected route. Therefore if the next-hop router of NAT router disables proxy ARP, the packet forwarding fails. Ping to same destination succeeds when the problem occurs.

  Conditions: This problem happens under the following conditions:

  - Static NAT or dynamic NAT is configured. - The next-hop router of NAT router disables proxy ARP. - H323 terminal device tries to call for another one over NAT router.

  Workaround: Enable proxy ARP on the next-hop router.

- CSCsk17564

  Symptoms: A Cisco 7200 series may crash when you perform a soft OIR of a port adapter.

  Conditions: This symptom is observed when Frame Relay encapsulation is configured along with QoS on a PA-4T+ port adapter. However, the symptom is not specific to the PA-4T+ port adapter.

  Workaround: There is no workaround.

- CSCsk18909

  Symptoms: A Cisco 7200 series that is configured for ATM and QoS may crash.

  Conditions: This symptom is observed when you attempt to change the priority parameters while traffic is being processed.

  Workaround: There is no workaround.

- CSCsk19108

  Symptoms: Before sending initial Invite, a Cisco gateway is doing DNS SRV query which gives the actual server name where SIP service is running. And then DNS A query for this server gives IP address of Proxy Server. So initial call is established through this SIP-proxy server. After getting SIP Refer message, to initiate call-transfer with Transfer-to location as Domain-Name, SIP-gateway is doing just DNS A Record Query for Refer-to Host which is returning an IP address where SIP is not running. This causes Transfer Failure.

  Conditions: This symmptom is observed on a Cisco 2800 series router but is not platform dependent. The Transfer-target address received in Refer is a FQDN (with default port -5060 OR no port).

  Workaround: There is no workaround.

- CSCsk19360

  Symptoms: Path confirmation fails when dtmf-relay is rtp-nte on gateways for dspware version 22.3.0

  Condition: This happens when the DTMF digit relay packet is treated as NTE-tone packet by DSP.

Workaround: IOS should not be setting the NTE-tone payload type if it's not configured by the user. Set the NTE-tone payload type to zero. NTE-tone and NTE must have different default payload types.

- CSCsk19661

  Symptoms: In a Cisco 7500 HA router in RPR+ mode when configuring and unconfiguring channel groups under an E1 controller, the router reports the following:

  ```
  *Aug 22 17:58:34.970: %HA-2-IPC_ERROR: Failed to open peer port. timeout *Aug 22
  17:58:34.974: %HA-3-SYNC_ERROR: CCB sync failed for slot: 1 *Aug 22 17:58:34.974:
  %HA-5-SYNC_RETRY: Reloading standby and retrying sync operation (retry 1).
  ```

  And the standby RSP is reloaded.

  Conditions: This symptom is observed when configuring and unconfiguring channel groups under an E1 controller.

  Workaround: There is no workaround.

- CSCsk21209

  Symptoms: A Cisco 7500 router may crash.

  Conditions: This symptom occurs when dLFIoFR and QoS are configured on the router and you try to move from dLFIoFR to dLFIoATM.

  Workaround: There is no workaround.

- CSCsk21328

  Symptoms: Router crashes during shutdown or deletion of interface.

  Conditions: Occurs on interfaces on which IPv6 is enabled.

  Workaround: There is no workaround.

- CSCsk21431

  Symptoms: A ping from the FR-DTE to the FR-DCE fails when FR-VCB is configured in the FR-DTE.

  Conditions: This symptom is observed in Cisco IOS Release 12.4(16.14c).

  Workaround: There is no workaround.

- CSCsk21764

  Symptoms: A Cisco router may reload unexpectedly due to a bus error crash.

  Conditions: The symptoms can be observed when the router is running Voice XML.

  Workaround: There is no workaround.

- CSCsk22420

  Symptoms: Time-based ACL matches packets even though the access list is set to INACTIVE.

  Conditions: Occurs on router running Cisco IOS Release 12.4.

  Workaround: There is no workaround.

- CSCsk22496

  Symptoms: Spurious access or a router crash may be seen when removing a crytpo key.

  Conditions: The crypto key was not generated in the router. when we try to remove the unconfigured crypto key the spurious access may be seen.

  Workaround: There is no workaround.

- CSCsk22854

Symptoms: A router might crash when attaching a service-policy at range of atm pvc.

Conditions: The service-policy contains configs which are not supported in IN direction,. The crash is seen only when attaching the service-policy at the unsupported IN direction.

Workaround: There is no workaround.

- CSCsk23367

  Symptoms: Some packets are seen as late arrival in "show ip sla stat" output, although all the packets arrived on time. The "debug ip sla trace" shows an rtt value of about 1 day - 1 second + real rtt. For example, rtt=86399012 (86400000-1000+12) instead of 12ms

  Conditions: This has been seen on a Cisco 1812 running Cisco IOS Software Version 12.4(6)T7

  Workaround: There is no workaround.

- CSCsk25046

  Symptoms: For a policy applied to an interface with an ifindex of 14, the corresponding entry will not appear in cbQosServicePolicyTable. This is impacting device monitoring.

  Conditions: The following two conditions are required for the issue to exist:

  - There should be an interface with an ifindex of 14 with a policy applied. - There should a be a policy applied on the control plane.

  Workaround: Remove the policy on the control plane.

- CSCsk25243

  Symptoms: Policy-map counters may not be accurate and may yield erroneous bps values. If these values are used in policers, it may mean unexpected packet drops.

  Conditions: This issue has been seen in a crypto/QoS environment where packet reassembly is needed (such as tunnel protection scheme with tunnel configured to have IP MTU of 1500).

  Workaround: In some platforms, such as Cisco 7200 NPE-G1/VAM2+, it has been seen that disabling hardware encryption fixes the issue.

- CSCsk25491

  Symptoms: A Cisco router may reload and display a message similar to the following:

  ```
  Aug 19 12:28:51.960: %SYS-3-MGDTIMER: Previous timer has bad forward linkage, timer =
  64176C30. -Process= "IPSEC key engine", ipl= 4, pid= 150 -Traceback= 0x607462F0
  0x6084FD88
  12:28:52 zulu Sun Aug 19 2007: Address Error (load or instruction fetch) exception,
  CPU signal 10, PC = 0x60815DD4
  ```

  Conditions: This symptom has been experienced on a Cisco 7206VXR that is running Cisco IOS Release 12.4(16).

  Workaround: There is no workaround.

- CSCsk25651

  Symptoms: With Cisco Unity Express (CUE) integrated to Cisco Unified Communication Manager (CUCM)/CallManager and utilizing SRST functionality, when the IP phones are registered to the SRST router, the message-waiting indication (MWI) states may be incorrect.

  Conditions: When a phone registers to a Cisco SRST router, each directory number (DN) gets a particular ephone-dn number that will have a particular MWI state. If the phone unregisters from the SRST router and later re-registers to the router (possibly due to an intermittent connectivity to the CUCM), the ephone-dn number may be different since the ephone-dn numbers are assigned sequentially in a first-come, first-served fashion. The MWI state, however, is remembered from the previous registration that used that ephone-dn number so the MWI status could be incorrect.

Workaround: Configure both the SRST router and the CUE to use SUBSCRIBE/NOTIFY MWI method.

- CSCsk26299

  Symptoms: When a service policy is modified after it has been applied to an interface, the changes do not take effect.

  Conditions: Occurs on a Cisco 2800 router running Cisco IOS Release 12.4(15)T.

  Workaround: Apply the service policy to the interface a second time.

- CSCsk26331

  Symptoms:

  This may cause configuration issue.After upgrading router code to 12.4.13a code, the cli will not allow any changes to an atm pvc. It gives the following error " Possibly multiple users configuring IOS

  simultaneously".

  Conditions: This is seen with a 7206vxr router with npe-g1. when an ima interface is configured with a bandwidth value higher than the allowed value before the "ima-group" has been added on the atm interface. When a "no - shut" is done on the ima interface, the pvc cannot be deleted.

  Workaround: Reload Router will correct the problem

  Further Problem Description: routerA (config)#int atm 1/ima1.14016 routerA config-subif)#no pvc innac 20/14018 Unable to delete PVC 20/14018 on ATM1/ima1.14016. Possibly multiple users configuring IOS simultaneously.

- CSCsk26774

  Symptoms: Native VLAN information is not included in CDP packets going out ports of an EtherSwitch (ESW) module in Cisco 28xx and Cisco 38xx routers. All the platforms using switchports (of any kind built-in/NM/WIC/HWIC) have this issue: Cisco 8xx, Cisco 17xx, Cisco 18xx, Cisco 26xx, Cisco 36xx, Cisco 37xx, Cisco 28xx, and Cisco 38xx.

  Conditions: This symptom causes Cisco IP phone models 7961, 7941 and 7970 that are running SCCP firmware to fail to forward traffic coming from a PC connected at the back of the phone.

  Workaround: Enable the "Voice VLAN Access" setting on the phone.

- CSCsk27077

  Symptoms: Cisco 7200 router crashed while clearing virtual access interface

  Conditions: It was observed while clearing virtual access interface with delay timer configured

  Workaround: There is no workaround.

- CSCsk27356

  Symptoms: Secure copy (SCP) from a server to a router fails.

  Conditions: Occurs when attempting to use SCP to copy a file from a server to a router running Cisco IOS Release 12.4(15)T.

  Workaround: There is no workaround.

- CSCsk28266

  Symptoms: A Cisco 871 router that is configured for VPN remote access re-initiates itself when the VPN server is unavailable.

  Conditions: Occurs when the VPN server is unavailable. The router repeatedly attempts to connect to the server.

Workaround: Configure a backup VPN server that can be used when the primary server fails.

- CSCsk28361

  Symptoms: 4000 virtual-template (VT) takes high CPU during system load configuration.

  Conditions: Occurs when 4000 VT interfaces are loaded from TFTP to running configuration.

  Workaround: There is no workaround.

- CSCsk28546

  Symptoms: In a setup with 32k EVCs configured, when the standby is reloading mpls reserved labels are deleted in the active. Explicit-null getting deleted was affecting the Cisco 7600 platform because of the way recirculation is handled.

  Conditions: The problem is triggered from active RP when standby is coming UP.

  Workaround: There is no workaround

- CSCsk28748

  Symptoms: When an IMA group subinterface (atm1/ima1.14016) is configured before a **no shut**is done on the IMA group interface, the maximum value VBR-NRT peak cell rate (PCR) option is displayed as 1536/1920(T1/E1) instead of 1523/1904.

  Conditions: Occurred when IMA group subinterface is configured before assigning ATM interface to the IMA group.

  Workaround: Configure the IMA group interface first and then configure image group sub- interface.

- CSCsk29216

  Symptoms: On an ATM interface, if tx-ring-limit were set to 1 with heavy traffics then the interface might get wedged. Throughput performance is degraded due to many packets got dropped.

  Conditions: This symptom occurs when setting tx-ring-limit to 1 under an ATM interface with heavy burst traffics.

  Workaround: Recommend minimal tx-ring-limit is 2 under this circumstance.

- CSCsk29283

  Symptoms: On a Cisco MWAM running gateway GPRS support node software (GGSN), if SGSN does not include recovery IE in initial signaling requests and then if the recovery IE is included subsequently, GGSN will initiate a path cleanup for the path recovery changed and hence deletes all existing PDPs on the path.

  Conditions: If the SGSN does not include recovery IE in the initial messages and then it includes recovery IE.

  Workaround: If Echo requests are enabled on the GGSN, this problem should occur since the GGSN will always have the current recovery IE of the SGSN which is received in the echo response. Or if SGSN can be set to include the recovery IE in all signaling messages, this problem will not occur.

- CSCsk30100

  Symptoms: Cisco 7200 router may crash when members are moved from a Distributed Link Fragmentation and Interleaving over Leased Lines (dLFIoLL) interface to a Multilink Frame Relay (MFR) interface.

  Conditions: Occurs when the QoS service policy is in suspend mode on a MFR interface.

  Workaround: Ensure the QoS policy is not in suspend mode before moving members from LFIoLL to MFR.

- CSCsk31883

Symptoms: Router crashes.

Conditions: Occurs while giving "**no radius-server domain-stripping vrf VRF1** "

Workaround: There is no workaround.

- CSCsk32095

  Symptoms: The Ethernet interface flaps after configuring QoS on the interface.

  Conditions: Occurs on PA-2FE-TX port adapter after applying QoS to the interface.

  Workaround: There is no workaround.

- CSCsk32970

  Symptoms: Alternative packets are not being dropped by Extended ACL with deny statements in CEF switching path.

  Conditions: Occurs when CEF is enabled.

  Workaround: Disable CEF or use standard ACL.

- CSCsk33054

  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/warp/public/707/cisco-sr-20070912-regexp.shtml

- CSCsk33780

  Symptoms: Compressed Real-Time Protocol (cRTP) shows errors and Low Latency Queuing (LLQ) shows drops from default queue although there is no traffic to match it.

  Conditions: This problem can be seen under load of MPPP bundle of several serial interfaces with LLQ and cRTP enabled.

  Workaround: There is no workaround.

- CSCsk34098

  Symptoms: Router crash immediately upon entering the command **no ip flow-export destination 0.10.10.2 3000**.

  Conditions: Specific deconfiguration of netflow export config

  Workaround: Do not deconfigure netflow export addresses.

- CSCsk34332

Symptoms: A Cisco 7200 router crashes when the **slm frame-relay interface** command is executed.

Conditions: This symptom is observed with a Cisco 7200 router that is loaded with a Cisco IOS 12.4(16.14)T3 image.

Workaround: There is no workaround.

- CSCsk34490

  Symptoms: Given a valid value, the ACT TTL command rejects the value with an error message.

  ```
  Router(config-ext-nacl)# permit ip host x.x.x.x any tos normal ttl lt ? <0-255> Time
  to live value
  Router(config-ext-nacl)# permit ip host x.x.x.x any tos normal ttl lt 4 % Invalid
  value for operator.
  ```

  Conditions: This symptom is observed under normal conditions.

  Workaround: There is no workaround.

- CSCsk34641

  Symptoms: A router may exception while registering a corrupt eToken.

  Conditions: This symptom is observed only when a particular corrupt eToken is inserted. This symptom has been observed only on a single eToken.

  Workaround: Format the eToken.

- CSCsk34715

  Symptoms: Router crashes when the **no ip nat outside** command is removed while traffic is being processed.

  Conditions: Occurs on a Cisco 7200 router that uses ACL as source.

  Workaround: There is no workaround.

- CSCsk34743

  Symptoms: The following message appears, and traffic is dropped:

  ```
  *Sep 5 12:50:49.159: %OCE-3-OCE_FWD_STATE_HANDLE: Limit of oce forward state handle
  allocation reached; maximum allowable number is 50000
  ```

  Conditions: This symptom is observed when using an image after Cisco IOS Release 12.4(16.14)T1 and when VSA is doing prefragmentation of process- switched packets.

  Workaround: Disable prefragmentation by using the **crypto ipsec fragmentation after-encryption** command.

- CSCsk34832

  Symptoms: Memory leaks out at about 10 to 15 percent overnight.

  Conditions: This symptom occurs when a mix of application traffic is sent to the HTTP Secure server and when CPU utilization is at about 30 percent.

  Workaround: There is no workaround.

- CSCsk35804

  Symptoms: A Cisco router may experience a bus error crash preceded by the following error message:

  %HMM_ASYNC-4-NO_MODEMS_PRESENT: HMM Digital Modem Card 1 contains no active modems

  Conditions: This symptom is seen if the router contains a Digital Modem Network module that contains no SIMMs.

  Workaround: Remove the card or install an NM-xDM card with valid SIMM modules.

- CSCsk35985

  Symptoms: The system crashes when the **show ipv6 ospf lsdb-radix** hidden command is entered.

  Conditions: This symptom is observed when the **show ipv6 ospf lsdb-radix** hidden command is entered.

  Workaround: Do not enter the **show ipv6 ospf lsdb-radix** command.

- CSCsk36324

  Symptoms: On a Cisco router, OSPF might go into a loop during SPF calculation, causing high CPU utilization and rendering the router inaccessible.

  Conditions: This symptom occurs when router LSAs with a link metric disallowed by RFC 2328 are present in the network (note that Cisco routers do not originate such LSAs) and when the network is unstable (link flapping during the SPF calculation).

  Workaround: To fix the problem, reload the router. To prevent the problem, manually configure a link metric according to RFC 2328.

  Important Note: CSCsk36324 caused MPLS TE defect CSCsl18176 and has been backed out under defect CSCsl18176. A new fix for this issue will be committed under defect CSCsl32318.

- CSCsk36559

  Symptoms: When one of the T1 or E1 controller NM-HDV2 goes down, the voice calls in the other controller are dropped.

  This condition relates to interface x/0 x/0/0 (for example, 4/0 causes 4/0/0 to go down).

  Conditions: This problem could happen in the MGCP PRI backhauled setup with NM- HDV2.

  Workaround: There is no workaround.

- CSCsk36600

  Symptoms: Router might crash when an extended ACL is applied.

  Conditions: Occurs when QoS with the extended ACL is configured first and ACL statements are defined later.

  Workaround: Configure permitted host statements successively and do the same for permitted networks, then configure ACL statements and attach this ACL to a class-map.

- CSCsk36639

  Symptoms: Memory leak occurs when multicast packets pass through an interface with crypto map attached and the VSA crypto engine is used.

  Conditions: Occurs because multicast packets coming in through the fast-switching path get replicated on different interfaces.

  Workaround: Use the **no ip mroute-cache** command to disable multicast fast- switching.

- CSCsk37675

  Symptoms: IKE security associations cause memory leak.

  Conditions: Caused by the failure of IKE phase one exchange.

  Workaround: There is no workaround.

- CSCsk38628

  Symptoms: Router fails to process traffic after a reload.

  Conditions: IKE/IPSec SA fails to come up, blocking traffic on the serial interface.

Workaround: Either remove the crypto map on the router and reapply them or remove the online diag.

- CSCsk38937

  Symptoms: Traffic is lost for more than 15 seconds after a cutover.

  Conditions: This symptom is observed when a cutover is performed.

  Workaround: There is no workaround. Traffic recovers after 15 seconds.

- CSCsk38994

  Symptoms: Changes made to Network-Based Application Recognition (NBAR) policies are not automatically applied. Instead the policy must be removed and reapplied to the interface.

  Conditions: Occurs in Cisco IOS Release 12.4.11(T) and later releases.

  Workaround: Upgrade to Cisco IOS Release 12.4(16).

- CSCsk39340

  Symptoms: High CPU usage may occur when the IP Rewrite Manager (IPRM) is active.

  Conditions: This symptom is observed on a Cisco router when there is a large number of prefixes and when there is network instability.

  Workaround: There is no workaround.

  Further Problem Description: The fix for this caveat alleviates the high CPU usage.

- CSCsk39642

  Symptoms: A router crashes.

  Conditions: This symptom is observed when you are running Cisco IOS Release 12.4(17) or Release 12.4T and when you copy the saved configuration to the running configuration.

  Workaround: There is no workaround.

- CSCsk39804

  Symptoms: The multicast Connection Admission Control (CAC) state may be incorrect after multicast routes have been cleared.

  Conditions: This symptom is observed on a Cisco router that has Source Specific Multicast (SSM)-mapped channels that are locally joined on the router.

  Workaround: There is no workaround.

- CSCsk40296

  Symptoms: A router may crash when the **clear pppoe all** command is entered.

  Conditions: Occurs when a service policy is attached to a virtual template.

  Workaround: There is no workaround.

- CSCsk40676

  Symptoms: The inside interface of a Cisco router running EZVPN may become unresponsive when sending ICMP messages from a remote VPN client connection.

  Conditions: Occurs when LZS compression is used on a Windows Vista client.

  Workaround: Disable LZS compression.

- CSCsk42373

  Symptoms: Memory leak observed.

  Conditions: Occurs with all config commands.

Workaround: There is no workaround.

- CSCsk42419

  The Secure Shell server (SSH) implementation in Cisco IOS contains multiple vulnerabilities that allow unauthenticated users the ability to generate a spurious memory access error or, in certain cases, reload the device.

  The IOS SSH server is an optional service that is disabled by default, but its use is highly recommended as a security best practice for management of Cisco IOS devices. SSH can be configured as part of the AutoSecure feature in the initial configuration of IOS devices, AutoSecure run after initial configuration, or manually. Devices that are not configured to accept SSH connections are not affected by these vulnerabilities.

  Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-1159 has been assigned to this bug.

  The Security Advisory for this issue is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080521-ssh.shtml

- CSCsk42469

  Symptoms: Router may crash or report a spurious access when a Data-Link Connection Identifier (DLCI) is altered.

  Conditions: Occurs on PA-MC-T3-EC and PA-MC-2T3-EC. When the **frame-relay fragment** command is entered, a router with NPE-G2 will crash or a router with NPE-G1 will produce a spurious access if frame-relay is unconfigured on the interface.

  Workaround: Unconfigure "Frame-relay fragment" first and then unconfigure frame-relay encapsulation.

- CSCsk42759

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS that can be exploited remotely to trigger a memory leak or to cause a reload of the Cisco IOS device.

  Cisco has released free software updates that address these vulnerabilities. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities addressed 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, if administrators do not require the Cisco IOS device to provide voice over IP services.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080924-sip.shtml.

- CSCsk43369

  Symptoms: HWIC-4SHDSL_IMA responds with a F5 end-to-end cell instead of a F5 segment cell.

  Conditions: HWIC-4SHDSL-IMA is used as a CPE and F5 segment cells are sent to it.

  Workaround: There is no workaround.

- CSCsk43463

  Symptoms: Router was forced to reload when the **no router ospf** <#> command is entered.

  Conditions: The problem happens when "memory record" was also configured.

  Workaround: There is a work around. Disable memory lite (using **no memory lite** configuration command) in which case crash will not be seen.

- CSCsk43745

Symptoms: The multicast switching path might be incorrectly displayed as fast- switched in the output of the **show ip interface tunnel x** command.

Conditions: This symptom is observed when the **tunnel-sequence datagrams** command is enabled on the tunnel interface, which should disable fast-switching.

Workaround: This is just a display issue. No workaround is needed.

- CSCsk44550

  Symptoms: The ATM interface line protocol goes down when configuring OAM-related configurations.

  Conditions: Occurs when configuring "oam-pvc" and "oam-bundle."

  Workaround: There is no workaround.

- CSCsk45076

  Symptoms: Router experiences traceback: ipnat_dns_fix_resou.

  Conditions: Occurs when DNS traffic traverses the router and NAT is configured.

  Workaround: There is no workaround.

- CSCsk45981

  Symptoms: Classification is not happening in third-level policy-map classes.

  Conditions: Occurs on a Cisco 7200 router that is running a prerelease build of Cisco IOS Release 12.4(15)T2.

  Workaround: There is no workaround.

- CSCsk47116

  Symptoms: Cisco 2811 router acting as a Dynamic Multipoint VPN (DMVPN) hub will corrupt multicast packets sent from spoke to spoke through the hub.

  Conditions: The symptom is seen when there are at least three spoke sites with receivers and senders on the same multicast group.

  Workaround: Disable hardware encryption on the Cisco 2811.

- CSCsk47888

  Symptoms: The standby processor continuously reloads because of the failure of bulk sync.

  Conditions: The IP address of the interface is configured with the same IP address as the HSRP virtual IP address. This can be performed while the interface is in the shutdown state.

  Trigger: A user configuration error.

  Impact: Continuous rebooting of standby processor.

  Workaround: Avoid sharing the interface IP address with the HSRP virtual IP.

- CSCsk48089

  Symptoms: This is to allow users to unconfigure policy on an interface when both route-map tag and "CR" option are given.

  Conditions: Enhancement in the **ip policy route-map** command for backward compatibility.

  Workaround: There is no workaround.

- CSCsk48250

  Symptoms: SW_MGR-3-SM_ERROR: Tracebacks found while establishing l2tpv3 tunnel and the tunnel is not established.

Conditions: This symptom is observed in a Cisco IOS Release 12.4(17.4)T1 image.

Workaround: There is no workaround.

- CSCsk48302

  Symptoms: Router crashes after adding link while member links are shut down.

  Conditions: Occurs on a Cisco 7200 router with PA-MC-T3-EC.

  Workaround: Reloads may be caused by route flapping. Add new members while existing members are active.

- CSCsk48525

  This is an enhancement to make ipv4fib global feature message ISSU compliant.

- CSCsk49705

  Symptoms: The **ip nat inside source static network** command does not have the <cr> option.

  Conditions: This symptom is observed on a Cisco 7200 router that is loaded with Cisco IOS Release 12.4 or 12.4T.

  Workaround: There is no workaround.

- CSCsk50163

  Symptoms: The help returned by the ? in the **crypto pki certificate storage on with-keypair** CLI is incomplete.

  Conditions: This issue is seen while loading Cisco IOS Release 124-17.4.T1 and 124-12.9.PI6.

  Workaround: There is no workaround.

- CSCsk50208

  Symptoms: Shape average percentage calculations seem to be wrong, and the configured shape average percentage cannot be changed.

  Conditions: This symptom is observed on a Cisco router that is configured with the MQC-Based Frame Relay Traffic Shaping feature.

  Workaround: There is no workaround.

- CSCsk50212

  Symptoms: A router reports a %SYS-2-CHUNKBOUNDSIB error and crashes because of "Unexpected exception to CPU."

  Conditions: This symptom is observed when all the following conditions are met:

  - The router is running Cisco IOS Release 12.4(15)T or T1. - A named access list is referenced in a service policy. - The service policy is applied to an interface.

  Under these conditions, the symptom is observed either during the boot or when the access list is being modified.

  Workaround: There is no workaround.

- CSCsk51927

  Symptoms: When the **ppp multilink** command is used, the Virtual-Access interface that is created and cloned from BRI interface is having punt adjacency.

  Conditions: This symptom is observed when the **ppp multilink** command is configured to create the multilink bundle.

  Workaround: Removing the **ppp multilink** command can make packets CEF-switchable on the physical interface.

- CSCsk52140

  Symptoms: A router crashes.

  Conditions: This symptom is observed while testing the NFAS feature.

  Workaround: There is no workaround.

- CSCsk52255

  Symptoms: With WIC-1SHDSL-V3 and Cisco IOS Release 12.4(11)XJ4, F5 OAM has incorrect response to F5 Loopback segment.

  Conditions: If OAM is configured, this problem will appear. This was introduced in Cisco IOS Release 12.4(15)T.

  Workaround: Do not configure OAM on an ATM interface.

- CSCsk52683

  Symptoms: The system crashes when there are clients trying to associate with AP.

  Conditions: This symptom is observed when AAA authentication fails with misconfigurations in the system or when the wireless clients are given the wrong password to try to associate.

  Workaround: Make sure that the AAA configuration is set up correctly and that the client password is configured correctly.

- CSCsk55016

  Symptoms: TCP checksum corruption occurs on A Cisco 7200 NPE-G2 router using VSA for IPSec encryption terminating GRE+IPSec tunnels into VRF's. NAT is applied on the GRE tunnel for translating post decrypted clear packets. If there also exists a Crypto Map (on any other interface), and even if the crypto map is not related to the GRE tunnels, then TCP packets traversing through the GRE+IPSec tunnel and getting NAT'd could lead to TCP checksum corruption.

  Conditions: 7200-G2-VSA as headend terminating GRE+IPSec Tunnel Protection tunnels into VRF's. The ingress WAN interface is also in a VRF (front-door VRF). NAT outside applied on the GRE tunnel, and NAT inside applied on the VRF LAN interface. When a spoke sends ICMP or UDP packets, the Cisco 7200 VSA decrypts the packets, NAT's them and sends forwards to the VRF LAN segment. No issues here. When the Spoke sends TCP packets, the 7200-VSA decrypts, NAT's and forwards. But the receiving router on the far-end complains about TCP checksum corruption and drops the packets. So the TCP checksum is not being correctly modified by the 7200-VSA post NAT.

  Workaround: Remove any CryptoMaps from all interfaces on the Cisco 7200. Or use VAM2+ instead of VSA.

- CSCsk55344

  Symptoms: Router crashes with simultaneous format on an ATA file system through CLI and SNMP.

  Conditions: This symptom is observed on a router that runs Cisco IOS with ATA file system.

  Workaround: There is no workaround.

- CSCsk55516

  Symptoms: Ezvpn connect using ACL fails to bring up the tunnel.

  Conditions: This symptom is observed with Cisco IOS Release 124-17.4.T1.

  Workaround: There is no workaround.

- CSCsk55532

  Symptoms: GGSN crashes.

  Conditions: This symptom is observed while unconfiguring service-policy under APN.

Workaround: There is no workaround.

- CSCsk56496

  Symptoms: On a router using high availability route processor redundancy (RPR)+, after an encapsulation change is done on serial interfaces of channelized port adapters, a reload of the slave Route Switch Processor (RSP) is occurs.

  Conditions: Occurs when you exit configuration mode.

  Workaround: There is no workaround.

- CSCsk56864

  Symptoms: EzVPN configured with virtual interface and using Cellular/Async interface as its outside interface with dial-on-demand routing (DDR), can not bring up a call. Also, when Cellular/Async interface loses its IP address, EzVPN gets stuck waiting for the interface to obtain an IP again.

  Conditions: Occurs on a Cisco router with DDR on the Ezvpn outside interface (Async or Cellular). Async/cellular losing its IP address

  Workaround: There is no workaround.

- CSCsk57114

  Symptoms: CPUHOG messages may be generated when an "snmpwalk" is performed on the cpwVcMplsNonTeMappingTable object.

  Conditions: This symptom is observed on a Cisco router that has a large number (about 30,000) of pseudowires configured.

  Workaround: Reduce the number of pseudowires that are configured on the router.

- CSCsk57589

  Symptoms: The following error messages may be displayed on the newly active RP after an SSO switchover is performed.

  ```
  %LFD-3-INVINSTALLER: Wrong installer 4 for packet 1/124 update (was 2)
  %BGP_MPLS-3-VPN_REWRITE: installing rewrite for 1:1:2.0.0.0/8 failed: General Error
  ```

  Conditions: This symptom may be observed on a router that is configured for both PE and ASBR functionality in an MPLS/VPN network, and the same RD is used for a VRF on all the routers in the network.

  Workaround: Reconfigure the ASBR to use a unique RD for the given VRF.

- CSCsk57730

  Symptoms: The **show flash** and **dir** commands cause an error message.

  Conditions: This symptom is observed only on Cisco AS5400XM and Cisco AS5350XM products that are running a Cisco IOS Release 12.4(17.7) image.

  Workaround: To upgrade to a newer Cisco IOS version, we must do a netboot because we cannot do a copy tftp flash:.

- CSCsk58014

  Symptoms: The module will not return to the steady state after a reset.

  Conditions: This symptom is observed whenever the module is reset.

  Workaround: There is no workaround.

- CSCsk58019

Symptoms: Low call success rate (CSR) is seen when calls traverse a Cisco 3845 router configured for Network Address Translation (NAT) and acting as a session border controller (SBC).

Conditions: This is seen while doing Performance testing on NAT-SBC. The CSR was as low as 25% while making just 75 SIP calls.

Workaround: There is no workaround.

- CSCsk60020

  The Secure Shell server (SSH) implementation in Cisco IOS contains multiple vulnerabilities that allow unauthenticated users the ability to generate a spurious memory access error or, in certain cases, reload the device.

  The IOS SSH server is an optional service that is disabled by default, but its use is highly recommended as a security best practice for management of Cisco IOS devices. SSH can be configured as part of the AutoSecure feature in the initial configuration of IOS devices, AutoSecure run after initial configuration, or manually. Devices that are not configured to accept SSH connections are not affected by these vulnerabilities.

  Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-1159 has been assigned to this bug.

  The Security Advisory for this issue is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080521-ssh.shtml

- CSCsk60054

  Symptoms: Upon certain configuration changes, the running configuration might not be able to be displayed and the following error message might appear:

  ```
  % Configuration buffer full, can't add command:! %Aborting Save. Compress the config,
  Save it to flash or Free up space on device
  ```

  Conditions: This symptom is observed either using or not using the **service compress-config** command on a Cisco IOS router that is running CallManager Express (CME) when configuring more than 22 voice user-profiles.

  Workaround: There is no workaround.

- CSCsk60112

  Symptoms: Uninitialized memory causes failures when label switched path (LSP) ping is performed

  Conditions: This error occurs when the allocated memory is non-zero.

  Workaround: There is no workaround.

- CSCsk61275

  Symptoms: No ring on Cisco Unified IP Phone 7941 while hunting the second overly number in call forward no answer (CFNA) configuration.

  Conditions: Overlay button is configured on Cisco 7941, and CFNA configured from first number to second number.

  Workaround: Use Cisco IOS Release 12.4(11)XJ3 or Cisco IOS Release 12.4(11)T3.

- CSCsk61643

  Symptoms: AFW application IVR is causing memory leak in Chunk Manager.

  Conditions: Occurred on a Cisco AS5400XM running Cisco IOS Release 12.4(15)T1 and Cisco IOS Release 12.4(11)T2.

  Workaround: Reload the router.

- CSCsk61790

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.

- CSCsk62253

  Cisco IOS software contains two vulnerabilities within the Cisco IOS WebVPN or Cisco IOS SSLVPN feature (SSLVPN) that can be remotely exploited without authentication to cause a denial of service condition. Both vulnerabilities affect both Cisco IOS WebVPN and Cisco IOS SSLVPN features:

  1. Crafted HTTPS packet will crash device - Cisco Bug ID CSCsk62253.
  2. SSLVPN sessions cause a memory leak in the device - Cisco Bug ID CSCsw24700.

  Cisco has released free software updates that address these vulnerabilities. There are no workarounds that mitigate these vulnerabilities. This advisory is posted at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20090325-webvpn.shtml

- CSCsk62514

  Symptoms: When applying a large number (over a thousand) of VRF configurations with BGP enabled to a router, it may take a longer time to complete the configuration. For example, when copying a large VRF configuration file into the running configuration of a router, it will take a longer time to transfer the configuration data.

  Conditions: The conditions under which this symptom occurs are unknown.

  Workaround: There is no workaround.

- CSCsk63655

  Symptoms: A Media Gateway Control Protocol (MGCP) gateway may return a 524 or 510 error code with the reason as "invalid local connection option" for a valid "L:" parameter in a CRCX message.

  Conditions: The symptoms can be observed on a router that is running Cisco IOS Interim Release 12.4(17.4)T1 or later, when the **debug mgcp parser** command with verbose tracelevel is disabled.

  Workaround: Enable **debug mgcp parser** with verbose tracelevel.

- CSCsk64021

  Symptoms: A VXML gateway intermittently fails to submit a recording.

  Conditions: This symptom is observed in Cisco IOS Release 12.4 and 12.4T.

  Workaround: There is no workaround.

- CSCsk64248

  Symptoms: Crypto maps support order entry of policy idents using sequence numbers. The sending of packets on the outbound interface cascades through the ordered list and applies encryption according to the first match. The packet is encrypted and encapsulated with the appropriate ESP header, which includes the SPI. When receiving an IPSec packet, the SPI is relevant for identifying the security association and the appropriate keys. Once the packet is decrypted, the IP header is compared against the policy idents, which should match. When an ordered list of policy idents is used, the IP header should be compared against the policy idents associated with the security association. This bug was identified based on the code attempting to compare the IP header against the first match in the ordered set of policy idents as opposed to the policy ident associated with the SPI. As a result, the packet is dropped because of invalid policy idents checking.

  Conditions:

1. A crypto map with a point-to-point IPSec SA is established to a remote peer.

2. A crypto map with a group IPSec SA is established to a GET VPN group.

3. The order of the crypto map entries is such that the point-to-point SA is prioritized ahead of the group SA.

4. The proxy idents of the group SA are a superset of the point-to-point SA.

5. Outbound traffic matches the point-to-point SA proxy idents first; therefore, it is encrypted with the point-to-point SA.

6. A received encrypted packet uses the SPI to identify the correct key, which happens to associate with the group SA.

7. The packet is decrypted using the group SA.

8. The packet is subsequently checked against the proxy idents. The check is done in priority order, which matches first on the point-to-point SA. The security association used for decryption and the security association used for proxy ident matching are inconsistent; therefore, the packet is dropped despite the fact that the proxy ident matches for the subsequent group security association.

9. The context of the decryption SHOULD have been preserved such that the group SA proxy idents are used for the matching. This would have made the key used for the decryption and the proxy idents consistent, allowing the packet to be forwarded.

Workaround: There is no workaround. The point-to-point IPSec policy ident must be removed in order for the GDOI policy to be applied. This prevents a graceful transition between point-to-point IPSec and GET VPN.

- CSCsk65172

  Symptoms: MLP fails to negotiate MRRU when changing the default MTU (1500 bytes) configuration of multilink interfaces on the client, LAC, and LNS.

  Conditions: This problem is seen only in a VPDN scenario.

  Workaround: There is no workaround.

- CSCsk65460

  Symptoms: Multicast fast switching fails on the decapsulating provider edge (PE) router when encryption is configured.

  Conditions: This happens on a Cisco 7200 router with Cisco IOS Release 12.4(17.4)T1.

  Workaround: There is no workaround.

- CSCsk65515

  Symptoms: Spurious or misaligned memory access can be seen at atm_nvgen_static_map.

  Conditions: The symptoms can be observed when an SVC is configured on an ATM interface and when executing the command **show running- config**.

  Workaround: There is no workaround.

- CSCsk65601

  Symptoms: PPP tunnel does not come up after PE edge interface flapped.

  Conditions: This symptom is observed on a Cisco router when the **show mpls l2transport vc** command is entered.

  Workaround: Use the **xconnect** command to unconfigure and then reconfigure the xconnect under the serial interface being flapped to restore.

- CSCsk65796

Symptoms: All frames received on gigabit ethernet interface are dropped. All drops are reported as overruns in the output of **show interfaces** and **show controllers**.

Conditions: Symptom is observed on gigabit ethernet interfaces on NPE-G2 network processor of Cisco 7200 Series Routers. All IOS trains that support NPE-G2 are affected.

Symptom is observed only when the gigabit ethernet controller is in promiscuous mode and with moderate traffic rate. Line protocol on the interface remains up when the error condition is present.

Workaround: There is no workaround. When the gigabit controller falls into this condition, the only way to recover is to power-cycle the router. Soft reload does not clear the problem.

Further Problem Description:

Ethernet controller goes into promiscuous mode under two conditions: - bridging is configured on the interface - number of MAC addresses that have to be stored in its MAC address filter table exceed the capacity of the table.

The latter case may happen when a large number of HSRP groups is configured or a large number of IP multicast groups are to be received on the interface.

- CSCsk66907

  Symptoms: A CPU Hog occurs because of a Skinny MOH Server that is causing phones to unregister:

  ```
  %SYS-3-CPUHOG: Task is running for (xxx)msecs, more than (xxx)msecs (xxxxxx),process =
  Skinny MOH Server.
  ```

  Conditions: This symptom is observed if Music on Hold (MOH) is being streamed from flash.

  Workaround:

  - Use the live feed option by plugging in a CD player or iPod or any such device to the MoH port on the UC500. - Disable MOH from flash - that implies tone on hold (or beep on hold).

  Further Problem Description: Similar to DDTS CSCsi09549.

- CSCsk68656

  Symptoms: ISSU upgrades among 12.2SRx releases will operate correctly as will upgrades among 12.2SB releases. ISSU upgrades between 12.2SB and 12.2SRx releases will not work correctly because the mpls_supported field and some counters will not be correctly interpreted. This is due to a different interpretation of the version 1 message format in the 12.2SBx and 12.2SB code base. This will impact only an internal **show** command display and will not affect the functionality of the router.

  Conditions: This symptom is observed with ISSU upgrades between 12.2SB and 12.2SRx.

  Workaround: There is no workaround.

  Further Problem Description: This DDTS is pertinent to ISSU upgradability and affects the output of an internal **show** command.

- CSCsk69533

  Symptoms: Card type configuration is lost on a Cisco 7500 router.

  Conditions: Occurs when dLFIoLL+SSO is configured on a Cisco 7500 and a controller is shutdown followed by a switchover.

  Workaround: Reload the router.

- CSCsk69758

  Symptoms: Router is unable to turn on the message waiting indicator (MWI) lights of phones connected to certain PBX systems that run a recent software release. The router fails to convert SIP notify messages into the appropriate QSIG MWI messages.

Conditions: This symptom is observed only on certain PBXs that have been upgraded to a recent software release.

Workaround: There is no workaround.

- CSCsk70446

  Symptoms: Cisco IOS software emits the %DATACORRUPTION-1-DATAINCONSISTENCY error message whenever it detects an inconsistency in its internal data structures.

  A traceback appears after the error message. This traceback is encountered with long URLs.

  Conditions: The conditions under which these symptoms occur are unknown.

  Workaround: There is no workaround.

  Further Problem Description: It is important to note that this error message does not imply that packet data is corrupted. However, it does provide an early indicator of other conditions that can eventually lead to poor system performance or a Cisco IOS restart.

- CSCsk71117

  Symptoms: The topo_name on the upgraded version remains null, causing XDR to become disabled. All features that use XDR as their distribution mechanism will not work.

  Conditions: Software upgrade (ISSU) from SB9 to SR, that is, from pre-MTR release to post-MTR release.

  Workaround: There is no workaround.

- CSCsk73415

  Symptoms: Power-on self tests (POSTs) are not run on FIPS approved crypto algorithms that are invoked during SSL, including AES128, 3DES, SHA1, and RSA.

  Conditions: This symptom is observed during booting.

  Workaround: There is no workaround.

- CSCsk74199

  Symptoms: Creation of a file or directory in the root directory of usb token causes a crash.

  Conditions: This symptom is observed only if the token is initialized using PKI CLIENT 4.5 with 3.65 compatible. If the token is initialized with PKI CLIENT 3.65, the symptom will not occur.

  Workaround: Use PKI CLIENT 3.65 for initializing the token.

- CSCsk75098

  Symptoms: A Cisco 7200 NPE-G2 router with a VSA encryption card, terminating IPSec EasyVPN Dynamic Virtual Tunnel Interfaces, exhibits high CPU utilization during IKE and IPSec rekeys, potentially causing some tunnels to go down.

  Conditions: This symptom is observed on a Cisco 7200-G2 router with a VSA card, acting as an IPSec HUB, terminating EasyVPN DVTI remote-access IPSec tunnels into VRFs. At high tunnel scale (more than 1000 tunnels), the CPU can spike close to 100 percent during IKE and/or IPSec rekey, potentially causing traffic and tunnels to drop.

  Workaround: Do not use more than 1000 RA EasyVPN DVTI tunnels on a Cisco 7200. Or switch to Legacy EasyVPN tunnels (with dynamic crypto maps).

- CSCsk75147

  Symptoms: A cbs3120 switch may crash during license installation, while reloading the slave switch that is being installed with license.

  Conditions: This symptom is observed when:

1. Installing up to 10 licenses in one file on Slave 4 in one vty session. 2. Reloading Slave 4 while installing the license on another vty session.

Workaround: There is no workaround.

Further Problem Description: The issue is related to Inter-Process Communication (IPC). The crash is due to accessing an already freed port info. But the crash may be prevented by adding a check atcipc_notify_session_closure.

- CSCsk76053

  Symptoms: When using route-map to redirect the traffic from one physical interface to be rerouted to the loopback interface, the traffic is not redirected.

  Conditions: Occurs when router is configured for "EZvpn client on stick" 1interface inside/outside, loop being the inside.

  Workaround: Configure interface vlan1.

- CSCsk76410

  Symptoms: A PPPoE client router crashes when a VMI PPPoE session from either end is cleared.

  Conditions: This symptom has been observed in MANET environments, where VMI and PPPoE are used to connect mobile ad-hoc routers (MARs). The triggering event is the **clear pppoe all** command from either the PPPoE server or the client router.

  Workaround: There is no workaround.

- CSCsk76478

  Symptoms: The Interfaces Multilink are down, and the following error message is seen:

  ```
  ATMPA-3-BADTXPACKET: Switch1: bad tx packet on vcd 9 size 0
  -Traceback= 0x60391080 0x60100024 0x6085BC6C 0x6090EF0C 0x6090F858 0x6030691C
  0x60306CD4 0x611F7748 0x611DFF70 0x611E0174 0x602A34BC 0x606E57D8
  0x603077F4 0x60307E14 0x60863A18 0x60118294$f
  ```

  Conditions: This symptom occurs only when:

  1. RTP packets are switched from one PPPoA interface to another PPPoA

  interface, and IP Header Compression is configured on both interfaces. That

  is, frames are decompressed, switched, and then recompressed.

  2. Traffic that is being pumped has no RTP payload. The RPM has configured

  RTP, and RTP traffic starts to be sent.

  Workaround: Enable the **ip rtp coalesce** command.

- CSCsk77282

  Symptoms: A Cisco IOS router may no longer be able to show the configuration or do other file operations because all of the file descriptors are in use by files opened by the Embedded Event Manager (EEM) Remote Procedure Call (RPC) Event Detector (ED) policies.

  Conditions: This occurs when a significant number of EEM RPC policies are executed. Each time a new EEM RPC session is started and then closed, a single file descriptor is left open.

  Workaround: The only way to recover is to reload the Cisco IOS device.

  Further Problem Description: The output of **show file descriptors** command can show you which file descriptors are open. Ones left open by EEM RPC will show a path of tmpsys:eem_rpc_n, where n is some integer. For example:

  ```
  Router#show file descriptors File Descriptors:
  FD Position Open PID Path 0 0 0002 137 tmpsys:eem_rpc_1 1 0 0002 118 tmpsys:eem_rpc_0
  2 0 0002 137 tmpsys:eem_rpc_1 3 0 0002 118 tmpsys:eem_rpc_0
  ```

- CSCsk78692

  Symptoms: A Cisco router that is running IOS Release 12.4(15)T1 may reload unexpectedly because of a bus error crash.

  Conditions: This symptom has been experienced repeatedly. The information gathered points to a software issue. At this stage, the root cause has not been identified. This enclosure will be updated as more information is gathered.

  Workaround: There is no workaround at the current time.

- CSCsk78854

  This is an enhancement to make the IPV6 GLOBAL FEATURE message ISSU backward compatible. This fix is only required in ISSU aware releases and should not have any customer impact.

- CSCsk79911

  Symptoms: When calls are pumped into a Cisco 5400xm and Cisco 5400hpx, the following tracebacks are displayed on the console:

  ```
  *Oct 4 23:12:46.195: %SYS-3-INVMEMINT: Invalid memory action (free) at interrupt
  level, -Traceback= 0x60480784 0x6061AD9C 0x6280CAC0 0x6062B9E4 0x6062C9A0 0x6062CA54
  0x600908BC 0x60093640 0x6008D88C 0x601EEF4C 0x600701A0 0x60245B54 0x60748EA0
  0x805FB57C 0x60224D58
  ```

  This is not service impacting because the calls are coming up fine and are staying up for the entire call duration.

  Conditions: These tracebacks are displayed when the calls are coming up on the Cisco 5400. This can be reproduced by loading the Cisco 5400 with Cisco IOS Release 124-17.4-T1 and starting to make bulk calls. Within 15 minutes of the test, a traceback can be seen on the console. Initially for a few times only the traceback is seen for the entire test duration.

  Workaround: There is no workaround.

- CSCsk81337

  Symptoms: Multipart post to HTTP server fails.

  Conditions: HTTP client uses multipart post recording data to server; the failure is caused by content-disposition filename string being enclosed between a pair of quote (") characters.

  Workaround: There is no workaround.

- CSCsk81602

  Symptoms: IPsec failover facilitated by Hot Standby Routing Protocol (HSRP) does not work because the subsystem is not correctly initialized.

  Conditions: Occurs on routers running Cisco IOS Release IOS 12.4(15)T and Cisco IOS Release 12.4(15)T1.

  Workaround: There is no workaround.

- CSCsk82241

  Symptoms: Security Device Manager (SDM) is unable to restore default alert frequency parameters after alert frequency has been set to another value.

  Conditions: Occurs when using SDM to manage Intrusion Prevention System (IPS) 5.x signatures on routers running Cisco IOS Release 12.4(11)T2 and later releases.

  Workaround: Use CLI to reset the alert frequency to default.

- CSCsk82507

  Symptoms: Per-PDP policing is not done.

Conditions: This symptom is observed when the **match flow pdp** command is configured under a class map.

Workaround: There is no workaround.

- CSCsk82537

  Symptoms: About once every 1 or 2 minutes, the value of the delta time found in the responding router in an IP SLA setup is 1 second behind the value it should have. This is causing false timeout as the RTT is then considered as being around 24 hours. The following output illustrates this problem:

  IP SLAs(100) jitter operation: Timed out arrival (rtt=86399012)

  For 3 consecutive probes:

  ST: 75656998, RT: 75657005, DT: 0, CT: 75657014 => correct ST: 75658006, RT: 75658009, DT: 0, CT: 75657018 => should be 75658018 ST: 75659006, RT: 75659009, DT: 0, CT: 75658018 => should be 75659018 ST: 75659998, RT: 75660005, DT: 0, CT: 75660014 => correct

  Conditions: This has been seen on a Cisco 1812 running Cisco IOS Release 12.4(6)T7.

  Workaround: There is no workaround.

- CSCsk82821

  Symptoms: The UUT is not able to receive the large ICMP message.

  Condition: This symptom occurs on the s72033-adventerprisek9_wan_dbg-vz.122- 32.8.11.SX117 image.

  Workaround: There is no workaround.

- CSCsk83480

  Symptoms: The multilink interfaces are going down while running LFIoFR.

  Conditions: This symptom is seen when configuring LFIoFR. Verify everything is working fine and follow these steps:

  - no encap frame-relay, on the interface - encap frame-relay, on the interface - configure LFIoFR DLCI, on the subinterface - default all configs under virtual-template - no int virtual-template 1 - int virtual-template 1 - configure back all configurations under virtual-template

  Workaround: There is no workaround.

- CSCsk86004

  Symptoms: Need to keep IVR related error debugs enabled all the time for pervasive CAP contact center.

  Conditions: When a voice gateway is used as an IVR "contact center," it is often necessary to turn on error debugs for ivr, vxml, http client, rtsp, and mrcp.

  Workaround: The error debugs need to be manually enabled each time the router is reloaded or when all debugs are disabled.

- CSCsk86150

  Symptoms: When EIGRP goes down, BGP installs the major network in the routing table. When EIGRP comes up again, it installs the subnet routes in the routing table, while the BGP major network remains in the routing table. Also, the BGP local source route is not installed in BGP table.

  Conditions: Occurs on routers running Cisco IOS Release 12.4(10b) and 12.4(13c) Enterprise Services images.

  Workaround: Reconfigure the network command

- CSCsk86596

  Symptoms: Traceback below is seen when NAT port-map feature is used:

  %SYS-3-INVMEMINT: Invalid memory action (free) at interrupt level, -Traceback= 0x60DCF214 0x600DE678 0x62444240 0x61400E0C 0x61423574 0x60162C2C 0x601411B8 0x6012EE48 0x60125008 0x60873574 0x60876730 0x6086F158 0x6030A9B0 0x60947FB8 0x60950810

  Conditions: This traceback is seen when packets match port-map configuration.

  Workaround: Disable CEF on the inside interface with the **no ip route-cache cef** command.

- CSCsk90741

  Symptoms: Intrusion Prevention System (IPS) causes high CPU usage and crashes on routers with 256 MB or less of memory.

  Conditions: Occurs if IPS 5.x signatures are loaded using the **copy <url> idconf** command before configuring "ip ips signature-category". If "ip ips signature-category" is configured (and only necessary categories are selected) prior to signature load, the crash does not occur.

  Workaround: Perform the following steps:

  1. Remove all IPS configuration from the router. 2. Make IPS configuration again (do not load the signatures). 3. Configure "ip ips signature-category" and enable only necessary categories there. 4. Load the signatures by "copy <url> idconf".

  Further Problem Description: It is strongly recommended to load only the BASIC set of signatures for Cisco IOS IPS 5.x.

  According to IPS 5.x documentation, enabling all signatures at the same time is NOT recommended because it can cause memory exhaustion and router crashes:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124t/124t11/ips_v5.htm

  Enabling signature categories prior to signature load ensures that only necessary signatures will be compiled. The documentation link above contains a correct configuration example. Follow this sequence to avoid memory exhaustion.

- CSCsk92135

  Symptoms: Routers with ADSL over POTS card hang on booting Cisco IOS Release 12.4(16.14)T4 and above.

  Conditions: Issue seems to be specific to the ADSL over POTS card.

  Workaround: There is no workaround.

- CSCsk92399

  Symptoms: The router reloads while initiating an ISDN call.

  ```
  ALIGN-1-FATAL message may appear as follows: %ALIGN-1-FATAL: Illegal access to a low
  address 06:54:29 UTC Thu Dec 6 2007 addr=0x9, pc=0x6094E688 , ra=0x609988C0 ,
  sp=0x65A957EC
  ```

  This will crash the router due to a bus error. The crashinfo will report a TLB exception as follows:

  TLB (store) exception, CPU signal 10, PC = 0x4059C548

  Conditions: This symptom is observed on a Cisco router that is configured with ISDN.

  Workaround: There is no workaround.

- CSCsk93241

  Cisco IOS Software Multiprotocol Label Switching (MPLS) Forwarding Infrastructure (MFI) is vulnerable to a Denial of Service (DoS) attack from specially crafted packets. Only the MFI is affected by this vulnerability. Older Label Forwarding Information Base (LFIB) implementation, which is replaced by MFI, is not affected.

  Cisco has released free software updates that address this vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080924-mfi.shtml.

- CSCsk94202

  Symptoms: Cisco GGSN reloads when data is sent through PDP context and if a PDP context is deleted at the same time.

  Conditions: This may happen under certain timing conditions involving the data transfer and PDP deletion events.

  Workaround: There is no workaround.

- CSCsk94226

  Symptoms: PA-MC-2T3-EC interface is not usable.

  Conditions: The interface is configured with Multilink Frame Relay (MFR) encapsulation and soft online insertion and removal (OIR) is done in that PA. Issue is seen only with frame-relay mfr encapsulation and is not seen with HDLC/PPP/ frame-relay encapsulations.

  Workaround: There is no workaround.

- CSCsk94464

  Symptoms: Cisco 1801 and Cisco 1803 routers fail to establish ISDN layer 2 connection with a certain third-party PBX.

  Conditions: Occurs on routers running Cisco IOS Release 12.4(15)T1 and earlier releases.

  Workaround: There is no workaround.

- CSCsk97130

  Symptoms: VXML application causes memory leak

  Conditions: If the calling document and called document of a subdialog share the same root document, the tree structure used for the root document will not be released after the call session is finished.

  Workaround: There is no workaround.

- CSCsk97384

  Symptoms: Abnormally large FreshTime value appears in IVR HTTP client cache entry.

  Conditions: This symptom is observed when a VXML voice browser downloads a file from an HTTP server. If the file was modified very recently, the FreshTime for that file may show up with a very large value.

  Workaround: There is no workaround.

- CSCsk98507

  Symptoms: Router crashes after IPX routing is enabled.

  Conditions: Problem happens only if an interface which has IPX network configuration is deleted after disabling IPX routing.

  Workaround: There is no workaround.

- CSCsl01874

  Symptoms: Cisco IOS configured with the Dynamic Multipoint VPN (DMVPN) feature allows stale tunnel endpoint entries to remain in the system. This occurs even though the Next Hop Resolution Protocol (NHRP) cache entry does not exist.

  Conditions: When a spoke registers with a changed tunnel IP address (overlay address), there will be two overlay addresses mapped to same NBMA address on the hub. As a result when the NHRP mapping for the stale overlay address (old tunnel address) expires on the hub, the tunnel endpoint entry is not deleted, resulting in a stale tunnel endpoint entry.

  Workaround: There is no workaround.

- CSCsl02427

  Symptoms: SIP traffic may not have port range correctly translated when using NAT port map. Destination ports that should be translated into standard SIP port range (16348 - 32768) are instead being translated to port numbers lower than 16384.

  Conditions: Symptom has been observed on pre-release version of Cisco IOS Release 12.4(15)T2. May exist in other 12.4T releases of IOS.

  Workaround: There is no workaround.

- CSCsl10459

  Symptoms: Routers that are running Cisco IOS Release 12.4(13b) and Release 12.4(16) may crash when the **show crypto pki timers** command is executed.

  Conditions: This symptom is observed under a narrow set of conditions. Offending conditions occur when certificates are issued Certificate Distribution Point formatted in URL format. Certain other unknown circumstances must also occur.

  Workaround: Avoid using the **show crypto pki timers** command.

- CSCsl11335

  Symptoms: The number of entries obtained from the "ciscoMvpnBgpMdtUpdateTable" table using the **getmany** command is incorrect

  Conditions: Occurred on a Cisco 7200 router running Cisco IOS version 12.4(17.9)T.

  Workaround: There is no workaround.

- CSCsl11708

  Symptoms: Dialer Cisco Express Forwarding (CEF) with IP Accounting fails with packet counters returning zero i.e 0 packets, 0 bytes for the dialer Interface.

  Conditions: This happens when **ip accounting output-packets** configured on NAS. The NAS is being checked for **show adjacency detail** which returns zero i.e 0 packets, 0 bytes for the dialer Interface.

  Workaround: There is no workaround.

- CSCsl11868

  Symptoms: With IP Cisco Express Forwarding (CEF) enabled, ACL is not denying packets as intended in MPLS scenario. Alternate ping passes with IP CEF enabled through an ACL, even though ping should fail. When IP CEF is disabled, the ACL works as expected.

  Conditions: This is observed on router running Cisco IOS Release 12.4(17.9)T image with CEF enabled.

  Workaround: If possible, disable CEF using the **no ip cef** command. There is no workaround for the MPLS environment.

- CSCsl12441

  Symptoms: After a software upgrade, router has an unnecessary command, **text relay fax rate disable**, added to its "voice service pots" configuration.

  Conditions: Occurs on routers for which "fax rate disable" is configured when you upgrade from Cisco IOS Release 12.3(11)T10 to Cisco IOS Release 12.4(15)T1.

  Workaround: There is no workaround.

- CSCsl13216

  Symptoms: Warm upgrade does not work as expected.

  Conditions: Occurs when you perform a warm upgrade from a small IOS image to a large image.

  Workaround: Use the **reload** command instead of the **reload warm file** *image-path* command to boot the new image.

- CSCsl19590

  Symptoms: An ISR router may crash during start up.

  Conditions: Occurs when USB Flash drives are connected to the router. If drives are removed, there is no crash.

  Workaround: There is no workaround.

- CSCsl20701

  Symptoms: A Cisco IOS router that is configured to run Embedded Event Manager (EEM) Remote Procedure Call (RPC) policies may leak memory when those policies are run.

  Conditions: This only occurs when EEM RPC is configured and an EEM RPC TCL policy is executed.

  Workaround: There is no workaround.

- CSCsl21168

  Symptoms: Router crashes. Prior to the crash, the log file contains numerous messages indicating:

  ```
  SYS-3-CPUHOG: Task is running for (2004)msecs, more than (2000)msecs (2/2),process =
  IP NAT Ager.
  ```

  Conditions: Occurs on a router with NAT enabled.

  Workaround: There is no workaround.

  Additional Details: The fix for this defect caused a new bug: CSCso62511. Ensure you have the fix for CSCso62511 in addition to this defect if you are encountering this problem.

- CSCsl22080

  Symptoms: WebVPN hangs after a few days of working. When this happens, no WebVPN connections are active and no new connections can be established. The **debug ip tcp transaction** command shows **connection queue limit reached: port 443** errors. The **show tcp brief** command displays many sessions in SYNRCVD and TIMEWAIT states. Problem is recovered either by reload or by entering the **clear tcp tcb *** command. There are few stale sessions in CLOSED state left after clearing TCP.

  Conditions: Issue seen in Cisco IOS Release 12.4.15T and Cisco IOS Release 12.4.15T1 when WebVPN is configured. The issue is intermittent and happens after few days or weeks of working.

  Workaround: To restore TCP connectivity, issue **clear tcp tcb *** or reload the router. Note that this will clear all TCP sessions on the router.

- CSCsl24858

Symptoms: Cisco 7200 router with PA-VXC/B may go into "hang" state and fail to respond to console.

Conditions: Occurs on a Cisco 7200 router with PA-VXC/B and configured for active calls over the PA.

Workaround: There is no workaround.

- CSCsl25732

  Symptoms: GPRS tunneling protocol (GTPv1) periodic interim accounting records are not sent out by device.

  Conditions: Occurs when using GTPv1 PDP together with AAA periodic interim accounting configuration.

  Workaround: There is no workaround.

- CSCsl32122

  Symptoms: VPN client users using a certificate to connect to a Catalyst 6000 or Cisco 7600 with VPN blade fail to connect. IPSec negotiation fails during mode configuration.

  Conditions: Conditions are unknown at this time.

  Workaround: Preshared key authenticated VPN clients can connect without problem.

- CSCsl32142

  Symptoms: A router may reload after reporting SYS-3-OVERRUN or SYS-3-BADBLOCK error messages. SYS-2-GETBUF with ‘Bad getbuffer’ error may also be reported.

  Condition: Occurs when PIM auto-RP is configured and IP multicast boundary is enabled with the **filter-autorp** option.

  Workaround: Configure IP multicast boundary without the **filter-autorp** option.

- CSCsl34481

  Symptoms: Router crashes due to IPv6 multicast routing.

  Conditions: This happens after applying multicast routing configurations, and again while unconfiguring.

  Workaround: There is no workaround.

- CSCsl36320

  Symptoms: Router crashes after Network Based Application Recognition (NBAR) configuration has been changed with a command like **ip nbar custom**. The following error message is displayed:

  ```
  %SYS-3-CPUHOG: %SYS-2-WATCHDOG: Process aborted on watchdog timeout
  ```

  Conditions: Occurred on a Cisco 2811 router running the c2800nm-advipservicesk9-mz.124-11.T3.bin image.

  Workaround: There is no workaround.

- CSCsl40687

  Symptoms: Router reloads due to a bus error. This occurs with the following messages:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address 08:32:13 AEST Tue Nov 20 2007
  addr=0xB8, pc=0x40099888 , ra=0x44020000 , sp=0x465870E8
  08:32:13 AEST Tue Nov 20 2007: TLB (store) exception, CPU signal 10, PC = 0x40099888
  -Traceback= 0x40099888 0x402F6358 0x415102F4 0x41510C7C 0x402FF5C4 0x414F1140
  0x402FF7B8 0x41C8B8E0 0x41C8EFC0 0x41C8F064
  0x41C85260 0x421EA0C4 0x421EA224
  ```

  Conditions: This occurs after applying a Modular Quality of Service Command-Line Interface (MQC) class on a PVC.

Workaround: Use frame relay traffic shaping (FRTS) instead of MQC under the PVC.

Further Problem Description:

MQC policy is not a supported configuration for MLPoFR connections. The above configuration is not valid. Currently, the MQC policies are configurable under MLPoFR PVCs and this results in router reload. However, the router should not crash even under those circumstances. This fix prevents MQC QOS policy from being configured on MLPoFR connections at config time when MLP may not yet be active. So, in effect, the config is blocked both if MLP is active or if MLP is just configured.

- CSCsl43035

  Symptoms: Disconnect message received on terminating router does not contain codeset 6.

  Conditions: Occurs with simple tdm-ip to tdm-ip call scenario.

  Workaround: There is no workaround.

- CSCsl44498

  Symptoms: Serial interface (CT1) goes down when attaching a policy with traffic and a class map that has an extended ACL.

  Conditions: Occurred on a Cisco 7200 Router with extended ACL with traffic.

  Workaround: There is no workaround.

- CSCsl47374

  Symptoms: Calls per Second (CPS) was calculated with Standalone LNS and LAC for Cisco IOS Release 12.2SR. The CPS result obtained was compared with CPS results for SB4, XN3 and XD9 images and showed that there was a drop in CPS for Cisco IOS Release 12.2SR.

  Conditions: The symptom is observed when 8000 PPPOX/8000 L2TP sessions were brought up with a single local name configured under VPDN group configuration on LAC Router. It is also observed when 8000 L2TP Tunnels were brought up using different values in Tunnel-Assignment-Id in Radius Profile.

  Workaround: If different local names are configured under VPDN group configuration, the CPS drop will not be observed.

- CSCsl47794

  Symptoms: Cannot configure **queue-limit** inside policy-map of type **queue-threshold**.

  Conditions: Occurs on routers running Cisco IOS Release 12.4 and Cisco IOS Release 12.4T.

  Workaround: There is no workaround.

- CSCsl51353

  Symptoms: All packets are dropped when a policy is configured on an ATM PVC.

  Conditions: Occurs when shaping is configured in the policy-map.

  Workaround: There is no workaround.

- CSCsl52594

  Symptoms: When two routers are configured to form an IPv6 EIGRP adjacency, attempts to ping one of the loopback IPv6 addresses from the neighbor fails with the following error:

  No valid source address for destination

  Conditions: Occurs on routers running Cisco IOS Release 12.4T.

  Workaround: There are two workarounds:

1. Disable IPv6 Cisco Express Forwarding (CEF) 2. Enter the **clear ipv6 eigrp neighbor** command

- CSCsl53327

  Symptoms: Phone range is shown incorrectly under telephony-service. Phones may not register more than 12.

  Condition: The router configuration "max-ephones" is not set to proper value for 16 users and 48 users SKU of uc520.

  Workaround: Under ROMMon, set the variable as FLU=.

- CSCsl56547

  Symptoms: While getting the output of the **show mls cef ipv6 vrf <id>** for a valid VPN routing/forwarding (VRF), the following error message is seen: % vrf v6 doesn't exist.

  Conditions: This issue is seen only for IPv6 VRF. If both IPv4 and IPv6 are configured, then this problem does not occur.

  Workaround: There are two scenarios to reproduce this problem: 1 Configure VRF, save the configuration and reload the router. To workaround, configure the global **vtp mode transparent** command. 2 Configure VRF and toggle IPv6 unicast-routing. There is no workaround for this scenario.

  Further Problem Description: Doing a SSO switchover can also be used as workaround.

- CSCsl56934

  Symptoms: "ip summary-address rip" is configured on an interface, but the summary address is not advertised by RIP.

  Conditions: Occurs, after the same interface was deleted and re-created with "ip summary-address rip" configured on it (e.g Virtual Access interface or Loopback). Originally observed when connecting and disconnecting virtual access sessions. The issue is platform-independent.

  Workaround: There is no workaround.

- CSCsl57469

  Symptoms: Cisco Unified CallManager Express (CME) B-ACD reports incorrect statistics. Here is an example of the queue stats that are wrong. Look at total calls per agent and total calls answered by agents >

  Conditions: CME reports incorrect "total call per agent" and "total calls answered by agents" as shown below:

```
Tue 09:00 - 10:00
Max Agents: 4
Min Agents: 3
Per agent statistics: Agent: 6353461
From Queue: Total Calls Answered : 6
Average Time in Call (secs) : 151
Longest Time in Call (secs) : 372
Total Calls on Hold : 3:
Average Hold Time (secs) : 48
Longest Hold Time (secs) : 122
Agent: 6353462 From Queue:
Total Calls Answered : 8
Average Time in Call (secs) : 85
Longest Time in Call (secs) : 140
Total Calls on Hold : 5:
Average Hold Time (secs) : 54
Longest Hold Time (secs) : 91
Agent: 6353463
From Queue:
```

```
Total Calls Answered : 7
Average Time in Call (secs) : 191
Longest Time in Call (secs) : 465
Total Calls on Hold : 1:
Average Hold Time (secs) : 168
Longest Hold Time (secs) : 168
Agent: 6353464
From Queue:
Total Calls Answered : 8
Average Time in Call (secs) : 165
Longest Time in Call (secs) : 319
Total Calls on Hold : 2:
Average Hold Time (secs) : 23
Longest Hold Time (secs) : 32
Queue related statistics:
Total calls presented to the queue: 42
Calls answered by agents: 40
Number of calls in the queue: 0
Average time to answer (secs): 18
Longest time to answer (secs): 92
Number of abandoned calls: 2
```

Workaround: There is no workaround.

- CSCsl58673

  Symptoms: A Cisco router running IOS or IOS Software modularity may not allow telnet connections when the device is configured to run an Embedded Event Manager(EEM) policy that contains actions that use the CLI. In addition CLI actions may not correctly wait for the prompt before going on to the next action or may not detect the prompt.

  Conditions: The symptom of not allowing telnet connections can occur when the device has been configured with an EEM policy to run a CLI command. When that policy exits the input buffer of the VTY way not be cleaned up properly so the next connection opened on that VTY may simply show three user name prompts and exit.

  The symptom of the CLI actions not waiting for the prompt can occur when using the CLI actions on a low-end system with a slower CPU. The system incorrectly checks for the prompt only 10 times and then assumes the prompt is blank instead of waiting for a valid prompt.

  The symptom of CLI actions not matching against the prompt properly can occur if the prompt has been changed from the default.

  When multiple EEM policies are triggered, they can use up all available VTY lines.

  Workaround: There is no workaround.

  Further Problem Description: If no VTY lines are available, the user will not be able to Telnet into the machine. Console access will not be affected.

  This only affects customers using the Embedded Event Manager (EEM). It affects EEM applets and policies which interact with the CLI library. This was only seen on the MCP platform however.

  Cisco IOS Release 12.2(33)SRA is not affected.

  Cisco IOS Release 12.2(33)SRB1 and Cisco IOS Release 12.2(33)SRB2 are not affected. But Cisco IOS Release 12.2(33)SRB3 is affected.

  Cisco IOS Release 12.2(33)SRC1 is not affected.

  Cisco IOS Release 12.2(33)SXF is not affected.

  Cisco IOS Release 12.2(33)SXH1 is affected. Cisco IOS Release 12.2(33)SXH2 is not affected.

- CSCsl58881

  Symptoms: A Cisco 2950 may crash unexpectedly.

Conditions: Occurs under the following scenario: - Cisco Discovery Protocol (CDP) is enabled globally. - The Cisco 2950 is connected to Cisco IP Phones. - A third party power-over-Ethernet adapter powers the IP Phones.

Workaround: Disable CDP.

- CSCsl61416

  Symptoms: Certain prompts will not play properly. Dead air is heard and call disconnects.

  Conditions: Occurs on a Cisco AS5350 acting as a VXML gateway in an IPCC environment and running Cisco IOS Release 12.4(7)b using streaming prompts.

  Workaround: Turn off streaming mode. Reloading the gateway temporarily fixes the issue.

- CSCsl62609

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS that can be exploited remotely to trigger a memory leak or to cause a reload of the Cisco IOS device.

  Cisco has released free software updates that address these vulnerabilities. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities addressed 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, if administrators do not require the Cisco IOS device to provide voice over IP services.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080924-sip.shtml.

- CSCsl63212

  Symptoms: L2TP network server (LNS) router crashes while establishing virtual private dial-up network (VPDN) and shutting down client interface.

  Conditions: Occurs while making call from client to LNS with specific configurations.

  Workaround: There is no workaround.

- CSCsl63494

  Symptoms: AAA server does not count active user sessions correctly. User authentication may be denied by the AAA server because max session limit has been reached.

  Conditions: This may occur with AAA authentication, when max session limit is configured on Cisco Secure ACS server (may happen with other AAA servers too). When user initiates X.25,ssh,rsh,rlogin or telnet sessions and later disconnects them, AAA server does not decrement active sessions counter due to wrong attributes present in the accounting records sent by the device. Eventually, the misbehaving counter may reach max session limit, and user will be denied a login.

  Workaround: Removing max session limit can be considered.

- CSCsl67527

  Symptoms: HTML pages inside a TAR file fail to load. This affects web applications such as Security Device Manager (SDM). If SDM is installed in a router's flash, the user is unable to invoke the HTML page that is archived inside the TAR. The SDM application fails to launch, and the user will receive a "page not found" error.

  Conditions: This symptom is observed only when files are contained in a TAR file. All other HTML files can be loaded successfully. For the Cisco IOS Release 12.4 train, the problem was introduced in Cisco IOS Release 12.4(17.6) and fixed in Cisco IOS Release 12.4(18.11).

  Workaround: There is no workaround.

- CSCsl67783

Symptoms: On certain router platforms, if multiple subinterfaces are configured on a Fast Ethernet interface and if these subinterfaces are configured for Hot Standby Routing Protocol (HSRP) and the same Virtual MAC address (VMAC), then whenever the router becomes HSRP standby for at least one of these subinterfaces, the router drops all traffic that is directed to the same VMAC on other subinterfaces.

The following is a sample configuration that would be exposed to this issue:

```
! interface FastEthernet2/0.4 encapsulation dot1Q 4 ip address 192.168.12.2
255.255.255.0 standby 102 ip 192.168.12.254 standby 102 priority 210 standby 102
preempt standby 102 mac-address 0200.0000.7700 ! interface FastEthernet2/0.5
encapsulation dot1Q 5 ip address 192.168.13.2 255.255.255.0 standby 2 ip
192.168.13.254 standby 2 priority 210 standby 2 preempt standby 2 mac-address
0200.0000.7700 !
```

Conditions: This symptom is observed on Cisco 7200/NPE-400 platform on the motherboard and Fast Ethernet port adapters.

Workaround: The problem does not occur if different VMAC addresses are configured on different subinterfaces or if static VMACs are not used. If the problem is encountered in a production environment, a quick workaround is to shut down the Fast Ethernet interface of the other router in order to make one router HSRP active in all VLANs.

- CSCsl70143

  Symptoms: Under heavy traffic, ISDN calls may be rejected due to high CPU usage with the following messages seen in the log (with tracebacks):

  %IVR-3-LOW_CPU_RESOURCE: IVR: System experiencing high cpu utilization (98/100). Call (callID=23524) is rejected.

  %SYS-3-CPUHOG: Task is running for (2000)msecs, more than (2000)msecs (32/18),process = ISDN.

  Conditions: This problem occurs only under heavy traffic.

  Workaround: There is no workaround.

- CSCsl72774

  Symptoms: A router may run out of memory and fail malloc due to a memory leak.

  Conditions: This problem only occurs on distributed platforms (like the Cisco 7600/Catalyst 6500) when the CEF consistency checkers have been enabled. By default, the CEF consistency checkers are disabled. When the CEF consistency checkers are turned on, memory is leaked on the RP, SP and line cards.

  If you want to use the consistency checkers, then do so for only short periods of time. For example, use the consistency checkers while diagnosing network problems.

  Workaround: Disable the CEF consistency checkers by using the following commands:

  no cef table consistency-check ipv4 no cef table consistency-check ipv6

- CSCsl74712

  Symptoms: When an existing Virtual Router Redundancy Protocol (VRRP) tracking entry is re-entered into the configuration of the active RP, the standby RP automatically resets.

  Conditions: This problem only occurs after the following sequence of configuration events:

  - VRRP is configured to track an existing tracking object.
  - The existing tracking object is removed from the global tracking configuration.
  - The standby is initiated and establishes the full STANDBY state.
  - The user re-enters the VRRP command to track the previously removed tracking object.

  - At this point the Standby RP will reset due to PRC mismatch.

  Workaround: During normal configuration it is unlikely that the above scenario will be repeated. Crucially the workaround for this defect is to make sure that when VRRP is using a tracked object, the global tracking config for that object must exist at all times. The global tracking config for that object can be removed as long as the tracking entry in VRRP is removed first.

- CSCsl76647

  Symptoms: The **clear crypto isakmp** command deletes SA with connection ID from 0 to 32766. The SA created with the VPN SPA has a connection ID higher than 32766, and cannot be singularly deleted.

  Conditions: This symptom occurs when SA is established using the VPN SPA.

  Workaround: There is no workaround.

- CSCsl78850

  Symptoms: When the WAN is restored between an MGCP/SRST gateway and CallManager, the MGCP gateway intermittently fails to register back with CallManager.

  Conditions: Connectivity to the CallManager from the gateway is stopped. When the gateway goes in SRST, a PSTN call is placed to a phone that registers with the gateway. WAN connectivity is then restored. MGCP has one primary call agent and two redundant hosts configured.

  Workaround: Reload the gateway.

  Further Problem Description: When the gateway is in this "stuck" state of not registering with the CallManager, if "no ccm-manager mgcp" is configured, it does not take effect, and "no ccm-manager redundant-host... " also does not take effect. The following error message is displayed:

  ```
  cmapp_service_emptying_redun_hostlist: Error: cannot execute CCM host change -- must
  configure again!
  ```

- CSCsl79588

  Symptoms: Router running Cisco IOS may crash with a bus error.

  Conditions: Occurs when a Cisco router is configured to stream music on hold (MoH) from a .wav file with a header longer than 256 bytes.

  Workaround: Do not use .wav files for MoH. Use only .au files.

- CSCsl80887

  Symptoms: The router may crash and there is high CPU usage if the Routing Information Protocol's (RIP) minimum update interval is configured to zero.

  Conditions: The symptom may be observed on a Cisco router using RIP version 2 process, with the timer values set to 0 1 0 1.

  Workaround: Do not configure RIP's minimum update interval to zero.

- CSCsl81011

  Symptoms: Hierarchical queuing framework (HQF) not cleared even after removing the service policy from the interface.

  Conditions: HQF hierarchy not cleared after entering the **no service-policy out <pname>**command. This is seen with Optical Services Module (OSM).

  Workaround: There is no workaround.

- CSCsl81170

Symptoms: When adding a static NAT translation, a permanent ARP entry is added. When configuring multiple translations for the same address and removing one, the ARP entry is removed even though there may be a NAT translation that still requires it.

Conditions: The symptoms are observed when there are multiple translations with the same addresses, for example: ip nat inside source static tcp 192.168.2.1 20 192.168.4.5 20 extendable ip nat inside source static tcp 192.168.2.1 21 192.168.4.5 21 extendable

Workaround: Remove and re-add the NAT configuration lines for the IP address.

- CSCsl82024

  Symptoms: AnyConnect does not work on Cisco 870 and Cisco 1800 routers. The client gets downloaded, and dialog states that the connection has been established. Nevertheless, the IP address has not been assigned, and the connection is actually not established. WebVPN works fine, as well as configuration with SCV.

  Conditions: Occurs when SSL VPN is configured with AnyConnect on Cisco 871 and Cisco 1800 routers running Cisco IOS Release 12.4(15)T1.

  Workaround: Either disable hardware crypto and use only the software crypto, or change the SSL encryption in the "webvpn gateway" configuration as follows.:

  webvpn gateway gateway_1 ssl encryption rc4-md5

- CSCsl82563

  Symptoms: Immediately after a GM registers with the KS, it will report a traceback and crash with:

  %ALIGN-1-FATAL: Corrupted program counter

  Conditions: Occurs on a router running an internal version of 12.4T.

  Workaround: There is no workaround.

- CSCsl83415

  Symptoms: After executing the following CLI commands (steps mentioned alphabetically) via a script (not reproducible manually), the router sometimes crashes:

  ```
  Test10 : --------- a. clear ip bgp 10.0.101.46 ipv4 multicast out b. clear ip bgp
  10.0.101.47 ipv4 multicast out
  Test 1: -------- c. show ip bgp ipv4 multicast nei 10.0.101.2 d. show ip bgp ipv4
  multicast [<prefix>] e. config terminal
  ```

  The crash does not happen for each of the following cases:

  1. If the same CLI is cut-paste manually, there is no crash.

  2. If the **clear cli** command is not executed, there is no crash.

  3. If the **config terminal** command is not entered, there is no crash.

  Conditions: The symptom occurs after executing the above CLI.

  Workaround: There is no workaround.

- CSCsl87400

  Symptoms: H323 setup message is malformed after NAT translation

  Conditions: Setup message includes the neededFeatures, desiredFeatures, supportedFeatures extensions.

  Workaround: Do not use the extensions listed above.

- CSCsl87404

  Symptoms: L2TP tunnels are not getting established.

Conditions: Occurs on a router running Cisco IOS Release 12.4(15)T2.

Workaround: There is no workaround.

- CSCsl88956

  Symptoms: Cisco 2800 and 3800 series routers will lose the running configuration and startup configuration when reloaded.

  Conditions: Occurs when the last physical sector of NVRAM, which is shared by NVRAM and licensing subsystem, is corrupted. Primary NVRAM is not restored properly.

  Workaround: There is no workaround.

- CSCsl90187

  Symptoms: Low memory leak may occur on VoIP gateway in VTSP process, which may cause router to reload.

  Conditions: The issue is specific to the C549 DSPs on Cisco 3700 series routers. The leak occurs when a call is disconnected due to non-availability of the circuit (cause code 0x22).

  Workaround: There is no workaround.

- CSCsl94410

  Symptoms: CPU hog condition occurs because of stressful BGP configuration.

  Conditions: Occurs in Cisco IOS releases in which CSCsj17879.

  Workaround: There is no workaround.

- CSCsl95431

  Symptoms: A router may reload when malformed packets are sent to the TFTP UDP port.

  Conditions: This symptom is observed when malformed traffic is sent to the router's TFTP UDP port 69 (TFTP). The TFTP server port must be listening within IOS.

  TFTP port 69 is opened in Cisco IOS under the following circumstances:

  * TFTP-Server is explicitly enabled with the command: **tftp-server** *filename*.

  For further information on the TFTP Server functionality, see:

  http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_file-transfer_ps6350_TSD_Products_Configuration_Guide_Chapter.html#wp1000933

  * E-Phones are configured If Cisco Unified Communications Express (CME) is being used and ephones are configured port UDP 69 (TFTP) will be opened within Cisco IOS. If the configuration contains **ephone-dn** *arguments* then port 69 is opened.

  For further information on the CME ephone functionality, see:

  http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/admin/configuration/guide/cmebasic.html#wp1013086

  Workaround: There is no workaround to this Cisco Bug ID, however the following mitigation may be suitable for some customer environments:

  Infrastructure ACLs (iACL): Although it is often difficult to block traffic transiting your network, it is possible to identify traffic which should never be allowed to target your infrastructure devices and block that traffic at the border of your network. 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 shown below should be included as part of the deployed infrastructure access-list which will protect all devices with IP addresses in the infrastructure IP address range:

```
!--- Permit TFTP (UDP port 69) packets !--- from trusted hosts destined to
infrastructure addresses.
access-list 150 permit udp TRUSTED_HOSTS MASK INFRASTRUCTURE_ADDRESSES MASK eq tftp
!--- Deny TFTP (UDP port 69) packets !--- from all other sources destined to
infrastructure addresses.
access-list 150 deny udp any INFRASTRUCTURE_ADDRESSES MASK eq tftp
!--- 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
interface serial 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. This white paper can be obtained here:

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

- CSCsl96254

  Symptoms: If an EIGRP distribute-list applied to an interface allows a route, the route will be installed into the routing table without first checking to see if the global distribute-list allows it as well. All platforms are affected.

  access-list 1 permit any access-list 2 deny any

  router eigrp 1 network 192.168.1.0 0.0.0.255 distribute-list 1 in FastEthernet0/0 distribute-list 2 in no auto-summary

  The above configuration should deny all routes by virtue of access-list 2. Instead, all routes are allowed per ACL 1.

  Conditions: Running EIGRP with interface distribute lists and a global distribute list. All platforms are affected.

  Workaround: Currently the only workaround is to apply the global distribute list to each interface distribute list as well.

- CSCsl99275

  Symptoms: High CPU can be seen on Cisco AS5400XM after given uptime.

  Conditions: Occurs after 2-3 weeks uptime. CPU usage increases because of "Background Loade" process.

  Workaround: Reload the access server.

- CSCsl99883

  Symptoms: The X.25 PVC experiences window closed on both the sides.

  Conditions: The problem is seen under heavy traffic conditions. The testing scenario passes 1000 packets containing 2000 bytes of data.

  Workaround: Reset the connection.

- CSCsm00496

  Symptoms: When v6 RP mappings with the same group range but with different mode (for example, bidir and sparse) are advertised to a bootstrap router (BSR), only one of the mappings is installed by the BSR.

  Conditions: When multiple v6 RP mappings with the same group range (for example, bidir and sparse) as shown below:

ipv6 pim bsr candidate rp 30::1:1:3 group-list acc_grp1 ipv6 pim bsr candidate rp 30::1:1:3 group-list acc_grp1 bidir are sent to a BSR router, the router installs only one of the mappings. The bidir mapping is installed in the above example.

Workaround: There is no workaround.

- CSCsm01126

  Symptoms: The standby fails to come up in SSO. The following message is seen on the active:

  %FILESYS-4-RCSF: Active running config access failure (0) <file size>

  Conditions: This symptom is observed when the router has a configuration greater than 0.5 megabytes.

  Workaround: There is no workaround.

- CSCsm04442

  Symptoms: Delete an interface which has ip summary-address rip configured. The router crashes.

  Conditions: In the scenario where different summary addresses are configured for different interfaces, if we delete an interface that has a summary-address configuration which is the last one for that summary-address that it leads to.

  Workaround: Remove the **ip summary-address rip** configuration from an interface which is going to be deleted.

- CSCsm07798

  Symptoms: Call forwarding fails when the call is made between phones behind two secure Cisco Unified CallManager Express (CME) routers.

  Conditions: Call forwarding between two phone fails when the platform is configured for secure CME, with media encryption and signaling.

  Workaround: There is no workaround.

- CSCsm08010

  Symptoms: A Cisco IOS VG224 voice gateway may reload unexpectedly if an FXS voice port configured with the **caller-id enable** command, receives a call where the calling number (ANI) is greater than 32 digits.

  Conditions: The symptom is observed when caller-id is enabled and the ANI is greater than 32 characters in length.

  Workaround: The workaround is to disable caller-id in the FXS voice port and restrict the ANI to less than 32 digits.

- CSCsm08030

  Symptoms: A router may crash while parsing "x28 profile <profile name>". This occurs when x28 mode is configured. The crashinfo file will show: %SYS-2-FREEFREE: Attempted to free unassigned memory at [...]

  Conditions: This symptom is observed on a Cisco AS5400 gateway that is running Cisco IOS Release 12.4(1c) and Release 12.4(18).

  Workaround: There is no workaround.

- CSCsm08085

  Symptoms: During performance testing, expected throughput is not achieved when doing QoS marking based on ACL classification.

  Conditions: Occurred on a router running Cisco IOS Release 12.4(15)T.

Workaround: There is no workaround.

- CSCsm08291

  Symptoms: Virtual access interfaces flap, and the following error message is displayed: %SYS-2-BADSHARE: Bad refcount in datagram_done.

  Conditions: Occurs on a Cisco 7206VXR with NPE-G2 and running Cisco IOS Release 12.4.(11)T1.

  Workaround: There is no workaround.

- CSCsm16309

  Symptoms: Crash in Bidirectional Forwarding Detection (BFD) subsystem may occur after last BFD session is removed.

  Conditions: Occurs after all BFD sessions are removed and the BFD finishes cleaning up data structures.

  Workaround: There is no workaround.

- CSCsm17110

  Symptoms: When setting the ‘FlipAddr’ attribute in an IPS signature, one expects the attacker and victim TCP/IP addresses to be swapped. This is not occurring as expected and signature actions will be created against the improper TCP/IP address.

  Conditions: Edit an IPS signature and set the ‘FlipAddr’ attribute to True. Receive traffic that should cause the edited signature to fire. If a deny action is configured, the destination/victim TCP/IP address will be used instead of the expected source/attacker TCP/IP address.

  Workaround: There is no workaround.

- CSCsm17314

  Symptoms: A router may experience a large buffer leak

  Conditions: Occurs when WebVPN is configured.

  Workaround: There is no workaround.

- CSCsm17625

  Symptoms: Policy attached to zone-pair with tunnel interface as source and self-zone as destination may not match traffic.

  Conditions: Occurs when firewall policy is applied to a zone-pair which has tunnel interface as source and self-zone as destination.

  Workaround: There is no workaround.

- CSCsm17711

  Symptoms: The **rmdir** command deletes a directory which has files and subdirectories in it. This behavior is not valid.

  Conditions: The symptom can be observed when using the **rmdir** command with a USBFLASH filesystem.

  Workaround: There is no workaround.

- CSCsm17767

  Symptoms: On a gateway configured for ISDN Non-Facility Associated Signaling (NFAS) with a primary and backup D channel, both the primary and backup D channel interfaces may be marked "OUT OF SERVICE" if the gateway sends the first "in-service" message during a D channel switchover.

Conditions: This only occurs when the gateway sends the first ISDN service messaging indicating that it is bringing the backup D channel in service. If the peer sends the message first, the switchover is completed successfully.

Workaround: There is no workaround.

- CSCsm17879

  Symptoms: After putting the onboard GE0/0-1 interfaces into promiscuous mode, they still will not accept packets with destination MAC other than the broadcast and the interface MAC.

  Conditions: This affects the onboard GE interfaces only.

  Workaround: Use FE/GE ports from a module to achieve this, if available.

- CSCsm19892

  Symptoms: Router crashes when WebVPN gateway is configured, used, and then unconfigured.

  Conditions: Occurs on a router running Cisco IOS Release 12.4(15)T2.

  Workaround: No workaround. Possible workaround for router to function is do not remove the configuration.

- CSCsm20461

  Symptoms: In an IPv6-over-IPv4 MGRE tunnel, disabling IPv6 Cisco Express Forwarding (CEF) without disabling IPv4 CEF results in dropped packets after decryption. Enabling **debug crypto engine packet** on the router helps verify the packet drops after decryption.

  Conditions: The bug is seen if IPv6 CEF is disabled but IPv4 CEF enabled and when tunnel protection is enabled on the MGRE interface.

  Workaround: If IPv6 CEF is disabled, disable IPv4 CEF also.

- CSCsm20994

  Symptoms: Kron occurrences are not rescheduled properly when the clock is set near the end of a calendar year.

  Conditions: A kron occurrence is scheduled daily or hourly. The clock is reset near the end of the year such that the next occurrence of the kron policy would happen in the next year.

  Workaround: After clock reset, remove/restore kron occurrences to cause them to be scheduled properly.

- CSCsm23764

  Symptoms: A device keeps reloading every 50 minutes.

  Conditions: The issue will occur only if the standby RP gets reloaded while CEF is part-way through synching initial data to the standby RP before standby hot state is reached in SSO mode.

  Trigger: Removal or reload of standby before CEF initial synch is complete.

  Impact: This issue affects operations.

  Workaround: Reload the active PRE if this issue occurs.

- CSCsm26130

  Symptoms: When removing a subinterface from the configuration that contains an IP address that falls into the major net of the static route, the static route is no longer injected into the BGP table. Since the route is not in the BGP table, it is not advertised to any peers.

  Conditions: This symptom is observed with auto-summary enabled in BGP. A static summary route is configured to null0 and is injected into the BGP table with a network statement.

  Workaround: There are four possible workarounds:

1) Use an "aggregate-address" configuration instead of the static route to generate the summary. 2) Remove auto-summary from the BGP process. 3) Enter the **clear ip bgp *** command. 4) Remove and reconfigure the BGP network statement for the summary route.

- CSCsm26610

  Symptoms: Router with QoS policer applied on the physical interface crashed after traffic starts. The crash causes subsequent crashes even after router is reloaded and when traffic rate is very low.

  Conditions: Occurs when 1000 IPSec tunnels are built on the same physical interface configured with the policer. This is specific to Cisco 7200 routers with NPE-G2 processors. This issue is not seen with cisco 7200s with NPE-G1s or NPE-400s.

  Workaround: There is no workaround.

- CSCsm27071

  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/warp/public/707/cisco-sa-20090325-ip.shtml

- CSCsm27467

  Symptoms: When using a kron routine to automatically copy configuration data using SCP causes the switch to crash.

  Workaround: Perform SCP operations manually.

- CSCsm27726

  Symptoms: After overwriting DHCP pool and client pool, status of client is IDLE.

  Conditions: Occurs on Cisco routers running a pre-release version of Cisco IOS Release 12.4(17b).

  Workaround: There is no workaround.

- CSCsm27943

  Symptoms: When **dlsw timer explorer-wait-time** is set, Ethernet redundancy could not establish DLSW circuit sometimes with the following message in the debug:

  ```
  Jan 15 15:32:22.643 JST: DLSW-ER:(CSM):startdl_pend timer expired for transparent
  circuit
  ```

  Conditions: The symptom only occurs when the router is configured for **dlsw timer explorer-wait-time** with DLSw Ethernet Redundancy and **dlsw transparent switch- support**.

  Workaround: There is no workaround.

- CSCsm27958

  Symptoms: After upgrading a Cisco 7600 to Cisco IOS Release 12.2(33)SRC, SSO does not come up and router stays in RPR.

  Conditions: Occurs only if the **passive-interface default** command is configured under OSPF.

  Workaround: After upgrade, unconfigure and configure again the **passive-interface default**.

- CSCsm27979

  Symptoms: A router crashes with "Address Error (load or instruction fetch) exception" when the **show ip vrf** *vrf-name* command is used.

  Conditions: On one vty session, enter the **show ip route vrf** *vrf-name* command and leave it in the "more" condition. From other user interface session, go to configuration mode, and then enter the **no ip vrf** *vrf-name* command using the same VRF name. After at least 5 minutes, the router will crash after hitting the any key on the session that is doing the **show ip vrf** command.

  Workaround: Make sure that there is no **show ip route vrf** command pending before entering the **no ip vrf** command.

- CSCsm28649

  Symptoms: P-IP GW acting as a SBC to route SIP traffic does not handle SIP REFER properly if configured to handle the SIP REFER locally.

  Conditions: Occurs on a Cisco AS5400Xm configured as an IP-IP gateway to route traffic from a SIP trunk to the MeetingPlace network. By default it forwards the REFER towards the other peer (SIP trunk) which is not supported by the peer. However if configured to handle the SIP REFER locally (by adding a **no supplementary-service sip refer** in the voice service voip section), then it:

  1. Truncates the called number received in the Refer-to header up to the point where it sees a non-numeric character 2. Routes the corresponding Invite to the wrong host: a) It either sends it to the same host from where the REFER was received OR b) If a dial-peer is defined for the called/transfer number pattern, then it uses the destination in this dial-peer

  This causes RSNA transfers in the MeetingPlace environment involving multiple MeetingPlace servers to fail.

  Workaround: There is no workaround.

- CSCsm30569

  Symptoms: Packet is not being fragmented when packet size is greater than IPSEC tunnel MTU.

  Conditions: This issue is seen on routers running Cisco IOS Release 12.4T when IPSec is configured and Cisco Express Forwarding (CEF) is enabled. When CEF is disabled this issue is not seen.

  It occurs when packet size is greater than IPSec tunnel MTU. Packet is not being fragmented, however traffic is passing successfully.

  Workaround: There is no workaround.

- CSCsm32130

  Symptoms: Router crashes while performing simultaneous operation in vc-class.

  Conditions: Occurs on a Cisco 7200 running an internal version of Cisco IOS Release 12.4T. This may happen when the router is accessed from multiple terminals simultaneously, configuring the **vc-class atm** <*WORD*> command.

  Workaround: Avoid simultaneous operation from multiple Telnet sessions on this configuration.

- CSCsm34361

  Symptoms: TCP ports may not show open as required during port scanning using NMAP.

  Conditions: This symptom is observed on a Cisco 7200 router.

  Workaround: There is no workaround.

- CSCsm34479

  Symptoms: The **Ping ethernet** command from customer edge router to remote MMPID of Metro Ethernet Ports is not successful.

Conditions: Occurs when Ethernet CFM is configured in all routers.

Workaround: There is no workaround.

- CSCsm34632

  Symptoms: PPTP connection does not get established properly. Users are stuck in authentication phase

  Conditions: Occurs when PPTP server is behind a NAT router configured with a static NAT entry.

  Workaround: There is no workaround.

- CSCsm36500

  Symptoms: Tracebacks are seen. These tracebacks have no functional impact.

  Conditions: Occurs on after online insertion and removal (OIR) of the 5x1 GE SPA of the SIP-600 on which multiple subinterfaces with IPv6 address have been created. This is a cosmetic issue and has no functional impact. The issue will eventually correct itself.

  Workaround: There is no workaround.

- CSCsm37058

  Symptoms: A Cisco 3800 router repeatedly reloads upon boot up.

  Conditions: Occurs if the IOS software has got fix for CSCsk32095 and NM-1FE-FX-V2 is installed.

  Workaround: There is no workaround.

- CSCsm43146

  Symptoms: Initial unexpected reload occurred a week after conversion from SIP-NOTIFY/2833 to sip-kpml based DTMF.

  Conditions: Occurs on a Cisco AS5400 running Cisco IOS Release 12.4(9)T3. Also occurred after the upgrade to Cisco IOS Release 12.4(15)T1.

  Workaround: Avoid sip-kpml based DTMF.

- CSCsm44620

  Symptoms: Multicast tunnel not coming up after RPM change. A misconfiguration with overlapping networks causes the join to be rejected. This can be seen on the PIM neighbor list.

  Conditions: There is a problem related to one of the hub card in rpm-xf.10 in forwarding PIM traffic from 2 PEs (rpm-xf.13 & rpm-xf.11). After RP migration from AVICI to CRS we found that tunnels from PE in slot 13 were not coming up. PE in slot 13 was in consistently in registering mode. PE was not coming out of registering mode which was preventing the tunnels from coming up. For PE to come out of registering mode S,G state should be built from new RP down to PE. At this stage the CRS (RP) showed that S,G tree was establish at the RP. S,G tree was OK all the way down from CRS to the last hop (P in slot 10) connecting to the slot 13 PE. The P router in slot 10, which is directly connected to PE, showed that S,G state was established and PE facing interface was in OIL. But there were couple of discrepancies on the P in slot 10. There were no flags set on this P for the mroute of PE. In addition, we found that PE was not receiving any PIM traffic from the P in slot 10. This led to suspicion that although the P showed the correct S,G and OIL but is still not able to forward traffic to the PE. And this could be the reason for PE to remain in registering mode hence preventing the tunnels from coming up.

  Workaround: Remove the following configurations:

  a. rpm-xfh10-z135 - shut & remove interface Switch1.4073

  b. rpm-xfh09-z134 - shut & remove interface Switch1.4073

c. rpm-xfp11-l172 - remove interface Switch1.3172

d. rpm-xfp13-z074 - remove interface Switch1.4074

e. rpm-xfp04-l171 - remove interface Switch1.3171

- CSCsm44792

  Symptoms: The **input gain auto-control -9** command is added automatically to the voice-port configuration. Additionally, this command cannot be removed with the **no input gain auto-control -9** command.

  Conditions: This issue is seen after upgrading router from Cisco IOS Release 12.4(6)T6 or Cisco IOS Release 12.5(15)T1 to Cisco IOS Release 12.(4)15XY.

  Workaround: There is no workaround.

- CSCsm45950

  Symptoms: A BOOTP client does not receive a DHCPOFFER message from the server.

  Conditions: This symptom is observed in Cisco routers that are loaded with Cisco IOS Release 12.5(0.11).

  Workaround: There is no workaround.

- CSCsm46114

  Symptoms: Applications requiring ALG processing (FTP,DNS,H.323) do not go through NAT NVI.

  Conditions: - NAT NVI is configured on one PE to provide access to Internet via packet leaking configuration - Traffic is initiated from CE connected to another PE - Traffic reaches PE/NAT through the VPN across MPLS cloud

  Topology is as follows: CE---PE----MPLS----PE/NAT----Internet

  Workaround: There is no workaround.

  Further Problem Description: This impacts all process-switched packets (not only packets requiring ALG processing)

- CSCsm46227

  Symptoms: Cisco 3845 may crash when there is an incoming trunk call.

  Conditions: Occurs if the shared trunk DN is monitored by a FXO port and it is call-forwarded to another trunk DN with "call-forward all".

  Workaround: There is no workaround.

- CSCsm47916

  Symptoms: Memory fragmentation and tracebacks occur after an uptime of 10 days of handling calls related to AA, ICD, and conference.

  Conditions: This is seen on a Cisco 1861 configured for Cisco Unified CallManager Express (CME) and interacting with Unified Contact Center Express (UCCX).

  Workaround: There is no workaround.

- CSCsm48415

  Symptoms: Cisco Customer Voice Portal (CVP) does not release the port if a user hangs up during database look up.

  Conditions: Occurs with the following software configurations: - CVP 3.0 and Cisco IOS Release 12.4.(3g) - CVP 4.1 and Cisco IOS Release 12.4(15)T

  Workaround: There is no workaround.

- CSCsm49143

  Symptoms: Extended ping parameters will not work for IPv6 source address if a VPN routing/forwarding (VRF) was specified on the initial command line.

  Conditions: The conditions to hit this bugs are: - Using the ping command with a VRF and a source address and, - specifying the source address via extended ping parameters rather that command line.

  Workaround: Use the command line to specify the source address.

- CSCsm50498

  Symptoms: During normal operation of Gateway Load Balancing Protocol (GLBP), when state changes from active to listen, the router stops forwarding traffic destined to the virtual MAC. Router still responds to the interface MAC.

  Conditions: Occurs on Cisco 1700 routers running Cisco IOS Release 12.4.

  Workaround: There is no workaround.

- CSCsm51299

  Symptoms: CSCsl27236 did not catch all of the areas needed to be fixed due to code divergence.

  Conditions: The symptoms can be observed under stress conditions and when ipsec-isakmp is enabled.

  Workaround: There is no workaround.

- CSCsm53996

  Symptoms: Router crashes while unconfiguring IP SLA RTP.

  Conditions: The issue is seen only when very large number of RTP operations (1000) are configured.

  Workaround: There is no workaround.

- CSCsm55045

  Symptoms: A Cisco router configured with Call Manager Express (CME) may reload due to point to illegal deallocation of unassigned/in-use memory.

  Conditions: Occurs when CME is enabled.

  Workaround: There is no workaround.

- CSCsm55553

  Symptoms: A continuous ringback tone is heard at the calling side even after the off-hook of the called side.

  Conditions: This symptom is observed on an MGCP endpoint using the LCS package, after the fix for CSCsb28921.

  Workaround: Use a Cisco IOS version without the fix for CSCsb28921.

- CSCsm57122

  Symptoms: This is an interoperability issue of SSH and SCP among several open SSH clients and the Cisco IOS client.

  Conditions: SCP is not working simultaneously with the Putty SSH client and CiscoWorks. When transferring the Cisco IOS image to the device, the CPU is being utilized heavily by the SSH process (noticed through the **show proc cpu** command). Also the file transfer rate is very low at 16 to 20 KB/s.

  Workaround: There is no workaround.

- CSCsm57910

Symptoms: All counters stay at zero when the **sh policy-map session** command is entered and when the forwarding sessions on the LAC router are being terminated on a remote router

Conditions: Occurs on routers running Cisco IOS Release 12.4(15)T3 and earlier releases.

Workaround: There is no workaround.

- CSCsm58240

  Symptoms: Traceback "%LSD-2-INVALID_VAR: app is not owner of label" may be seen while removing router Border Gateway Protocol (BGP) configuration.

  Conditions: Occurs in SSO mode when there are 1000s of routes in BGP table. If we try to remove router BGP configuration traceback is seen. There is no issue with forwarding of packets due to this.

  Workaround: Instead of removing entire **router bgp** config you could remove VPN routing/forwarding (VRF) address family in a step by step way to avoid this traceback.

- CSCsm59100

  Symptoms: When error.noresource due to a missing audio source occurs in an input state, it will cause handoff to fail.

  Conditions: Occurs on Cisco Voice XML Gateway running Cisco IOS Release 12.4T. The handoff failure occurs only in an input state, not in a transition state.

  Workaround: There is no workaround.

- CSCsm61105

  Symptoms: The router can crash due to bus error. The crash is seen after repeatedly after removing virtual-template interfaces under ATM.

  Conditions: The crash is seen under the following conditions. 1) Bring up nearly 3000 PPPoE and PPPoEoA sessions. 2) Configure **no interface virtual-template<no>** under ATM interfaces

  Repeating Step 2 continuously will cause a crash.

  Workaround: There is no workaround.

- CSCsm62033

  Symptoms: L2TP session does not come up.

  Conditions: Occurs when a Cisco router marks the Call Serial Number AVP in the ICRP as mandatory. This causes a third-party router to reject it.

  Workaround: There is no workaround.

- CSCsm62608

  Symptoms: MGDtimer traceback occurs and GM might reregister.

  Conditions: Occurs on a Cisco 7200 router when COOP & unicast key is used.

  Workaround: There is no workaround.

- CSCsm62680

  Symptoms: Dynamic NAT using a route-map with reversible fails to allow outside-inside traffic when the route-map has a deny statement first.

  Conditions: This symptom is observed when the route-map is configured.

  Workaround: Remove the route-map deny statement, or use an ACL.

- CSCsm64118

  Symptoms: The router may crash when the **no ip dhcp pool** *word* command is issued from the VTY.

Conditions: This symptom is observed on a Cisco router when the **ip dhcp pool** *word* command is issued from the console and removed from VTY. Configuring dhcp class (class abcd) in the **ip dhcp pool** *word* mode, causes the router to crash.

Workaround: There is no workaround.

- CSCsm65445

  Symptoms: IVR prompt playback is garbled.

  Conditions: Occurred after the **audio-prompt load** command was used to load a file from flash into memory.

  Workaround: A router reload will correctly load the prompt file.

- CSCsm66688

  Symptoms: Device may crash due to watchdog timeout or may hang.

  Conditions: Occurs when turbo-ACL is enabled, which means that "ip access-list compiled" or "ip access-list compiled reuse" is enabled. The QoS and/or ACL configuration is modified.

  Workaround: Remove either "ip access-list compiled" or "ip access-list compiled reuse".

- CSCsm67086

  Symptoms: Router crashing when attaching a policy-map to an interface.

  Conditions: Occurs on a Cisco 2811 running Cisco IOS Release 12.4(15)T2 and 12.4(15)T3. Does not occur in 12.4(15)T1. The router crashes whenever the following policy-map is attached to a multilink bundle interface:

```
policy-map QOS
class af31
priority percent 70
set dscp af31
class af21
bandwidth remaining percent 5
random-detect
set dscp af21
class ef
set dscp ef
bandwidth remaining percent 5
class be
bandwidth remaining percent 5
random-detect
set dscp default
class class-default
fair-queue
random-detect
```

  The issue also affects other devices and other interfaces.

  Workaround: There is no workaround.

- CSCsm69001

  Symptoms: After packets are sent via ping from ce2 to ce1, the NetFlow cache exported from pe1 to the collector has incorrect length for MPLS_TOP_LABEL_IP_ADDR

  Conditions: This is observed in an MPLS-enabled network with MPLS VPN configured between the CEs.

  Workaround: There is no workaround.

- CSCsm69147

  Symptoms: An H.323 gateway may crash with memory corruption.

Conditions: The symptom is observed on a Cisco platform that functions as an H.323 gateway and that is running Cisco IOS Release 12.4(7e) and 12.4(13e). It may be observed in other releases as well. It occurs whenever the H.323 gateway wants to connect to a remote host and there are no free sockets available for this process.

Workaround: There is no workaround.

- CSCsm69163

  Symptoms: H.323 process fails to release memory.

  Conditions: Occurs on a Cisco IPIPGW configured for PSTN and VXML and running Cisco IOS Release 12.4(15)T2.

  Workaround: There is no workaround.

- CSCsm69989

  Symptoms: Class maps are not seen is **show running** output after executing **show auto qos**. This is a display issue with no functional impact.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4(15)T3 and all releases prior to that. Occurs when the router is configured for QoS.

  Workaround: There is no workaround.

- CSCsm70668

  Symptoms: A soft OIR over E3:POS impacts complete traffic with a biscuit tunnel.

  Condition: A soft OIR over E3:POS impacts complete traffic with a biscuit tunnel configured. In OIR "test mbus power 6 off" and "test mbus power 6 on" are performed followed by a microcode reload on slot 6.

  Workaround: There is no workaround.

- CSCsm70774

  Symptoms: The router crashes when a kron policy-list is modified from the console after that kron policy-list has been deleted by another user on a different vty.

  Conditions: This symptom can be observed on a Cisco router when the **kron policy-list** *word* is issued from the console and removed from the VTY. Using the command **cli** *abcd* in the console, while still in the **kron policy-list** *word* mode, causes the router to crash.

  Workaround. There is no workaround.

- CSCsm70913

  Symptoms: When a port channel interface (that is being used in the tunnel configuration) is deleted, then related configuration from the tunnel also should be removed.

  Conditions: When port channel interface (used in the tunnel configuration) is deleted.

  Workaround: There is no workaround.

  Further Problem Description: Following output shows the problem.

  ```
  Router(config-if)#int loop 0 Router(config)#int tun 0 Router(config-if)#tun udlr
  receive-only loopback 0 Router(config-if)#no int loop 0 Router(config-if)#int loop 0
  Router(config-if)#no tun udlr receive-only loopback 0 Router(config-if)#
  *Apr 9 14:03:44.859: %TUN-4-UDLR_IDB_ERROR: UDLR Loopback0 - failed to disable
  receive-only tunnel in udlr_tunnel_receive_only_remove (idbtype *udl_idb) we no longer
  have udl_swsb on loop 0.
  ```

  All loop 0 config should be removed from tunnel when we delete the loopback interface.

  Loop 0 can be replaced by a port-channel interface.

- CSCsm71240

Symptoms: Standby unable to ping to Virtual IP address.

Conditions: Occurs when HSRP groups are removed or changed. The active router is not replying to the standby router with Virtual IP address ARP, and the ARP table in standby shows Virtual IP arp as incomplete.

Workaround: There is no workaround.

- CSCsm72284

  Symptoms: A supervisor engine may crash because of a low memory condition that is caused by an Ethernet Out of Band Channel (EOBC) buffer leak and a big buffer leak.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch that runs Cisco IOS Release 12.2(18)SXF9 but could also affect a Cisco 7600 series router that runs Cisco IOS Release 12.2SR.

  Workaround: There is no workaround.

- CSCsm72479

  Symptoms: A router may crash when configuring extension mobility.

  Conditions: Router must be running Cisco Unified CallManager Express (CME) and a large list of numbers must be configured in the voice user-profile.

  Workaround: There is no workaround.

- CSCsm72482

  Symptoms: CPUHOG messages due to watchdog timeout when empty ACL's are configured:

  ```
  Feb 10 04:37:04.242: %SYS-3-CPUHOG: Task is running for (124000)msecs, more than
  (2000)msecs (7/1),process = CEF Reloader. -Traceback= 0x21E6D0D0 0x21CF1324 0x203353AC
  0x20335390 Feb 10 04:37:06.242: %SYS-3-CPUHOG: Task is running for (126000)msecs, more
  than (2000)msecs (7/1),process = CEF Reloader. -Traceback= 0x21E6D0C0 0x21CF1324
  0x203353AC 0x20335390 Feb 10 04:37:08.242: %SYS-3-CPUHOG: Task is running for
  (128000)msecs, more than (2000)msecs (7/1),process = CEF Reloader. -Traceback=
  0x21E6D0C0 0x21CF1324 0x203353AC 0x20335390
  ```

  Conditions: This issue is seen when ACL are configured but do not have any statements.

  Workaround: Remove ACLs that are empty

- CSCsm72546

  Symptoms: Console flooded by syslog messages. User might have to reboot the machine to get back. Problem may persist until KS interfaces are shut down.

  Conditions: Occurs when there are misconfigurations in an ACL, such as lack of Traffic Encryption key (TEK)

  Workaround: There is no workaround.

- CSCsm72944

  Symptoms: Member links belonging to Multilink Frame Relay (MFR) bundles appear to be sending packets over freedm HIQ.

  Conditions: Display issue only. No functional impact.

  Workaround: There is no workaround.

- CSCsm73592

  Symptoms: A reload may occur when an anything over MPLS (AToM) VC is torn down. Bug triggered initial crash of SIP-400 in slot 4 & ES20 in slot 3. Both cards had to be powered down and reset from the console to recover.

  Conditions: Occurs when AToM VC is setup and torn down later.

Workaround: There is no workaround.

Further Problem Description: The crash may occur when an event triggers access to a previously set up AToM VC. For example, the crash may occur when fast reroute (FRR) is configured on the tunnel interface and the primary interface is removed, such as in the following scenario:

```
pseudowire-class ER1_to_HR1_EoMPLS no preferred-path interface Tunnel501331
disable-fallback ! interface tunnel501331 shutdown ! no interface tunnel501331
```

- CSCsm74168

  Symptoms: Cisco Unified Border Element (CUBE) crashes.

  Conditions: CUBE crashes when Org. transferred to party (also on terminating side) answers the call. Call flow is as follows:

  ```
  - Org.--(SIP Trk)--CSPS--(SIP Trk)--CUBE1--(SIP Trk)--CUBE2--(H323 Trk)--Term.
  ```

  Workaround: There is no workaround.

- CSCsm75286

  Symptoms: A route-map which is configured with both IPv4 and IPv6 for a BGP peer does not work as expected.

  Conditions: Observed after the route-map is modified to delete a sequence.

  Workaround: Apply a fresh route-map

- CSCsm76194

  Symptoms: When a client connects to the router's web page, authentication and authorization are successful, and then ACS starts accounting. When the user logs in, the router sends a correct start accounting request, but when the user is disconnected, the stop accounting request does not include the username field. The router sends the radius information to ACS, but in the request there is no user- name parameter. On the ACS the disconnection is logged as "user=.."

  Conditions: Occurred on a router configured with SSLVPN and when performing AAA with ACS via RADIUS. If the user is connecting via telnet, the stop-accounting works as expected.

  Workaround: There is no workaround.

- CSCsm77059

  Symptoms: The GM crashes after keeping the system idle for few hours. This is noticed when it was kept idle with the following config in key server:

  ```
  ipsecb-7301a(config)#crypto gdoi group GETVPN_QOS_GROUP
  ipsecb-7301a(config-gdoi-group)#server local ipsecb-7301a(gdoi-local-server)#no rekey
  transport unicast
  ```

  Conditions: Occurs on a 3845 configured for Group Encrypted Transport VPN (GET VPN) and running Cisco IOS Release 12.4(15)T4.

  Workaround: There is no workaround.

- CSCsm77608

  Symptoms: IP multicast packets are process switched instead of being switched by Cisco Express Forwarding (CEF), possibly leading to high CPU consumption.

  Conditions: Under normal condition IP Multicast Packets are Process switched instead of CEF switched. Process switching traffic such as multicast, runs the risk of impacting all control plane traffic due to input queue exhaustion as well as high CPU. It also introduces delay and jitter in the data streams.

  Workaround: Manually configure **ip mroute-cache** on all interfaces.

- CSCsm81529

Symptoms: Router reloads if you do the following:

- Open two VTYs to the router

- From one VTY, edit a crypto map or crypto transform

- From the other VTY, delete the crypto map (transform) that the first VTY is editing

- From the first VTY, continue to edit that same crypto map (transform)

Conditions: Occurs on a router running Cisco IOS Release 12.4 and Cisco IOS Release 12.4T.

Workaround: Avoid performing simultaneous operations.

- CSCsm83906

  Symptoms: After a shutdown of the serial interface, the **no shutdown** command will not restore the interface.

  Conditions: This issue is seen on a Cisco 3800 series router installed with a VWIC2-xMFT-G703 card (either onboard slot or HDV2 slot) connected back-to-back with another Cisco 3800 series router with a VWIC2-xMFT-G703 card, that is configured for unframed service.

  Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the controller, or unplug and replug the E1 cable.

- CSCsm84257

  Symptoms: A Catalyst 6500 or a Cisco 7600 may reload unexpectedly. On the console or in the RP crashinfo file, the following message can be seen:

  ```
  %SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = Per-Second Jobs.
  ```

  Conditions: This has been seen on a Cisco 7600 running Cisco IOS Release 12.2(33)SRC and 12.2SXH. The bug can occur for 6500 and 7600.

  Workaround: Disable Netflow by using one of the following commands on every sub-interface for which Netflow is configured. **no ip flow ingress no ip flow egress no ip route-cache flow**

- CSCsm85249

  Symptoms: Mobile IP (MoIP) tunnel never comes up on a mobile router when roaming to the cellular interface. This is because the HWIC-3G-GSM never receives or accepts the registration reply from the Home Agent.

  Conditions: Occurred on a Cisco 3845 router

  Workaround: There is no workaround.

- CSCsm86039

  Symptoms: After switchover, DHCP relay is unable to forward the DHCP REQUEST received from client during RENEW to the server.

  Conditions: Occurs when unnumbered DHCP relay with server address configured under class submode in relay pool config mode.

  Workaround: Configure the server address directly under relay pool mode (rather than class submode) or under the interface (helper address).

- CSCsm86236

  Symptoms: The standby RP reloads continuously.

  Conditions: This occurs on a router in the SSO mode when the **no address-family <name> command is followed rapidly by a address-family <name>** command in the "vrf definition" sub-mode.

  Workaround: Wait for a few seconds to reconfigure the address family after deconfiguring it.

- CSCsm87166

  Symptoms: The **list** command under **ephone-hunt** cannot have 20 numbers configured if the number is 8 digits each,

  Conditions: The following configuration example shows the issue:

  rtrhkglt2(config)#ephone-hunt 1

  rtrhkglt2(config)#list 17465301, 17465302, 17465303, 17465304, 17465305, 17465306, 17465307, 17465308, 17465309, 17465310, 17465311, 17465312, 17465313, 17465314, 17465315, 17465316, 17465317, 17465318, 17465319, 17465320

  Number 1746531 is not a normal ephone-dn or a *. The maximum numbers of ephone-dn we can input is 14 for 8 digits ephone-dn.

  However, it is ok to have 20 ephone-dn in the list if the ephone-dn is of 4 digits each, as an example,

  ephone-hunt 1 longest-idle

  pilot 17465711

  list 5301, 5302, 5303, 5304, 5305, 5306, 5307, 5308, 5309, 5310, 5311, 5312, 5313, 5314,5315, 5316, 5317, 5318, 5319, 5320

  Workaround: There is no workaround.

- CSCsm88305

  Symptoms: A router running Cisco IOS may crash with a bus error.

  Conditions: This is seen on the Cisco 2800 series platform when one or both of the onboard ethernet ports are configured as part of an etherchannel. Under low to medium traffic loads, the device may crash when executing **show run** or **write mem** commands. It also might crash without user intervention under high traffic loads.

  Workaround: Do not use the etherchannel feature for onboard ethernet ports on the Cisco 2821.

- CSCsm88549

  Symptoms: The **spec file install add-entry** command fails for an SFE. It works fine when copied normally to a router.

  Conditions: Occurs when using the **tftp copy** command to copy a file.

  Workaround: Avoid TFTP. If possible, use FTP or RCP.

- CSCsm89475

  Symptoms: No output is seen from the **show policy-map interface** command when **service-policy output OUT_WAN** is configured on ATM interfaces when router is receiving QoS traffic from testing device.

  Conditions: Observed on a Cisco 3800 series router. May affect other mid-range routers.

  Workaround: There is no workaround.

- CSCsm89642

  Symptoms: Cisco router may experience bus crash when the **show crypto sessions** command is entered.

  Conditions: Occurred on a Cisco 7301 router configured as an VRF-aware IPSEC EzVPN server with clients using RADIUS x-authentication.

  Workaround: There is no workaround.

- CSCsm91525

Symptoms: Router may crash during certain types of traffic when IPS is enabled.

Conditions: Occurs on routers running IOS IPS with traffic requiring TCP resets to be sent.

Workaround: There is no workaround.

- CSCsm92206

  Symptoms: A router may crash when a range of interfaces is set to default configurations.

  Conditions: The crash occurs when a range of interfaces is configured in a console connection to belong to a bridge group and when the same set of configurations is removed simultaneously from a vty connection.

  Workaround: Avoid simultaneous tasks (configuring/unconfiguring) through the console and vty.

- CSCsm92967

  Symptoms: Router intermittently deletes crypto socket for hub router which has static mapping in spoke tunnel interface. statically.

  Conditions: Occurs on a Cisco router running Cisco IOS Release 12.4(15)T3.

  Workaround: Remove NHRP mapping entry from tunnel interface and then re-enter again.

- CSCsm94875

  Symptoms: No voice path between IP phone and analog phone when using TLS/SRTP in Cisco Unified CallManager Express (CME) scenario.

  Conditions: Occurs with SRTP calls between VG224 SCCP analog phone and Secure IP phone.

  Workaround: There is no workaround.

- CSCsm95129

  Symptoms: The **no ip next-hop-self eigrp** command does not work after mutual redistribution with BGP (either iBGP or eBGP).

  Conditions: This has been observed on any platform. The combination RIP/EIGRP or OSPF/EIGRP works instead.

  Workaround: There is no workaround.

- CSCsm99079

  Symptoms: The kron process may generate the following syslog and cause the device to reload:

  ```
  Dec 30 23:47:31.920: %SYS-3-CPUHOG: Task is running for (2004)msecs, more than
  (2000)msecs (1/0),process = Kron Process. -Traceback= 0x42725288 0x42725778 0x42724AC0
  0x41E0D72C 0x41E0E0BC 0x41E0E3FC
  ```

  Conditions: The symptom is observed when the command **kron** is configured with the *at* parameter.

  Workaround: Try redesigning the **kron** command to use the *in* parameter.

- CSCsm99638

  Symptoms: Intermittent hung calls are seen in large numbers on a Cisco AS5400XM with AS5X-FC that handles a large volume of calls.

  Conditions: Occurs with calls which are requested as a DSP-less hairpin. This is because DSP-less TDM hairpin calls are not supported on the Cisco AS5400XM with AS5X-FC.

  Workaround: Block this type of call at the software level.

- CSCsm99690

  Symptoms: Router crashing when it tries to export with Netflow Version 9 format.

Conditions: Router is configured with Netflow Version 9 on aggregation and netflow main cache. Problem is seen when aggregation caches are configured, and export is configured to one collector in the global table and one collector in a VPN.

Workaround: Do not use Netflow Version 9.

Further Problem Description: Netflow Version 9 configuration should be configured with destination. When Version 9 configuration and unconfiguration tried on aggregation and main cache many times may lead to crash due to reset of aggregation functionalities set to NULL.

- CSCso00104

  Symptoms: Modifying the aggregation-type prefix-length under Optimized Edge Routing (OER)/learning, along with the ACL used by oer-map for traffic matching can lead to router crash

  Conditions: The router crash was observed when aggregation-type prefix-length and the ACL used by OER-MAP was changed. The aggregation-type prefix-length can be configured as:

  ```
  ! oer master learn aggregation-type prefix-length 16 !
  ```

  The OER-MAP can be configured as follows: (in this case, oer-map is used to set monitor mode to active for the traffic matching the ACL) ! oer-map BRANCH 10 match traffic-class access-list OerMapAclHttp set mode route control set mode monitor active set unreachable threshold 10 set active-probe echo 10.1.6.254 set probe frequency 10

  Workaround: After making the configuration changes, if the configuration is saved right away, and then the router is reloaded, the crash was not observed. This can be used as a workaround for this crash.

- CSCso00792

  Symptoms: After receiving disconnect message from ISDN, the actual call disconnection is delayed by 64 seconds.

  Conditions: The symptom is observed when the disconnect is received from the incoming ISDN call leg for a TDM-hairpin, DSPless call.

  Workaround: There is no workaround.

- CSCso00801

  Symptoms: After tuning IOS IPS signatures via CSM or SDM and deploying changes, IOS IPS **show commands** display change, but newly-applicable traffic is not detected.

  If three separate updates to service-ports and regular expressions are applied successively, the device may crash.

  Conditions: Occurs when user tunes IOS IPS signatures, modifying the service-ports parameter. User deploys change. To confirm change, user issues **show ip ips sig sig** *SIG_ID* **subid** *SUB_ID* command on the IOS device. The command output will contain the new value; however, newly-applicable traffic that should now cause this signature to fire, will not. Any originally applicable traffic that would match original values, will still cause the signatures to fire.

  This behavior will continue until the device is reloaded.

  Workaround: Retiring and un-retiring the altered signature will causes the changes to take effect. To prevent crashes, apply the delta updates in one update rather than multiple ones.

  You can also remove IOS IPS configuration from all interfaces, then re-apply IOS IPS configuration back to interfaces.

- CSCso03047

  Symptoms: The multilink interfaces stop forwarding traffic, and the serial interfaces out of the multilink start to flap.

Conditions: This symptom is observed when the E3 controller is saturated.

Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the controller.

- CSCso03424

  Symptoms: Group member (GM) goes into re-registration loop.

  Conditions: Occurs when only deny ACLs exist in a security association (SA) in a group.

  Workaround: Add at least one permit ACL in all SAs in a group.

- CSCso03783

  Symptoms: Router stuck in UNKNOWN-MODE and not accepting any commands.

  Conditions: Occurs after configuring xconnect VC through interface range mode

  Workaround: Power cycle the router.

- CSCso04075

  Symptoms: The router will reload and write a crashfile after issuing the **vlan-range dot1q** command with certain configurations (see below).

  Conditions: This defect will only occur if there exists a current VLAN-range which was configured using identical first and last VLAN id's (ie **vlan-range dot1q** *5 5*, in which case the range length is zero), and this range overlaps with the range being configured.

  Trigger: Configuring the same first VLAN ID range with different value for the last VLAN ID range when configured earlier with first and last with same value

  Workaround: Use the **vlan-id dot1q** command instead of configuring a VLAN-range with the same first and last VLAN ids (a range with range length of zero).

  If you have configured a VLAN-range with a range length of zero, then do not attempt to configure an overlapping range where the IDs overlap with an existing zero length range on the same interface. This configuration is erroneous and prohibited.

- CSCso04657

  Symptoms: SSLVPN service stops accepting any new SSLVPN connections.

  Conditions: A device configured for SSLVPN may stop accepting any new SSLVPN connections, due to a vulnerability in the processing of new TCP connections for SSLVPN services. If "debug ip tcp transactions" is enabled and this vulnerability is triggered, debug messages with connection queue limit reached will be observed. This vulnerability is documented in two separate Cisco bug IDs, both of which are required for a full fix: CSCso04657 and CSCsg00102.

- CSCso05177

  Symptoms: User-defined class and non-shape based queuing policy can be attached to a tunnel interface. This should not be allowed.

  Conditions: Occurs in internal builds of Cisco IOS Release 12.4T.

  Workaround: There is no workaround.

- CSCso05771

  Symptoms: When clearing the first entry of local domain lists with similar entries, the router crashes if **show run** is entered.

  Conditions: Occurs with routers configured with a domain list similar to this example:

```
ip urlfilter exclusive-domain permit www.cisco112.com ip urlfilter exclusive-domain
permit www.cisco186.com ip urlfilter exclusive-domain permit www.cisco173.com ip
urlfilter exclusive-domain permit www.cisco21.com ip urlfilter exclusive-domain permit
www.cisco194.com ip urlfilter exclusive-domain permit www.cisco78.com ip urlfilter
exclusive-domain permit www.cisco124.com
```

If the following command is entered: **no ip urlfilter exclusive-domain permit www.cisco112.com**

The router crashes when **show run** is entered.

Workaround: Do not delete the first entry in similar domain lists.

- CSCso06542

  Symptoms: On a Cisco router configured for NAT VPN routing/forwarding (VRF), **ip nat inside source** commands might get corrupted at boot up time in running config even though they are perfectly fine in startup config. The corruption could be observed in the following form (but not only)

  ip nat inside source list *[ACL]* **pool***[pool-name]* **vrf** *[vrf name]* **match-in-vrf overload vrf** *[vrf name]*

  the "vrf [vrf name]" after overload should not be there

  Conditions: This was observed on a Cisco 3845 running Cisco IOS Release 12.4(18.3)T configured with NAT VRF but it could be observed on other platforms and IOS versions.

  Workaround: Remove and re-configure the affected VRFs. The problem might reappear after bootup.

- CSCso06849

  Symptoms: Some multicast packets may get dropped when VSA is used for hardware acceleration.

  Conditions: Occurs when there is multicast replication for multiple interfaces with crypto map applied on the same router.

  Workaround: There is no workaround.

- CSCso07411

  Symptoms: In a router having redundant RP and configured for stateful switchover (SSO), traffic engineering (TE) tunnels and Open Shortest Path First (OSPF) as IGP configured, the standby RP may continue rebooting after a SSO switchover and the following config-sync error will be seen in the console log:

  ```
  Mar 5 13:14:19.749 PST: Config Sync: Bulk-sync failure due to Servicing
  Incompatibility. Please check full list of mismatched commands via: show redundancy
  config-sync failures mcl
  Mar 5 13:14:19.749 PST: Config Sync: Starting lines from MCL file: interface
  Tunnel3000 ! <submode> "interface" - ip ospf interface-retry 0 ! </submode>
  "interface"
  ```

  Conditions: The symptom will only happen in a mis-configuration where the TE tunnel interface does not have an IP address configured.

  Workaround: Use the loopback address for TE tunnel interface IP address, such as **ip unnumbered loopback 0** for tunnel address.

- CSCso07514

  Symptoms: Call drops if both IPPhone1 and IPPhone2, with CUBE (IPIPGW) in between, are put on hold and then Resume.

  Conditions: Occurs when CUBE (IPIPGW) interworking with CallManager or CVP, in H323-H323 is configured. If phones from both ends are put on hold and then resume, CUBE sends TCS Reject and drops the call.

Workaround: Configure the **h245 passthru all** command under "voice service voip" as follows:

#voice service voip h323 h245 passthru all

- CSCso09376

  Symptoms: Originating SIP Gateway does not disconnect the call when mandatory precondition (RSVP) is configured but the terminating gateway does not honer the preconditions and alerts the user before preconditions are met.

  Conditions: This happens only in a negative scenario where the terminating gateway ignores the "precondition" tag in "Require" header and alerts the user before preconditions are met.

  Workaround: There is no workaround.

- CSCso10596

  Symptoms: Polling cvpdnSessionAttrDevicePhyId from the CISCO-VPDN-MGMT MIB may show that multiple users are mapped to the same Virtual-Access SNMP ifIndex. This affects statistics collection or billing using IF-MIB counters.

  Conditions: This symptom is observed when PPP renegotiates an existing PPP connection on a Virtual-Access interface.

  Workaround: When possible, use RADIUS accounting for gathering statistics or billing.

- CSCso12297

  Symptoms: ISDN PRI does not come up in MGCP mode. The **pri-group timeslots <> service mgcp** CLI does not come up.

  Conditions: Occurs when configuring a PRI in MGCP mode only.

  Workaround: Use the PRI in H323 mode.

- CSCso12305

  Symptoms: The IPv6 Cisco Express Forwarding (CEF) table may be missing prefixes which are present in the IPv6 RIB.

  Conditions: Occurs when CEF is disabled and re-enabled.

  Workaround: Enter the **clear ipv6 route ***.

- CSCso12748

  Symptoms: Tunnels between Cisco and non Cisco peers fail to come up since the Mandatory of Message Type AVP for SCCRQ that is sent by Cisco is FALSE.

  Conditions: This symptom occurs because the Mandatory of Message Type AVP for SCCRQ that is sent by Cisco is FALSE.

  Workaround: There is no workaround.

- CSCso14464

  Symptoms: The router may fail to load Cisco IOS Release 12.4(19.8)T and may show the following error message: loadprog: error - program section linked to illegal address

  Conditions: The symptoms are observed on a Cisco 1800/1810 series, a Cisco 1700 series and a Cisco 815 series router running Cisco IOS Release 12.4(19.8)T.

  Workaround: There is no workaround.

  Further Problem Description: This is a compiler/link issue.

- CSCso14546

  Symptoms: Users cannot tune IPS signatures that start with 61.

Conditions: Occurs when the following steps are performed:

1. Configure IPS 5.x on a router.

2. Edit an event action for a signature where signature id starts with 61 and it has more than one subsignature-id.

3. Generate IPS XML files using SDM/CP.

4. The updated event action is missing in the XML file for the corresponding signatures.

5. <var name="event-action">xxxxx</var> tag is missed for the signature id.

Workaround: There is no workaround.

- CSCso14884

  Symptoms: The router may crash upon changing interface physical-layer from sync to async on a serial interface while it is in loopback mode.

  Conditions: The symptom occurs on Cisco 3800 series router.

  Workaround: Remove loopback mode before changing physical-layer from sync to async.

- CSCso15151

  Symptoms: When Multicast Distributed Fast Switching is configured, a VIP crashes on a Cisco 7500 router that is running a Cisco IOS 12.3 release.

  Conditions:

  1) The router has around 1000 interfaces/subinterfaces. 2) Distributed multicast is configured. 3) The router is running any Cisco IOS 12.3 release.

  Workaround: There is no workaround.

  Further Problem Description: In summary, the line card is accessing the memory location that has been freed already. This results in the VIP crashing. There are sanity checks that are missing in Cisco IOS 12.3 releases. The problem is similar to what bug CSCdm29808 does on line cards of the Cisco 12000 Internet series router (this router does not support Cisco IOS Release 12.3). This basically checks if the interface index on MDFS messages is less than the MDFS Idb map size, which indicates the current size of the Idb map table.

- CSCso15220

  Symptoms: A Cisco router may experience a memory leak in the VTSP process. The router appears to lose its free memory until it starts to display "SYS-2-MALLOCFAIL" messages in the log and finally crashes per low memory condition.

  Conditions: The symptoms occur only when a call fails before it reaches the connect state.

  Workaround: The only workaround is to schedule router manual reloads at regular intervals, so that the outages occur at the lowest-impacting moments.

- CSCso20347

  Symptoms: VXML handoff is failed if MRCPV2 client is used.

  Conditions: Handoff is failed when vxml application uses "builtin://com.cisco.callhandoff" tag to handoff and the MRCPV2 client is used.

  Workaround: Use "vxml subdiag" to handoff to another application instead.

- CSCso20810

  Symptoms: A buffer leak may occur when a router is configured with the combination of NAT, multicast and encryption. Occurs when multicast subsequently flows out a crypto-enabled interface.

Conditions: This bug will effect only those users whose routers are part of a multicast group. They must also have NAT and crypto configured on one or more of the interfaces in the multicast group.

Workaround: Multicast traffic can be forwarded via a GRE tunnel instead of in the clear.

- CSCso21432

  Symptoms: Router fails to send out secondary DNS requests when the primary DNS server is down.

  Conditions: Occurred on a Cisco 1800 running 12.4(15)T3. The router forwards DNS requests to the primary server as expected. However, the router fails to send requests to the secondary server after the primary DNS goes down.

  Workaround: Configure the router to act as a DNS fowarder as follows:

  ```
  Router(config)#ip dns view default Router(cfg-dns-view)# dns forwarder <primary dns ip> Router(cfg-dns-view)# dns forwarder <secondary dns ip>
  ```

  Then configure PCs to send DNS requests to the affected router for forwarding.

- CSCso21611

  Symptoms: Device crashes due to memory allocation issue.

  Conditions: Observed on Cisco 7200, but this is not a platform-specific bug.

  Workaround: There is no workaround.

- CSCso21888

  Symptoms: Router may spontaneously reload.

  Conditions: Occurs on routers configured with iSPF computation algorithm in OSPF.

  Workaround: Disable iSPF.

- CSCso22331

  Symptoms: A Cisco 2811 router running as voice gateway may crash after enabling the **debug voip vtsp event** command.

  Conditions: The symptom can be seen when 2-stage dialing is enabled and SETUP_ACK with a Progress Indicator is received on the outbound leg of the router.

  Workaround: Disable the **debug voip vtsp event** command.

- CSCso23419

  Symptoms: The CBTS master tunnel goes down on rare occasion when the path change occur on all the members. Even after a member tunnel comes up, the master tunnel does not report up for 10 seconds.

  The CBTS members are configured with the same sequence of explicit path-options. When the link down occur on head-end on the LSP path, the new LSP are setup as the next-path on all the members in this case.

  This only impacts the reporting of the master tunnel state.

  Conditions: Configure the same sequence of explicit path-options on all the members.

  Workaround: There is no workaround.

- CSCso24243

  Symptoms: A VC associated with a VT keeps flapping.

  Conditions: This symptom is observed when LFIoATM is configured on a Cisco 7200 or when dLFIoATM is configured on a Cisco 7500 router.

  Workaround: There is no workaround.

- CSCso25511

  Symptoms: IP/PPPOE over QinQ encapsulation may fail.

  Conditions: Problem seen with QinQ where second-dot1q is set to "any" option.

  Workaround: Use valid inner and outer VLAN ID instead of "any" option,.

- CSCso25524

  Symptoms: Router crashes with "%SNMP-3-DVR_DUP_REGN_ERR: Attempt for dupe regn with SNMP by driver having ifIndex 1201 and ifDescr Virtual-Access1.186-mpls layer" error.

  Conditions: Testing with PPPOE sessions established through a Virtual-template with "mpls ip" and "mpls label protocol ldp" configured on the Virtual-template interface. Basic PPPOE configs needed for PTA mode are applied at RouterA and RouterB. A police-map with policing is attached to Virtual-template at both IN & OUT direction. PPPOE sessions will be established through this Virual-template. When MPLS LDP is enabled at RouterB virtual-template and session is initiated from RouterA, The RouterB crashes.

  Workaround: Do not configure "mpls ip" and "mpls label protocol ldp" on the Virtual-template interface.

- CSCso25559

  Symptoms: IKE/IPSec fails to come up.

  Conditions: This symptom occurs when two different sub-CAs of a third-party vendor are used as peers.

  Workaround: There is no workaround.

- CSCso25823

  Symptoms: Router causes neighbor router to crash.

  Conditions: Error message are seen when "mpls ip" is enabled on the interface, but causes the neighbor router to crashes upon issuing the command.

  Workaround: There is no workaround.

- CSCso27236

  Symptoms: Cisco IOS CA shows incorrect renew date (Jan 1 1979). Example:

  Before restart Start Date: 1 Jan 2008 10:00:00 End Date : 1 Jan 2011 10:00:00 Renew Date : 1 Jan 2008 09:58:00

  After restart Start Date: 1 Jan 2008 10:00:00 End Date : 1 Jan 2011 10:00:00 Renew Date : 1 Jan 1970 08:00:00

  Conditions: Occurs when auto-enroll is enabled and the router is reloaded.

  Workaround: There is no workaround.

- CSCso30073

  Symptoms: EIGRP neighbors are not coming up after an IP address change on the interface and the new subnet is added to the EIGRP autonomous system.

  Conditions: The symptom is observed on a Cisco router that is running Cisco IOS Release 12.4(20)T.

  Workaround: There is no workaround.

- CSCso30221

  Symptoms: Service policy removed from ATM interface after changing ABR value in ATM PVC.

Conditions: Happens with a Cisco 7200 router which is running Cisco IOS version 12.4(19.9)T1. This is a platform-independent defect. Last pass release is Cisco IOS Release 12.4(17.9)T.

Workaround: There is no workaround.

- CSCso32814

  Symptoms: Bytes value in **show policy-map session** output is zero on LAC router.

  Conditions: Occurs on a Cisco 7200 router running Cisco IOS Release 12.4(19.9)T1.

  Workaround: There is no workaround.

- CSCso32831

  Symptoms: A Cisco 7200 NPE-G2 router may crash when the command **show usb device** *1 0A* is entered.

  Conditions: The symptoms are observed on a Cisco 7200 NPE-G2 router that is running image c7200p-adventerprisek9-mz.124-19.9.T1.

  Workaround: Use the command **show usb device** to list all USB devices.

- CSCso32982

  Symptoms: NSE-100 processor crashes while bringing up L2TPV3oATM-FR circuit.

  Conditions: It occurs consistently when we bring up L2TPV3oATM-FR.

  Workaround: There is no workaround.

- CSCso34076

  Symptoms: A Cisco router may reload when unconfiguring **ccm-manager**.

  Conditions: This is seen on MGCP gateway running Cisco IOS Release 12.4(15)T4 while entering the **no ccm-manager config** command.

  Workaround: There is no workaround.

- CSCso36664

  Symptoms: Router crashes while removing the match criteria for class-map.

  Conditions: Occurs on a Cisco 7200 router loaded with Cisco IOS Release 12.4(19.10)T IOS.

  Workaround: There is no workaround.

- CSCso37716

  Symptoms: Following error is seen:

  ```
  ISDN **ERROR**: LIF_Build_L3_Hdr: Invalid call reflen
  ```

  Conditions: Occurs when raw message received by SIP application is corrupted.

  Workaround: There is no workaround.

- CSCso38132

  Symptoms: Attempt fails while placing analog dial-in call to as5400 router. Ping fails in caller by throwing error as Timeout expecting: CONNECT.

  Conditions: Occurs on a Cisco AS5400 running Cisco IOS Release 12.4(19.9)T1.

  Workaround: There is no workaround.

- CSCso39444

  Symptoms: SP/LC might crash after SSO cutover.

  Conditions: This problem is a timing issue and would be more easily seen in SSO cutover case.

Workaround: There is no workaround.

- CSCso39518

  Symptoms: Traceback displayed on the console.

  Conditions: Before applying patch with Cisco IOS Embedded Event Manager (EEM) policy dir subsystem in it, there is one or more EEM applets configured, after the patch is activated, trigger an EEM applet.

  Workaround: Unconfigure all the EEM applets before patching, then apply all the EEM applets after activating the patch.

  Further Problem Description: This would lead to (fh_policy_dir.proc)process crash, not a device crash. This bug is specific to modular IOS image.

- CSCso39964

  Symptoms: The router hangs when attempts are made to modify pure ACL configuration while traffic is still flowing.

  Conditions: Occurs on routers running Cisco IOS Release 12.4(15)T4. The router returns back to normal if the traffic is stopped.

  Workaround: There is no workaround.

- CSCso40618

  Symptoms: A Cisco 871 router may crash with error %SYS-2-NOTQ with Process="DNS Resolver" after loading an image.

  Conditions: Firewall application inspection for IM protocols is configured. Protocol-info parameter-map is configured to resolve the IM server host names and is associated to IM protocols in firewall class-map.

  Trigger: Issue is caused when router uses "parameter-map protocol-info" which has a list of IM server host names, to resolve list of IM servers.

  Workaround: Do not associate the protocol-type parameter-map to IM protocol in firewall class-map.

- CSCso42792

  Symptoms: A router does not boot with the secured image after securing the image an the disk.

  Conditions: This happens on a Cisco router loaded with Cisco IOS Release 12.4(19.9)PI8.

  Workaround: There is no workaround.

- CSCso44547

  Symptoms: Router crashes while accessing non-functional Common Internet File System (CIFS) server that is configured in WebVPN NetBIOS Name Service (NBNS) list.

  Conditions: Occurs only with a non-functional CIFS server.

  Workaround: Configure functional NBNS servers.

- CSCso44593

  Symptoms: A router with VSA may crash while booting.

  Conditions: Occurs when the startup configuration has group domain of interpretation (GDOI) crypto map applied on the interface.

  Workaround: Copy the configuration after the router is booted.

- CSCso45508

Symptoms: Fragmented multicast rekeys and pings are not acknowledged by a multicast receiver.

Conditions: Occurs when fragmented multicast packets are received on a multicast receiver interface with crypto map attached.

Workaround: There is no workaround.

- CSCso47048

  Symptoms: A router may crash with the following error message:

  ```
  %SYS-2-CHUNKBADFREEMAGIC: Bad free magic number in chunk header, chunk 6DF6E48 data
  6DF7B48 chunk_freemagic EF430000 -Process= "Check heaps", ipl= 0, pid= 5,
  -Traceback= 0x140C170 0x1E878 0x1EA24 0x1B4AC 0x717DB8 chunk_diagnose, code = 2 chunk
  name is PPTP: pptp_swi
  current chunk header = 0x06DF7B38 data check, ptr = 0x06DF7B48
  next chunk header = 0x06DF7B70 data check, ptr = 0x06DF7B80
  previous chunk header = 0x06DF7B00 data check, ptr = 0x06DF7B10
  ```

  Conditions: Issue has been seen on Cisco 7200 router with NPE-G2 configured for L2TP and running Cisco IOS Release 12.4(15)T3 and Cisco IOS Release 12.4(15)T4.

  Workaround: There is no workaround.

- CSCso47363

  Symptoms: A Cisco router may crash when the **no bba-group pppoe** *word* command is issued from the VTY.

  Conditions: This symptom is observed on a Cisco router when the **bba- group pppoe** *word* command is issued from the console and removed from VTY using the **no bba-group pppoe** *word* command. In this mode, when giving the command service profile "abcd refresh 2" in the console, the router will crash.

  Workaround. There is no workaround.

  Further Problem Description: The issue impacts device operations. This is a corner case issue, seen in an unusual sequence of testing. This issue is not seen on Cisco IOS Release 12.4(21).

- CSCso47627

  Symptoms: A Cisco router may crash while doing a simultaneous operation in **pvc-in-range** *0/32* and **vc-class atm** *word*.

  Conditions: This symptom is observed while configuring simultaneously in **pvc-in-range** *0/32* and **vc-class atm** *word*.

  Workaround. There is no workaround.

- CSCso47738

  Symptoms: Gateway sends 200 OK with media direction as SENDRECV for a reINVITE with offer having media direction INACTIVE.

  Conditions: This is seen for the supplementary services when the call is put on HOLD and then RESUMED.

  Workaround: There is no workaround.

- CSCso47788

  Symptoms: Customer initially running a 6xT1 MLP bundle using three VWIC-2MFT-T1 modules on same slot 0 of a Cisco 3825 router. The Customer is running both voice and data over this MLP link with QoS (LLQ/CBWFQ) applied to the multilink. The MLP circuit is connected to an MPLS network. The customer has fragmentation disabled on the multilink.

The issue occurs when customer adds a 7th and/or 8th T1 to the MLP bundle, which is connected on slot 2 (VWIC2-2MFT-T1/E1). The customer sees increased latency and jitter using extended pings over the MLP bundle.

Conditions: Occurs on a Cisco 3825 running the c3825-spservicesk9-mz.124-7b Cisco IOS image and using a VWIC2-2MFT-T1/E1 module installed in slot 2 (NM-HDV2-2T1/E1).

Workaround: Manually configure **tx-ring-limit 2**under serial interfaces residing on the VWIC2-2MFT-T1/E1.

- CSCso53653

  Symptoms: A Cisco router may leak memory if configured for an Embedded Event Manager (EEM) applet that utilizes the **action** *tag* **cli** command.

  Conditions: This occurs under two conditions. Either there is not enough memory for the action to complete properly, in which case there will be memory allocation failure messages sent to the log. Alternatively, there is not enough vtys available to run the action, in which case the following errors may be seen in the log:

  ```
  %HA_EM-3-FMPD_CLI_CONNECT: Unable to establish CLI session: no more tty lines
  %HA_EM-3-FMPD_ERROR: Error executing applet appletname statement tag
  ```

  This only occurs in EEM versions 2.2 and earlier. EEM 2.2 is available in Cisco IOS Release 12.4 Mainline. EEM 2.3 and later are not affected.

  Workaround: Increase the number of vtys so that the policy will always be able to get one. Do not run the IOS device low on memory.

- CSCso54391

  Symptoms: An MLPP call receiving preemption for reuse on unanswered call from the PBX fails to complete.

  Conditions: This symptom is observed on all platforms.

  Workaround: There is no workaround.

- CSCso55047

  Symptoms: Router crashes while unconfiguring **debug condition all** on L2TP network server (LNS).

  Conditions: This symptom occurs when **no debug condition all** is configured to remove the condition that was initially set.

  Workaround: There is no workaround.

- CSCso55072

  Symptoms: System traceback occurs during TCL code execution which causes subsequent system reboot.

  Conditions: Occurs when ESM is still processing events in the background and another syslog message is being processed from the ESM logger queue.

  Workaround: Avoid ESM filters that executes background events like CLI commands for an extended period of time, such as in a loop with high loop count.

- CSCso56185

  Symptoms: L2TP Start-Control-Connection-Reply (SCCRQ) and Start-Control-Connection-Reply (SCCRP) messages have incorrect setting of mandatory-bit for the receive window Size attribute-value pair (AVP). This may cause L2TP/VPDN sessions to fail to connect.

  Conditions: Occurs in VPDN environments where the peer requires tight protocol adherence.

  Workaround: There is no workaround.

- CSCso57001

  Symptoms: Router crashes when interfaces flap and the device is running the MetroE IPSLA feature.

  Conditions: When the device is set to automatically start jitter/ping probes and the interfaces flap, it results in a crash when trying to re-create auto generated MetroE operations.

  Workaround: There is no workaround.

- CSCso57457

  Symptoms: Sending long caller ID causes the gateway to crash while populating the caller id.

  Conditions: Occurs when sending long caller ID for ETSI Mode.

  Workaround: Avoid sending long caller ID.

- CSCso60063

  Symptoms: Router crashes when the **no password pass** is issued from the console while configuring "dot1x credentials" in configuration mode.

  Conditions: Occurs only when the **no password pass1** command is entered.

  Workaround: There is no workaround.

- CSCso61743

  Symptoms: Router crashes when stcapp is disabled, stcapp ccm-group is removed from configuration, and then stcapp is re-enabled.

  Conditions: Occurred on Cisco 2691 and Cisco 3745 routers running Cisco IOS Release 12.4(15)T05. Can also occur on other platforms running this Cisco IOS release. Can also occur if stcapp is disabled and the user attempts to enable stcapp but stcapp fails to start for any reason.

  Workaround: There is no workaround.

- CSCso62266

  Symptoms: Router forwards Bridge Protocol Data Unit (BPDU) after disabling spanning-tree. But after reload, it blocks the BPDU.

  Conditions: Occurs when switch-port is configured.

  Workaround: Enable spanning-tree. You may then disable it again if it is not desired.

- CSCso62511

  Symptoms: A router may crash. The log file before the crash indicates:

  ```
  %SYS-3-CPUHOG: Task is running for (44004)msecs, more than (2000)msecs (1/1),process =
  IP NAT Ager. -Traceback= 0x61F9B630 0x61FA31BC 0x61F6B9F8 0x62E47F04 0x62E48048
  0x61F6BDF4
  ```

  Conditions: The symptom is observed on a router configured for NAT and running SIP calls.

  Workaround: There is no workaround.

- CSCso63693

  Symptoms: Configuring the **passive-interface default** command in ISIS when existing interfaces exceed 255, or loading/reloading the router when interfaces exceeding 255 exist in the startup-configuration, may generate the following error message: ISIS: Maximum circuit limit (255) has reached. Subsequent interfaces are not advertised into ISIS as expected.

  Conditions: The symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(33)SXH1 and where interfaces exceeding the 255 limitation exist in the startup-configuration and the router is loaded/reloaded. It is also observed when interfaces exceeding the 255 limitation are configured after the command **passive-interface default** is used.

Workaround: Use the **passive interface** command to manually configure all interfaces.

- CSCso64104

  Symptoms: A router may crash after applying the configurations related to PA- MC-2T3-EC immediately after the router reloads.

  Conditions: The symptom is observed on Cisco 7200 series and a 7301 router.

  Workaround: Do not configure PA-MC-2T3-EC immediately after the router reloads.

- CSCso64585

  Symptoms: Jitter or voice quality issues may occur.

  Conditions: The symptoms are observed when there is more than one ephone monitoring the same Park DN. This causes more than one of the same SCCP message to be sent to the phone in a few milliseconds.

  Workaround: There is no workaround.

- CSCso65148

  Symptoms: Group member crashes after running for 8-10 hours.

  Conditions: Occurs in the rare condition that a re-registration happens at the same time as the re-key is being processed.

  Workaround: There is no workaround.

- CSCso65193

  Symptoms: The memory occupied by the IP SLA Event Processor may gradually increase.

  Conditions: The issue occurs when IP SLA jitter operation is configured on the router without source port specification.

  Workaround: There is no workaround.

  Further Problem Description: With 1000 IP SLAs configured (200 each of following types: path-echo, path-jitter, icmp-echo, udp-jitter and udp-echo, each with a unique destination), the memory allocated for "IP SLAs Event Pr" increases and the level of available processor memory goes down. This issue will have a performance impact.

- CSCso66473

  Symptoms: A router may crash when the user moves from one segment to another and attempts to log onto SSG.

  Conditions: The symptom is observed in the following situation: 1. Open a user known to SSG through accounting-start, with an IP address of "IP1." 2. User then logs onto SSG. 3. User moves to another segment which generates another accounting-start for the same mac address but a different IP address, IP2. 4. The SSG then crashes.

  Workaround: There is no workaround.

- CSCso66862

  Symptoms: Router crashes due to bus error. The crash is seen after repeatedly removing virtual-template interfaces under ATM.

  Conditions: The crash is seen under the following conditions.

  1) Bringing up nearly 3k PPPoE and PPPoEoA sessions. 2) Configuring **no interface virtual-template <no>** under ATM interfaces.

  Repeating Step 2 continuously will cause a crash.

  Workaround: There is no workaround.

- CSCso68344

  Symptoms: The command **no service dhcp** to stop DHCP server/relay from the router may cause a crash.

  Conditions: The symptom is observed when router is receiving requests from DHCP clients at high rate and duplicate-address detection ping is active.

  Workaround: There is no workaround.

- CSCso68463

  Symptoms: The router may crash when the command **test crash** is executed and then option "S" is selected.

  Conditions: The symptom occurs on a Cisco router that is running Cisco IOS Release 12.4(15)T5.

  Workaround: There is no workaround

  Further Problem description: When the router is configured with the commands **memory record** *filter exclude <WORD>*, **memory record** *traceback depth 16 hashbits 12*, **memory record** *events buffer 1024* and then execute the command **test crash** and select the option "S" from the crash menu, the router crashes.

- CSCso68864

  Symptoms: Shape peak percent and absolute value calculations are wrong while attaching policy-map to interface.

  Conditions: Occurs when policy-map is attached to interface.

  Workaround: There is no workaround.

- CSCso69350

  Symptoms: When changing the type of a class-map from "match-all" to "match- any," the filter level stats may not show, although functionality is unaffected.

  Conditions: The symptom is observed after a policy is applied to an interface, and then the type of the class-map is changed.

  Workaround: Reapplying the service-policy will fix this issue.

- CSCso70587

  Symptoms: The RTP ports are being opened at H323 and the SSRC for the SRTP call is being updated before the PROCEEDING/ALERTING indication is received on the ISDN end. This may result in a "%DSM-3-INTERNAL" error message.

  Conditions: The symptoms are observed on a Cisco 2811 series and an AS5xxx router.

  Workaround: Disable the SRTP configuration and initiate normal RTP calls.

- CSCso72893

  Symptoms: A warning message may be seen when the encapsulation value changes on an interface with CDP disabled, and c5350-boot-mz image build is failed with the following errors:

  ```
  sub_core_platform.o(.text+0x1a10c): In function ‘encapsulation_command’: : undefined
  reference to ‘cdp_supported_int’ make-3.79.1-p3: *** [c5350-boot-m.czsun] Error 1
  sub_core_platform.o(.text+0x1a10c): In function ‘encapsulation_command’: : undefined
  reference to ‘cdp_supported_int’
  ```

  Conditions: The symptom is observed when the encapsulation value is changed on an interface with CDP disabled, followed by CDP enabled.

  Workaround: There is no workaround.

Further Problem Description: This is an expected behavior. Warning messages will be seen whenever encapsulation changes with CDP being disabled on the interface. This is due to the commit of CSCso59137.

- CSCso73533

  Symptoms: Traceback is seen after unconfiguring the tunnel interface.

  Conditions: The symptom is seen when using Ipv4 multicast PIM tunnels where the route to the Rendezvous Point (RP) is via another tunnel interface. If this tunnel interface was unconfigured, then there is a race condition between: 1. learning about the new route to the RP via another interface; and 2. periodic update of the PIM tunnel adjacency. If the latter occurs first the traceback is seen

  Workaround: There is no workaround.

- CSCso78427

  Symptoms: A voice gateway is crashing at ccsip_apply_sip_to_pstn_calling_policy with a TLB (store) exception.

  Conditions: This symptom is observed on a Cisco AS5400XM that is running either Cisco IOS Release 12.4(19) or Cisco IOS Release 12.3(14)T6.

  Workaround: There is no workaround.

- CSCso78991

  Symptoms: An L2TPv3 tunnel fails to establish between Cisco routers when one is running Cisco IOS Release 12.4(T) and the other is running Cisco IOS Release 12.2(33)SRC.

  Conditions: This issue is only seen when the L2TPv3 tunnel terminates on Cisco routers running Cisco IOS Release 12.4(T) on one side and Cisco IOS Release 12.2(33)SRC on the other. Other combinations of IOS versions allow the L2TPv3 to establish successfully.

  Workaround: There is no workaround.

- CSCso81854

  Multiple Cisco products are vulnerable to DNS cache poisoning attacks due to their use of insufficiently randomized DNS transaction IDs and UDP source ports in the DNS queries that they produce, which may allow an attacker to more easily forge DNS answers that can poison DNS caches.

  To exploit this vulnerability an attacker must be able to cause a vulnerable DNS server to perform recursive DNS queries. Therefore, DNS servers that are only authoritative, or servers where recursion is not allowed, are not affected.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080708-dns.shtml

  This security advisory is being published simultaneously with announcements from other affected organizations.

- CSCso82469

  Symptoms: If a user tries to create new mail, the OWA displays an improper message (such as the page cannot be displayed or that the page cannot be loaded) and the OWA session hangs. This will cause the rest of the session to be unresponsive to any more connections.

  Conditions: The symptom is observed on a server configured with the OWA feature. The issue only occurs when trying to access OWA.

  Workaround: There is no workaround.

- CSCso82575

  Symptoms: A service policy may not be attached to the interface with compression when the interface is enabled with MQC

  Conditions: The symptom is seen only when interface group-async is configured with service policy attached.

  Workaround: There is no workaround.

- CSCso82732

  Symptoms: Every hour (at 31 mins past the hour), three to six calls fail. The cause is given as "cause 47" (resource not available) and "cause 16" (cause 16 errors usually follow cause 47 errors).

  Conditions: The symptoms are observed every hour under load conditions when 20 or more T1 channels are turned on. No errors are seen with a load less than 20 channels.

  Workaround: Use Cisco IOS Release 12.4(15)T5. Alternatively, remove the NTP configuration from the GK.

  Further Problem Description: CPU spikes are seen at the time of failures on NTP process. There are no call failures if the NTP configuration is removed.

- CSCso83840

  Symptoms: Certain reserved characters (for example, the ampersand character: "&") may get lost if they are used in the http submit URL.

  Conditions: The symptom is observed on an IVR Voice Browser that is running Cisco IOS Release 12.4(15)T.

  Workaround: There is no workaround.

- CSCso84447

  Symptoms: When using an SCCP phone over NAT, the following NAT error message may be received: "NAT-Frag pyld failure seq-out of range" and the phone may fail to register.

  Conditions: The symptoms are observed when using an SCCP phone over NAT. The SCCP phone sends segmented packets to the TCP and NAT tries to reassemble these packets. The error message displays when the packets are outside the expected data range.

  Workaround: Use alternatives to the SCCP phone such as the SIP/H323 application.

- CSCso85132

  Symptoms: The codec CLIs under the **dspfarm profile** submode fail when entered manually. After a reload the CLIs may disappear from the configuration and the profile will need to be deleted and created again.

  Conditions: The symptom is observed when a reload of the router/gateway causes the codec CLIs under the **dspfarm profile** submode to be removed.

  Workaround: For default codec configurations, the dspfarm profile can be deleted and configured again. Otherwise, there is no workaround.

- CSCso87054

  Symptoms: A router may crash on an absolute command of the ACL configurations.

  Conditions: The symptom is seen when an absolute sub-command for time-range is used.

  Workaround: There is no workaround.

- CSCso87348

  Symptoms: A Catalyst 6500 or a Cisco 7600 may reload unexpectedly.

Conditions: Occurs when NetFlow is configured on one of the following: * Cisco 7600 running Cisco IOS Release 12.2(33)SRC. * Catalyst 6500 running Cisco IOS Release 12.2SXH.

Workaround: Disable Netflow. This is done with the following commands:

```
no ip flow ingress
no ip flow engress
no ip route-cache flow
```

Enter the appropriate command for each sub-interface for which NetFlow is currently configured.

- CSCso88429

  Symptoms: CME or CUBE will reject an inbound SIP INVITE if Max-Forwards is greater than 70.

  Conditions: The symptoms are observed when a Max-Forwards header field in SIP INVITE is greater than 70.

  Workaround: There is no workaround.

  Further Problem Description: From RFC 3261: 20.22 Max-Forwards

  The Max-Forwards header field must be used with any SIP method to limit the number of proxies or gateways that can forward the request to the next downstream server. This can also be useful when the client is attempting to trace a request chain that appears to be failing or looping in mid-chain.

  The Max-Forwards value is an integer in the range 0-255 indicating the remaining number of times this request message is allowed to be forwarded. This count is decremented by each server that forwards the request. The recommended initial value is 70.

  This header field should be inserted by elements that can not otherwise guarantee loop detection. For example, a B2BUA should insert a Max-Forwards header field.

- CSCso89945

  Symptoms: The CMM: Transcoder may not get registered to the CUCM.

  Conditions: The symptom is observed while configuring the dspfarm transcoding profile.

  Workaround: There is no workaround.

- CSCso90235

  Symptoms: A router may crash when a trust point which has the IP address interface configured is deleted.

  Conditions: The symptom is observed on a router that is loading Cisco IOS Release 12.4T.

  Workaround: Unconfiguring the IP address interface command on trustpoint before deleting the trustpoint may work.

- CSCso91078

  Symptoms: A Cisco IAD2430 may reload unexpectedly due to a bus error (Sig=10).

  Conditions: The symptom is seen on a Cisco IAD2430 that is running Cisco IOS Release 12.4(15)T4.

  Workaround: There is no workaround.

- CSCso91230

  Symptoms: A router may display the following error:

  ```
  %LINK-2-INTVULN: In critical region with interrupt level=0, intfc=ATM0 -Process= "IGMP
  Snooping Receiving Process"
  ```

  Conditions: The symptom is observed when bridged traffic is passing to an MLPP interface.

  Workaround: Disable IGMP snooping with the **no ip igmp snooping** command.

- CSCso91341

Symptoms: The following operations are legal but are rejected on the grounds that there is insufficient bandwidth: 1. A QoS policy-map is attached as a service-policy to an interface or other valid target; or 2. A previously attached policy-map is modified.

Conditions: The symptoms are observed when, prior to the error, a policy-map failed to be attached or modified due to insufficient bandwidth to meet the bandwidth guarantees in the policy-map.

Workaround: Remove all policy-maps from the affected target. Attach a simple policy-map with no bandwidth guarantees (e.g., having only a **shape** command). Remove this service-policy. This should remove all queueing datastructures from the target. Proceed to attach the original policy-map.

- CSCso92175

  Symptoms: The configured value of a queue-limit gets changed and locked at 16000 bytes when random-detect is applied to the policy-map and service policy is attached to the interface.

  Conditions: The symptom is observed when a queue-limit is configured in front of the WRED in the same class of policy-map.

  Workaround: Configure the WRED in front of queue-limit in the same class of policy-map.

- CSCso92323

  Symptoms: A router may crash upon the attachment of the WebVPN gateway to the WebVPN context.

  Condition: The symptom is observed when the WebVPN gateway is attached to the WebVPN context.

  Workaround: There is no workaround.

- CSCso92494

  Symptoms: Spurious access may be seen on a Cisco 7200 series router.

  Conditions: The symptom is observed when LFIoFR is configured on a Cisco 7200 series router and when attaching a QoS policy to a Virtual-Template.

  Workaround: There is no workaround.

- CSCso93065

  Symptoms: Standby RP crashes while receiving dynamic sync from active RP during DHCP relay binding creation.

  Conditions: Occurs when outer is configured as DHCP relay and running IOS images that include the fix for CSCsm86039.

  Workaround: There is no workaround.

- CSCso93867

  Symptoms: Router crashes with bus error exception.

  Conditions: This happens when **qos service-policy** is unconfigured or reconfigured on a virtual-template interface.

  Workaround: There is no workaround.

- CSCso94463

  Symptoms: GET VPN group members may fail to register to the key server.

  Conditions: The problem is found under these two conditions: 1. GDOI crypto map (with local address) is applied to multiple interfaces; and 2. One of these applied interfaces is down.

  Workaround: There is no workaround.

- CSCso94780

  Symptoms: Router crashes after changing matching criteria, as shown in the following example:

```
config terminal Enter configuration commands, one per line. End with CNTL/Z.
7301D(config)#class-map myclass6 7301D(config-cmap)#no match ip prec 6
7301D(config-cmap)#match ip dscp cs6
%ALIGN-1-FATAL: Corrupted program counter 20:48:36 UTC Wed Apr 23 2008 pc=0x6CFFFFB0 ,
ra=0x625BBA54 , sp=0x66270000
%ALIGN-1-FATAL: Corrupted program counter 20:48:36 UTC Wed Apr 23 2008 pc=0x6CFFFFB0 ,
ra=0x625BBA54 , sp=0x66270000
20:48:36 UTC Wed Apr 23 2008: TLB (load or instruction fetch) exception, CPU signal
10, PC = 0x6CFFFFB0
```

  Conditions: The above symptom is observed on Cisco 7200 and Cisco 7301 routers.

  Workaround: There is no workaround.

- CSCso95136

  Symptoms: Cisco 181x series router crashes.

  Conditions: Occurs while unconfiguring dialer in band on asynchronous interface.

  Workaround: There is no workaround.

- CSCso97946

  Symptoms: An H320 GW2 may crash when a call is made from an H323 endpoint.

  Conditions: The symptom is observed when an H323 endpoint that sends the audio codecs G.729, G.711 u-law, G.711 A-law, G.728, G.722 64k, G.722 56k, G.722 48k in the TCS to the H320 GW.

  Workaround: Configure a single audio codec under the VOIP dial-peer.

- CSCso98389

  Symptoms: The **initiate-to** command is being rejected under the "config-vpdn-req-out" mode.

  Conditions: The symptom is seen in Cisco IOS Interim Release 12.4(19.16)T1.

  Workaround: There is no workaround.

- CSCso98430

  Symptoms: A PPPoE session fails to come up.

  Conditions: This symptom is observed on a Cisco router loaded with Cisco IOS Release 12.4T, and when virtual-template is configured.

  Workaround: There is no workaround.

- CSCso98579

  Symptoms: A router configured with ccm-manager config may crash.

  Conditions: The symptom is observed on a router that is configured with ccm- manager config. If there is an interface with a configuration line longer than 100 bytes, the problem will be seen when Call Manager tries to configure the router.

  Workaround: Remove any lines of configuration longer than 100 bytes from controllers, interfaces and voice ports.

  Further Problem Description: This issue has been seen most often with a long description on either T1/E1 controller, or corresponding serial interface, but any long configuration line would cause the problem.

- CSCsq02689

  Symptoms: The WCCP service will not come up. Instead of a "SERVICEFOUND" message, the following error message is generated every 10 seconds in the router log:

```
%WCCP-5-SERVICEMISMATCH: Service 00 mismatched on WCCP client 10.1.1.2 BST:
WCCP-EVNT:S00: Here_I_Am packet from 10.1.1.2: service mismatch
```

Conditions: The symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 12.4T. It is observed under normal WCCP use for WAAS or web caching.

Workaround: There is no workaround.

- CSCsq02771

  Symptoms: DHCP relay may hang when request for IP address is received from a DHCP client on an unnumbered in an MPLS and VPN setup.

  Conditions: The symptom is observed on a Cisco 7200 router that is running Cisco IOS Interim Release 12.4(19.16)T1.

  Workaround: There is no workaround.

- CSCsq03115

  Symptoms: The PIM configuration may be missing and the following traceback is seen:

  ```
  %SYS-3-MGDTIMER: Running timer, init, timer = 895661C. -Process= "Exec", ipl= 0, pid=
  80, -Traceback= 0x14C0F30 0x31DA638 0x31DA7C8 0x31DA914 0x1E019B4 0x1E35634 0x1E34AD0
  0x15160F8 0x1515234 0x1542208 0x695548
  ```

  Conditions: The symptom is observed symptom is observed after performing an OIR of the PA-T3+ serial port adapter. The symptom occurs twice.

  Workaround: Reconfigure the PIM mode.

- CSCsq03760

  Symptoms: Packets are dropped on the end host in the return path, when using dot1q encapsulation on the on-board Gigabit Ethernet interface.

  Conditions: The symptom is observed when the router, with VLAN encapsulation on the ingress path, is using CEF switching. The trigger is when the router forwards packet with wrong VLAN encapsulation to the next hop on the ingress path.

  Workaround: There is no workaround.

- CSCsq03843

  Symptoms: The debug message may fail to display.

  Conditions: The symptom is seen while doing the AAA test.

  Workaround: There is no workaround.

- CSCsq05997

  Symptoms: The following error messages may appear in the log file multiple times:

  ```
  %ARP-3-ARPINT: ARP table accessed at interrupt level 1, -Traceback= 0x61013944
  0x60B61F80 0x60B5A2A4 0x6019DDAC 0x600FA37C 0x600FCC6C Because the message is
  generated frequently, the log file may fill up too soon.
  ```

  Conditions: The symptom is observed because an IOS component is accessing the arp cache table in the interrupt context, which against the design of the IOS module. The error message indicates that the software is in danger of causing the router to crash.

  Workaround: There is no workaround.

- CSCsq06645

  Symptoms: Packets may get dropped when a route map is applied to peergroup members.

  Conditions: The symptom is observed on a Cisco router that is running Cisco IOS Release 12.4T. The problem is seen when the combination of peergroup and route map is used.

  Workaround: There is no workaround.

- CSCsq06813

  Symptoms: Only one RELEASE message is seen on a DHCPv6 when the server is shut, even though multiple messages are expected.

  Conditions: The symptom occurs on Cisco 7200 series router that is running Cisco IOS Release 12.4T.

  Workaround: There is no workaround.

- CSCsq09592

  Symptoms: The router is black-holing traffic that is going to be encrypted. The crypto-counters are not showing an increase.

  Conditions: The symptoms are observed when service-policy is configured on the main interface and crypto map is configured on a subinterface and when IP CEF is enabled.

  Workaround: Redesign the configuration to apply service policy on the subinterface. Disable CEF globally.

  Further Problem Description: Clear text-traffic is effectively received by the router. It triggers the creation of Phase I/Phase II. However, it then appears to be blackholed:

  ```
  interface Ethernet0/0 no ip address service-policy output shape ! interface
  Ethernet0/0.10 encapsulation dot1Q 10 ip address 10.0.0.1 255.255.255.252 crypto map
  mymap
  ```

- CSCsq09836

  Symptoms: 1. For some 3660 platform images, the **connect** command is not working and as a result local switching does not work. 2. For some images, the **no connect** command is not working to remove an existing connection.

  Conditions: The symptoms are observed with 3660 platform images where both ac_atm and atm_switching subsystems are responsible for local switching.

  Workaround: Remove ac_atm and use only atm_switching for local switching.

  Further Problem Description: Problems may arise for other 3660 platform images having both ac_atm and atm_switching.

- CSCsq10730

  Symptoms: A Cisco router may display the following messages after enabling the advanced signature set in IOS-IPS: Too many UUIDs in pdu type 0x0E Too many UUIDs in pdu type 0x0B Too many UUIDs in pdu type 0x0E Too many UUIDs in pdu type 0x0B

  Conditions: The symptom is observed on a Cisco router that is running Cisco IOS Release 12.4(15)T, that is utilizing IOS IPS v5 feature, and is running with the advanced signature set (MSRPC). Symptom occurs when incoming MSRPC packets are malformed or do not comply with protocol.

  Workaround: There is no workaround. The message is informational (cosmetic).

- CSCsq11620

  Symptoms: Crashes may be caused by the code which uses "strncpy" and "sprintf".

  Conditions: The symptoms are observed when accessing a specific string.

  Workaround: There is no workaround.

- CSCsq11750

  Symptoms: A Cisco router may crash when the **no mgcp** and the **no mgcp profile** *profile-name* commands are issued from the VTY, and the command **call- agent** *ip-address* is configured through the console in "config- mgcp-profile" mode.

Conditions: The symptom is observed when there is simultaneous operation between the console line and the VTY line.

Workaround: Configure using a single telnet connection instead of two.

- CSCsq12337

  Symptoms: Parsing of a SIP message with MIME content fails, which causes call termination.

  Conditions: The symptoms are seen when the SIP message contains application/qsig or application/x-q931 contents in MIME without a Content- Length SDP header.

  Workaround: Add a Content-Length SDP header for application/qsig or application/x-q931 contents with appropriate value. Alternatively, disable sending application/qsig or application/x-q931 contents in the SIP message.

- CSCsq13576

  Symptoms: The router may crash when the multilink interface goes down.

  Conditions: The symptoms are observed when the multilink interface has interleave configured.

  Workaround: There is no workaround.

- CSCsq14210

  Symptoms: A router may crash when a ping is issued and when the **clear ip cef * prefix-statistics** command is issued on router.

  Conditions: The symptom is observed when encapsulation FR is configured on the dialer interface, having profile configuration, and CEF switching is also configured.

  Workaround: There is no workaround.

  Further Problem Description: When encapsulation FR is configured on the dialer interface having profile configuration, it was made as a CEF switchable interface by default. When the CEF looks for a fastsend vector, the vector was NULL and router crashes at this point. Encapsulation ppp has its own way of installing the punt adjacency when the call is not UP and then it makes the interface a CEF switchable interface when the call comes UP.

- CSCsq15560

  Symptoms: In creating a multi-party video conference by calling into a Cisco IPVC MCU device, a call may intermittently suffer from one-way video.

  Conditions: The symptom is seen with a multi-party video conference which calls into a Cisco IPVC MCU device and where a local CME video endpoints calls the MCU via a gatekeeper over H323. This is a timing issue in the H.323 state machine. In a call flow, two sets of OLCs (for audio and video) are exchanged. BRQ is sent for audio OLC. Before BCF is received, GW gets video OLC. This updates the total channel bandwidth and checks if it is less then the approved BW. As it is not so, OLC is rejected resulting in one-way video.

  Workaround: There is no workaround.

  Further Problem Description: This scenario works fine with third party H323 endpoints with their own H323 stacks working with the same gatekeeper and MCU. A more heavily loaded (for instance, with debugs) CME gateway will experience the problem less often.

- CSCsq16611

  Symptoms: IPv6 packets are process switched instead of using Cisco Express Forwarding (CEF)

  Conditions: The above symptom is observed on a Cisco 7301 and Cisco 7200 routers.

  Workaround: There is no workaround.

- CSCsq19047

Symptoms: A VXML gateway may stop handling calls due to lack of memory.

Conditions: The symptom is observed on a VXML gateway that is running Cisco IOS Release 12.4(15)T and when the SIP Take back application is configured to initiate a REFER-based call transfer in a CVP scenario.

Workaround: There is no workaround.

Further Problem Description: Page 374 of this configuration & administration guide states how this configuration must be setup:
http://www.cisco.com/en/US/docs/voice_ip_comm/cust_contact/contact_center/customer_voice_portal/cvp4_0/configuration/guide/cvp40cfg.pdf

- CSCsq20970

  Symptoms: On the 2432 platform UUT, the ‘atm’ option is missing in the ‘mode’ CLI when the T1 controller is being configured for ATM.

  Conditions: The symptom is observed on the 2432 platform with a T1 controller.

  Workaround: There is no workaround.

- CSCsq21347

  Symptoms: Sometimes WebVPN login page may not come up when a client browser connects to the gateway. Sometimes, login page may come up, but after entering the login credentials portal page does not come up. The following syslog messages are seen.

  1) We are able to enter the webvpn login page, but after entering the username and password, the page returns the error message "Internal Error" and does not let us login. Also, the traceback below is seen.

  ```
  May 10 06:15:19.183 PDT: %SYS-2-CHUNKINVALIDHDR: Invalid chunk header type 0 for chunk
  0, data 0 -Process= "SSLVPN_PROCESS", ipl= 0, pid= 265, -Traceback= 0x61898E8C
  0x6002DFC4 0x63D802FC 0x63D70C64 0x63D78A5C 0x63D79054 0x63D7986C 0x63D736A8
  ```

  2) The webvpn login page is not thrown up at all when we try to connect to the webvpn gateway. The ’Page is not displayed’ due to the following Traceback May 10 21:57:30.963 PDT:

  ```
  %SYS-2-CHUNKINVALIDHDR: Invalid chunk header type 0 for chunk 0, data 0 -Process= "IP
  Input", ipl= 0, pid= 120, -Traceback= 0x61898E8C 0x6002DFC4 0x63D6D564 0x63D72F48
  0x63D5C804 0x62285B20 0x62288158 0x61F81940 0x61F83264 0x61F8367C 0x61F83738
  0x61F83980
  ```

  Conditions: This can happen if WebVPN configuration is being removed and a client tries to connect.

  Workaround: Avoid removing WebVPN configuration once it is configured.

- CSCsq30717

  Symptoms: A NPE-G1 resets due to a hardware watchdog timeout. This is indicated in the **show version** output with "Last reset from watchdog reset".

  Conditions: The Cisco 7200 must have an enabled PA-MC-2T3-EC with channelized T1s.

  Workaround: Disable the PA-MC-2T3-EC.

- CSCsq31808

  Symptoms: With eiBGP multipath, incoming labeled packets may get looped in MPLS core instead of getting forwarded to CE, causing traffic issues. The following symptom may be found:

  - The error message below is frequently generated.

  ```
  Dec 17 07:44:46.734 UTC: %COMMON_FIB-3-BROKER_ENCODE: IPv4 broker failed to encode msg
  type 0 for slot(s) 0B -Traceback= 6044E470 60465864 6043BCFC 6043B570
  ```

  - The **debug cef xdr** command yields the following message:

```
Mar 31 17:44:40.576 UTC: FIBrp_xdr: Table IPv4:<vrf name>, building insert event xdr
for x.x.x.x/y. Sources: RIB Mar 31 17:44:40.576 UTC: FIBrp_xdr: Encoding path
extensions ... Mar 31 17:44:40.576 UTC: FIBrp_xdr: - short ext, type 1, index 0 Mar 31
17:44:40.580 UTC: FIBrp_xdr: Getting encode size for IPv4 table broker FIB_FIB xdr Mar
31 17:44:40.580 UTC: - short path ext: len 12 Mar 31 17:44:40.580 UTC: - short path
ext: len 24 Mar 31 17:44:40.580 UTC: - feat IPRM, len 12 Mar 31 17:44:40.580 UTC: =>
pfx/path 113 + path_ext 24 + gsb 8 + fs 16 = 161
```

- checking the prefix, it point to drop entry.

```
router#show mpls forward vrf <vrf name> x.x.x.x Local Outgoing Prefix Bytes Label
Outgoing Next Hop Label Label or VC or Tunnel Id Switched interface 937 No Label
x.x.x.x/y[V]  0 drop <========= it is drop
- checking the MOI flag of EBGP path, the No_Global flag (0x10) was incorrectly set
router#show ip cef vrf <vrf name> x.x.x.x int [snip] path_list contains at least one
resolved destination(s). HW not notified path 70BFFC5C, path list 20E87B58, share 1/1,
type recursive nexthop, for IPv4, flags resolved MPLS short path extensions: MOI flags
= 0x16 <-------MOI flags 0x10 is incorrectly set (for ebgp path, correct flag should
be 0x4, 0x5, 0x6 ..) correct now. [snip]
```

Conditions: eiBGP multipath enabled; iBGP path comes up first, then the eBGP path. Both eBGP & iBGP paths could be in MPLS forwarding causing the issue.

Workaround: Using the **clear ip route vrf <name> x.x.x.x** clears the issue.

- CSCsq33653

  Symptoms: The caller ID transmission may fail from FXS port to FXO port.

  Conditions: The symptoms are observed when the sub-command **caller- id** is configured under "voice-port x/y".

  Workaround: There is no workaround.

- CSCsq34171

  Symptoms: A router may crash when the ip address/mask is changed on the interface.

  Conditions: The symptom occurs if EIGRP authentication is enabled.

  Workaround: Disable authentication.

  Further Problem Description: When the authentication is removed from the interface, the crash does not occur on changing the mask.

- CSCsq35036

  Symptoms: An HWIC-1DSU-T1 card comes up with line loopback turned on.

  Conditions: The symptom is observed with Cisco 2801 and 1841 routers only.

  Workaround: Press the button to clear loopback condition.

  Alternate workaround: Execute the **clear service-module <>** command.

  Further Problem Description: The problem happens because HWIC reset assert/deassert is not happening before and after the FPGA download respectively in these platforms.

- CSCsq37010

  Symptoms: Unable to set up SSL VPN full-tunnel from clients.

  Conditions: Occurs on Cisco 3845 router running the c3845-adventerprisek9-mz.124-19.18.T2 image. When Windows client attempts to connect, tunnel set up fails with error "The VPN client driver has encountered an error."

  Workaround: There is no workaround.

- CSCsq37349

  Symptoms: A router may crash due to a corrupted Program Counter.

Conditions: The symptom is seen with Zone-based Firewall and IPS, along with VRF and IPSec tunnel configured.

Workaround: There is no workaround.

- CSCsq40088

  Symptoms: A Cisco 3845 router may crash when unconfiguring IPv6 nodes.

  Condition: The symptom is observed on a Cisco 3845 router that is running Cisco IOS Release 12.4T. The traceback is produced after configuring the **no ipv6 unicast-routing** command.

  Workaround: There is no workaround.

- CSCsq40659

  Symptoms: A client may not get a prefix when it has two relay agents on two interfaces of a single DHCP relay agent, with one of them being an unnumbered interface.

  Conditions: The symptom is seen on a router that is running Cisco IOS Release 12.4T.

  Workaround: There is no workaround.

- CSCsq40813

  Symptoms: Queue-limit locked with the given value and remains dead with "random-detect discard-class-based."

  Conditions: Happens only with random-detect discard-class-based and queue-limit configuration.

  Workaround: There is no workaround.

- CSCsq41455

  Symptoms: The router hangs and has to be reset.

  Conditions: This crash happens when out-of-order sequence numbers are used in an ACL. In the ACL in the description, ACE 1 triggers the crash.

  Workaround: Instead of making the changes to the ACL with the ACL applied to the interface, if the changes are made to the ACL after it is removed from the interface, the crash will not happen.

- CSCsq41508

  Symptoms: An ACL with more than 13 ACEs will not show any matches on the OG ACEs.

  Conditions: If the ACL has more than 13 ACEs, any object group ACEs will not function properly.

  Workaround: There is no workaround.

- CSCsq42399

  Symptoms: Shortly after upgrade, the router shows the following error:

  ```
  May 22 09:05:53.109 METDST: %SYS-2-MALLOCFAIL: Memory allocation of 261116 bytes
  failed from 0x61A37948, alignment 0 Pool: Processor Free: 6427012 Cause: Memory
  fragmentation Alternate Pool: None Free: 0 Cause: No Alternate pool -Process= "Virtual
  Exec", ipl= 0, pid= 234, -Traceback= 0x61452110 0x6000A7FC 0x60010638 0x60010C2C
  0x634CB644 0x61A37950 0x61461910 0x 614BD940 0x6149E000 0x614C1B08 0x62AA2494
  0x62AA2478
  ```

  Traffic is affected, and the router unable to display output from the **show run**.

  Conditions: Occurs on a Cisco 7200 router running the c7200-adventerprisek9-mz.124-15.T3.bin. Service Selection Gateway (SSG) and RADIUS are involved.

  Workaround: There is no workaround.

- CSCsq43934

Symptoms: TCP/HTTP zone-based firewall (ZBF) session failed to established with dynamic or overload NAT mode.

Conditions: Normal deployment condition.

Workaround: There is no workaround.

- CSCsq44428

  Symptoms: Under certain conditions with IPv6 for EIGRP, the router may log error messages such as the following:

  ```
  00:00:09: %DUAL-3-INTERNAL: IPv6-EIGRP(0) 80: Internal Error
  ```

  Conditions: The error message is currently not causing a operational impact.

  Workaround: There is no workaround.

- CSCsq45836

  Symptoms: Dynamic Multipoint VPN (DMVPN) shortcut tunnels may fail to get established on a DMVPN spoke running a phase 3 setup.

  Conditions: Occurs in Cisco IOS Release 12.4(20)T.

  Workaround: There is no workaround. However, data traffic would not be affected since the packets would take the spoke-hub-spoke path.

- CSCsq46742

  Symptoms: SIP gateway crashes when a 302 response contains a contact header with the same IP address as that of SIP gateway.

  Conditions: The crash occurs only when the 302 response contains a contact header with an IP address the same as that of the gateway IP address. The crash also occurs only when the IP address is mapped to a domain name exceeding the length of the IP address received in the contact header.

  Workaround: Ensure that the IP address that is received in the 302 response is mapped to a domain name not exceeding the length of the IP address.

- CSCsq46832

  Symptoms: The "IP SLAs: RTP VoIP Operation" feature was introduced in Cisco IOS Release 12.4(4)T to allow users to obtain some realistic VoIP Round Trip Time (RTT), Jitter, Packet Loss, and Mean Opinion Score (MOS) measurements from a live VoIP call over a real IP cloud and using a bonafide voice codec supported over voice DSPs. It has been found that in certain versions of the IOS 12.4T release train this feature is not functioning at all. The output of the **show ip sla statistics N** EXEC prompt command, where N is the IP SLA probe tag number, returns something similar to the following output reporting all zeroed-out measurements:

  ```
  VoiceGateWay#sh ip sla statistics 3 IPSLAs Latest Operation Statistics
  IPSLA operation id: 3 Type of operation: rtp Latest operation start time: 11:35:15.606
  EST Tue May 27 2008 Latest operation return code: No connection Latest RTT
  (milliseconds): 0 Source to Destination Path Measurements: Interarrival Jitter: 0
  Packets Sent: 0 Packets Lost: 0 Estimated R-factor: 0 MOS-CQ: 0.00 Destination to
  Source Path Measurements: Interarrival Jitter: 0 Packets Sent: 0 Packets Lost: 0
  Estimated R-factor: 0 MOS-CQ: 0.00 Operation time to live: 72083 sec Operational state
  of entry: Active Last time this entry was reset: Never
  ```

  Conditions: This behavior is observed on Cisco 1700, 2600, 3700, 7200, 7500, 2800, and 3800 voice platforms installed with IOS 12.4(19.18)T or newer in the IOS 12.4T release family, and configured with the RTP VoIP IP SLA feature.

  Workaround: There is no workaround.

- CSCsq48201

Symptoms: A crash may occur when creating a Bridge-Group Virtual Interface (BVI) while traffic is flowing.

Conditions: The crash could occur when a BVI interface is first created with the command **interface BVI** and traffic is being process switched by a physical interface in the same bridge-group. Once the BVI interface is created, subsequent **interface BVI** commands to configure that interface will not cause the crash.

Workaround: Remove the physical interface from the bridge-group, or prevent traffic from being process switch by the interface when the BVI interface is first created.

- CSCsq48717

  Symptoms: Attaching the following policy:

  ```
  policy-map p1 class prec1 class class-default shape
  ```
  will result in the packets to class prec1 not being enqueued to class-default.

  Conditions: Occurs on a router running Cisco IOS Release 12.4(19.18)T02.

  Workaround: Remove the policy from the interface, remove class prec1, add the policy back and then add class prec1.

- CSCsq49100

  Symptoms: Removal of last class-map before the qos-group class-map causes the router to crash.

  Conditions: Happens every time when the class-maps change from type (Mix) to type (Un-Mix), such as the following:

  ```
  Mix : dscp precedence qos-group
  Un-Mix: qos-group qos-group qos-group
  ```
  Workaround: There is no workaround.

- CSCsq49768

  Symptoms: MAC L2TP clients failed to setup tunnel after L2TP network server (LNS) upgraded to Cisco IOS Release 12.4(19.18)T3.

  Conditions: Occurs when Mac OS X 10.4 and Mac OS X 10.5 clients attempt to connect to a LNS running Cisco IOS Release 12.4(19.18)T3. image loaded.

  Workaround: There is no workaround.

- CSCsq50100

  Symptoms: When a call is placed between secure phone from SIP gateway to secure Cisco Unified CallManager (CCM) phone call is established as SRTP call. After hold/resume the call becomes non-secure.

  Conditions: All supplementary services are affected (hold/resume of a secure call, call transfer, conferencing, etc.).

  Workaround: There is no workaround.

- CSCsq51500

  Symptoms: When attempting to bring up the Secure Device Provisioning (SDP) Welcome page, the following message is displayed in the web browser: "IPv6 unicast-routing is not enabled".

  When using Internet Explorer, this is simply a cosmetic bug. With Firefox v2.0.0.14, this message gets displayed and the web page is corrupted and unusable so that SDP cannot continue.

  Conditions: When the config is saved and you do not have IPv6 unicast routing enabled, this problem sometimes occurs when attempting to display the SDP Welcome page.

  Workaround: Use Internet Explorer rather than Firefox.

- CSCsq51826

  Symptoms: Router crashes when Flexible NetFlow for IPv6 is received and IPv6 fragmented packets are received.

  Conditions: Flexible Netflow for IPv6 must be configured and fragmented IPv6 packets must be received.

  Workaround: Deconfigure IPv6 Flexible NetFlow.

- CSCsq52048

  Symptoms: Router crashed while running **show vpdn tunnel all** command.

  Conditions: When there are thousands of L2TP tunnels coming up, going down, running **show vpdn tunnel all** may result in crash.

  Workaround: There is no workaround.

- CSCsq52847

  Symptoms: Connection establishment failed with the event agent.

  Conditions: Occurs when the Event Gateway is killed and restarted on a Cisco 1812 router while running Cisco IOS Release 12.4(19.18)T2.

  Workaround: There is no workaround.

- CSCsq54601

  Symptoms: SCCP and SIP registration fail with EzVPN and NAT configured. Only Voice traffic is affected

  Condition: Occurs when SCCP Registration traffic is passing through NAT Router.

  Workaround: There is no workaround.

- CSCsq57856

  Symptoms: When Cisco 2431 and Cisco 2691 router is configured with 1DSU-T1-V2 card, router crashes while loading.

  Conditions: The crash is seen while loading the router, when router is configured with 1DSU-T1-V2.

  Workaround: There is no workaround.

- CSCsq60016

  Symptoms: Router crashes after entering a long RSA key string

  Conditions: Occurs when a very long hex string is entered.

  Workaround: Break the entry into shorter strings.

- CSCsq62269

  Symptoms: If a Cisco 3270 has no startup configuration, it will crash if the "autoinstall" option is selected.

  Condition: Occurs when there is no startup configuration and the router is using the c3270-adventerprisek9-mz.124-15.XZ.bin image.

  Workaround: Execute **tftpdnld -r in rommon to boot c3270-entbase-mz.124-15.XZ.bin**. Do not allow the "autoinstall" option to run. Save the default configuration and reboot it with the c3270-adventerprisek9-mz.124-15.XZ.bin image.

- CSCsq63176

  Symptoms: PA-MC-T3/E3-EC PA does not pass full traffic after a sudden burst near line rate.

Conditions: Occurs when 256 interfaces are configured on the port adapter with multilinks operating on those serial interfaces.

Workaround: Configure fewer than 256 serial interfaces.

- CSCsq63278

  Symptoms: Shape rate under child policy is not met. Shape rate of child policy is equal to parent shape rate

  Conditions: Occurs on a Cisco 7200 router is running Cisco IOS Release 12.4(21.1)T.

  Workaround: There is no workaround.

- CSCsq64663

  Symptoms: Router Crashes when EtherChannel is shut down

  Conditions: Occurs on a Metro Ethernet device with over 2000 IP SLA operations configured and CFM services defined for a EtherChannel. The **no int ether-channel...** command causes the device to crash.

  Workaround: There is no workaround.

- CSCsq64843

  Symptoms: An IOS router configured with Dynamic Multipoint VPN (DMVPN) may run of memory.

  Conditions: The symptom may occur when hub or spoke is behind a NAT device.

  Workaround: There is no workaround.

- CSCsq67163

  Symptoms: Scheduling of IP SLA RTP operation crashes the router.

  Conditions: This problem occurs only when IPSLA RTP operation is configured and scheduled to run.

  Workaround: There is no workaround.

- CSCsq70872

  Symptoms: Router crashes when executing the **clear zone-pair inspect session** command.

  Conditions: Occurs when the router has a TCP session active when the user executes the command.

  Workaround: There is no workaround.

- CSCsq74300

  Symptoms: Loopbacks, Null0 and other non Point-to-Point interfaces are not allowed in a route-map set command due to the changes introduced with caveat CSCsk63775.

  Conditions: This issue is seen with Cisco IOS Release 12.4(18) or a later release. Upgrading to Cisco IOS Release 12.4(18) or a later release may break the existing network.

  Workaround: Use Cisco IOS Release 12.4(17) or an earlier release.

- CSCsq75526

  Symptoms: When DNS forwarding source interface is configured in a split DNS environment, the source address being populated in the packet while forwarding the DNS query is wrong. It always takes the first interface in the VPN routing/forwarding (VRF) view even when the DNS forwarding source interface is changed. DNS query fails.

  Conditions: The above symptom is seen on a router running Cisco IOS Release 12.4(15)T6.

  Workaround: There is no workaround.

- CSCsq75944

  Symptoms: A Catalyst 6500 or a Cisco 7600 may reload unexpectedly. On the console or in the RP crashinfo file, the following message can sometimes be seen:

  %SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = Per-Second Jobs.

  Conditions: Occurs during normal use on a Catalyst 6500 or Cisco 7600. NetFlow must be enabled.

  Workaround: Disable Netflow by using one of the following commands on every sub-interface for which Netflow is configured:

  no ip flow ingress no ip flow egress no ip route-cache flow

- CSCsq76338

  Symptoms: Call across SIP trunk takes around 10 seconds to resume after called party goes on hold.

  Conditions: Occurs during normal operating conditions.

  Workaround: There is no workaround.

- CSCsq77968

  Symptoms: Changing the connect command configuration may reload the router.

  Conditions: Occurs when the same connection is configured twice with different interfaces and Data-Link Connection Identifiers (DLCI). This is observed when running the latest version of Cisco IOS Release 12.4T.

  Workaround: Instead of changing the connect command configuration, use the **no connect** command to remove the command and then re-apply the new connect command configuration.

- CSCsq78208

  Symptoms: The router is crashing during start up when NTP update is received from SUP.

  Conditions: Occurs when there is an NTP update and a Cisco Multi-Processor WAN Application Module (MWAM) is present.

  Workaround: There is no workaround.

- CSCsq80546

  Symptoms: Router crashed when policy-map modified while passing traffic.

  Conditions: The problem was seen on Cisco routers running Cisco IOS Release 12.4(19.18T5).

  Workaround: There is no workaround.

- CSCsq80658

  Symptoms: H325 call is not connected properly in Cisco Unified Border Element (CUBE).

  Conditions: In CUBE, tokens received in H225 CONNECT will be not passed to the other leg if the following CLI is enabled:

  voice service voip supplementary-service media-renegotiate

  Workaround: Disable the **supplementary-service media-renegotiate** command under **voice service voip**.

- CSCsq81116

  Symptoms: Router may reload when Optimized Edge Routing (OER) master configuration is **shut/no shut**.

  Conditions: Only occurs when OER master controller goes down and then rarely.

  Workaround: There is no workaround.

- CSCsq92063

  Symptoms: Router may crash.

  Conditions: This symptom is observed when Flexible NetFlow is configured with a flow record that includes layer 4 fields and the flow monitor is applied to IPv6 traffic, and the traffic that FNF is monitoring has a payload length that does not allow us to reach the transport header in the IPv6 packet.

  Workaround: Configure Flexible NetFlow with a record that does not have any layer 4 (transport) fields.

- CSCsr09062

  Symptoms: Cisco 7200 crashes due to memory corruption.

  Conditions: Occurs when MLP+QoS is configured on a Cisco 7200 router. QoS policy is having bandwidth, change the BW parameter and flap the multilink using **clear int multilink1** to see the crash.

  Workaround: There is no workaround.

- CSCsr14879

  Symptoms: The device crashes when it boots up.

  Conditions: Occurs on a router running the svcmwam-g8is-mz image.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(15)T17

Cisco IOS Release 12.4(15)T17 is a rebuild release for Cisco IOS Release 12.4(15)T. The caveats in this section are resolved in Cisco IOS Release 12.4(15)T17 but may be open in previous Cisco IOS releases.

- CSCtd67940

  Symptoms: A Cisco router may crash while traffic is flowing through the ATM AIM interface.

  Conditions: This symptom is observed when a QoS configuration is copied/modified while traffic is flowing through the ATM AIM interface. This affects the interface even if minimal traffic is flowing through it.

  Workaround: Stop the traffic (for example, using the **sh** command), copy the configuration, verify that the interface comes up with the new configuration, and then restart the traffic.

- CSCtg47129

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

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

  This advisory is available at the following link:

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

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

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

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

- CSCti10222

  Symptoms: The following exceptions are seen:

```
%SYS-2-MALLOCFAIL: Memory allocation of XXXX bytes failed from 0xYYYYYYYY,
alignment # Pool: I/O  Free: #  Cause: Memory fragmentation Alternate Pool:
None  Free: 0  Cause: No Alternate pool
-Process= "IGMP Snooping Receiving Process", ipl= #, pid= #,  -Traceback=
0x81E8B6BCz 0x81EB0660z 0x802EC198z 0x802EC8E4z 0x802ED88Cz 0x802F1988z
0x803BBD88z 0x803BBF2Cz 0x8045E5CCz 0x804615F4z

 Can't duplicate packet
 Can't duplicate packet
 Can't duplicate packet
```

  Conditions: This symptom is observed when VLANs are added while multicast traffic is flowing through the router.

  Workaround 1: Prune the multicast feed that is coming from the respective VLAN using the following command: **switchport trunk allowed vlans except <mcast vlan#>**.

  Workaround 2: Upgrade to Cisco IOS Release 15.1(2)T1.

- CSCtj33003

  A vulnerability exists in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause an affected device to reload. Affected devices must be configured to process SIP messages and for pass-through of Session Description Protocol (SDP) for this vulnerability to be exploitable.

  Cisco has released free software updates that address this vulnerability. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerability.

  This advisory is available at the following link:

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

- CSCto32044

  Symptoms: The interface hangs and fails to pass traffic. It will still show an "up/up" status but the input and output rates will go to 0. The following errors will be seen:

```
%SBETH-3-ERRINT: GigabitEthernet0/0, error interrupt, mac_status =
0x0000040000000000
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to reset
```

  The interface number will vary.

  Conditions: The conditions are unknown.

  Workaround: There is no workaround.

- CSCto60047

  Symptoms: A crash occurs either due to a chunk corruption or at ssh_send_queue_data.

Conditions: This symptom occurs under the following conditions:

- An SSH session exists between two routers.
- The **show tech** command is issued and then aborted.

Workaround: There is no workaround.

- CSCtr28857

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

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available. This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-msdp

- CSCtr91106

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

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

  Cisco has released free software updates that address these vulnerabilities.

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

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai

- CSCts38429

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

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

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-ike

- CSCtu02835

  Symptoms: While running Cisco IOS Release 15.1(4)M2, slow performance is exhibited through the Fast Ethernet WAN ports.

  Conditions: This symptom is observed when the **scheduler interval** command is configured. This causes the Fast Ethernet WAN ports to display many throttles in the **show interface** command.

  Workaround: Remove the **scheduler interval** command.

Resolved Caveats—Cisco IOS Release 12.4(15)T16

Cisco IOS Release 12.4(15)T16 is a rebuild release for Cisco IOS Release 12.4(15)T. The caveats in this section are resolved in Cisco IOS Release 12.4(15)T16 but may be open in previous Cisco IOS releases.

- CSCsl11129

  Symptoms: A Cisco IOS device configured with Cisco IOS Gateway for T.37 On-Ramp Fax Support may crash with a bus error.

  Conditions: The device is configured for:

  1. Cisco IOS Gateway for T.37 On-Ramp Fax Support.
  2. The combination of both the configured **hostname** and **ip domain-name** has characters exceeding 50 characters.

  Workaround: Reduce the size of the hostname.

- CSCso02147

  The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:

  - NetMeeting Directory (Lightweight Directory Access Protocol, LDAP)
  - Session Initiation Protocol (Multiple vulnerabilities)
  - H.323 protocol

  All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-nat.shtml.

- CSCso30221

  Symptoms: Service policy removed from ATM interface after changing ABR value in ATM PVC.

  Conditions: Happens with a Cisco 7200 router which is running Cisco IOS version 12.4(19.9)T1. This is a platform-independent defect. Last pass release is Cisco IOS Release 12.4(17.9)T.

  Workaround: There is no workaround.

- CSCso33003

  Symptoms: If a child policy is attached to a parent policy twice, the router will reload if the child policy configuration is removed.

  Conditions: The parent policy needs to be attached to the target interface.

  Workaround: Do not attach the same child policy twice in the same parent policy. Use a different policy instead.

- CSCso46409

  Symptoms: mbrd_netio_isr and crypto_engine_hsp_hipri traceback log messages are produced.

  Conditions: This symptom is observed using WebVPN on a Cisco 3845 with an AIM- VPN/SSL-3.

  Workaround: There is no workaround.

- CSCsu95080

  Symptoms: A router remains in the init_process state when parsing the configuration.

Conditions: The symptom is observed when an IPv6 multicast group joins without MLD configured. When the groups unjoin, the system suspends.

Workaround: Configure MLD.

- CSCsw70555

  Symptoms: A Cisco 1811 V.92 interface sees CRC errors against different modems using Pagent.

  Conditions: This symptom occurs when50 PPS of 64-byte frames are being sent in each direction through the V.92 interface on the Cisco 181x.

  Workaround: Configure the **no ppp microcode** command under the async interface.

- CSCsw99171

  Symptoms: The Xconnect feature does not function properly. Packets sent to an interface with **xconnect** *peer router* **1 encapsulation mpls** configured are dropped.

  Conditions: The problem occurs only when Xconnect is configured on an interface.

  Workaround: Do not configure the Xconnect feature.

  Further Problem Description: Cisco 7300 platforms also do not support native vlan when Xconnect is configured on the same subinterface.

- CSCsz39222

  Symptoms: The Cisco CMTS reloads and crash file indicates a cache error.

  Conditions: This issue is observed when register 26/0 contains 0xC0000000.

  This issue affects the NPE-G1 on a Cisco 7200 platform, and the PRE4 on a Cisco UBR10012 router. NPE-G2 is not affected. There is no specific trigger for this failure other than having a single bit parity error on ECC memory.

  Workaround: There is no workaround.

  Further Problem Description: This symptom does not cause a parity error or actually cause the crash. This symptom is just to add a error handler for the specific case of a single bit correctable parity error in ECC memory. The crash results from the parity error itself. The following is an example of the beginning of a crashinfo collection for a hardware corrected cache error:

```
Cache error detected!
   CPO_ECC     (reg 26/0): 0xC0000000
   CPO_CACHERI (reg 27/0): 0x34001DE0
   CPO_CACHERD (reg 27/1): 0x10800580
   CPO_CCHEDPA (reg 27/3): 0x017B4580
```

- CSCsz97833

  Symptoms: HTTP-based certificate revocation list (CRL) checking fails.

  Conditions: This symptom occurs due to an extra character appended to the URL.

  Workaround: Disable CRL checking.

- CSCtb36521

  Symptoms: A Cisco Catalyst 6500 may stop processing IKE traffic, which results in IPSec tunnels not working. Under extreme circumstances, system IO memory might become completely depleted, at which point all traffic processing will stop.

Conditions: This symptom is observed on a Cisco Catalyst 6500 with a VPN-SPA module running a Cisco IOS SXH image when PKI infrastructure is used to authenticate IKE peers. The certificate in use must contain a CDP that uses HTTP protocol to retrieve the CRL. Revocation-check must be configured to fetch the CRL using the **revocation-check** *crl* or **revocation-check** *crl none* command.

Workaround: Disable CRL validation by using the **revocation- check** *none* command instead of the **revocation-check** *crl* or **revocation-check** *crl none* commands in the trustpoint being used. Note that disabling CRL validation poses a possible security risk.

Alternate Workaround: Create a certificate map tied to the trustpoint in use to override the CDP using a URL which specifies the IP address of the CDP server instead of a name.

For example, if the router1 certificate tied to cdp_override trustpoint contains a CDP URL such as:

http://ca_server.yourdomain.com:80/crl.txt

replace it with the ca_server.yourdomain.com IP address by using:

crypto pki trustpoint cdp_override match certificate cert_map_1 override cdp url http://XXX.xxx.x.x:xx/crl.txt

crypto pki certificate map cert_map_1 1 subject-name co router1

- CSCtb72550

  Symptoms: Call Detail Record (CDR) files pushed via FTP are not created on the FTP server.

  Conditions: This symptom is observed when the **gw-accounting** *file* command is configured to point to an FTP server.

  Workaround: Push the CDR records locally to the flash instead of to an FTP URL.

- CSCte98702

  Symptoms: When using NAT, "%SYS-3-INVMEMINT and %SYS-2-MALLOCFAIL" are printed to the console and no traffic passes.

  Conditions: The symptom is observed when NAT is configured.

  Workaround: There is no workaround.

- CSCth11006

  The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:

  - NetMeeting Directory (Lightweight Directory Access Protocol, LDAP)
  - Session Initiation Protocol (Multiple vulnerabilities)
  - H.323 protocol

  All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-nat.shtml.

- CSCth87458

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

  Conditions: This was experienced during internal protocol robustness testing.

  Workaround: Allow SSH connections only from trusted hosts.

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

https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:S/C:N/I:N/A:C/E:F/RL:OF/RC:C CVE ID CVE-2011-2568

has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCti13493

  Symptoms: A router crashes and the following traceback is seen:

  ```
  ASSERTION FAILED : ../voip/ccvtsp/vtsp.c: vtsp_cdb_assert: 1491: unkn - Traceback=
  ASSERTION FAILED : ../voip/ccvtsp/vtsp.c: vtsp_cdb_assert: 1491: unkn - Traceback=
  %SYS-3-MGDTIMER: Uninitialized timer, timer stop, timer = 47523D58. - Process= "DSMP",
  ipl= 0, pid= 226, -Traceback=

  TLB (load or instruction fetch) exception, CPU signal 10, PC = 0x430853EC
  ```

  Conditions: The symptom is observed with the DSMP process.

  Workaround: There is no workaround.

- CSCti48483

  The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:

  - NetMeeting Directory (Lightweight Directory Access Protocol, LDAP)
  - Session Initiation Protocol (Multiple vulnerabilities)
  - H.323 protocol

  All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-nat.shtml.

- CSCtj81533

  Symptoms: The following error messages is seen:

  ```
  np_vsmgr_modify_connection: invalid service id 11 passed
  ```

  No detrimental consequences or effects on the correct operation of the router are observed; however, thousands of these error messages may appear on the console.

  Conditions: This symptom is observed on Cisco AS5400 platforms during VoIP calls, and is more evident when the router is handling multiple calls.

  Workaround: There is no workaround.

- CSCtk53674

  Symptoms: An rtr running Cisco IOS Release 12.4(15)T14 and Cisco IOS Release 15.0M will crash when SNMP v3 configuration is removed.

  Conditions: This symptom occurs when the running configuration contains the following depending on the Cisco IOS Release:

  Cisco IOS Release 12.4(15)T14 snmp-server user QOSqosuser1 QOSqosgroup v3 enc auth sha <DIGEST> priv aes 128 qosQOO!priv acc SNMP

  Cisco IOS Release 15.0(1)M4 snmp-server user QOSqosuser1 QOSqosgroup v3 enc auth sha <DIGEST> priv aes 128 qosQOO!priv acc SNMP

When you remove the above configuration using the **no snmp-server user** command, the rtr crashes.

Workaround: There is no workaround.

- CSCtk67934

  Symptoms: A Cisco router is forced to reload after a few days of encryption and decryption while processing high traffic.

  Conditions: This symptom is observed when VSA is enabled as a hardware crypto engine used for processing both firewall and encryption/decryption on the same interface.

  Workaround: Switch from VSA HW crypto engine to either SW crypto engine or VAM2+ HW crypto engine.

- CSCtl19305

  Symptoms: %SYS-2-BADSHARE: Bad refcount is seen in datagram_done in udp process. The **show ip traffic** command will show the “no port” counter incrementing under the UDP section:

  UDP statistics: Rcvd: 3218 total, 0 checksum errors, 25 no port

  Conditions: This message is a side effect of a packet being incorrectly dropped in the process switching path after having translation done by NAT. One way this scenario is seen is having “ip nat outside source static ...” configured.

  Workaround: There is no workaround.

- CSCtl20508

  Symptoms: A Cisco router fails to decrypt a packet, and for all packets received, the following message is logged:

  ```
  IPSEC(epa_des_crypt): decrypted packet failed SA identity check
  ```

  In the “sh crypto ipsec sa”, the counter which increases is the “#recv errors’’.

  Conditions: This symptom is observed on a Cisco 3270 running Cisco IOS Release 15.0(1)M4. The tunnel interface has a crypto ipsec profile. Transport mode is being used. Packets received on this tunnel are not properly decrypted.

  This issue is not observed when reverting to default tunnel mode.

  Workaround: There is no workaround.

- CSCtl54975

  Symptoms: A small number of Cisco 1812 routers have been observed to unexpectedly restart due to software-forced crashes, repeatedly.

  Conditions: Unknown.

  Workaround: While the root cause is being investigated, units that are experiencing this problem should be replaced. Please replace the Cisco 1812 and send the unit for Failure Analysis, after contacting the Cisco TAC and referencing this bug ID.

- CSCtn00405

  Symptoms: A Cisco router may crash when “isdn test call” is run.

  Conditions: This symptom has been experienced on multiple IOS versions, including Cisco IOS Release 12.4(15)10, 12.4(24)T4, and 15.0(1)M4.

  Workaround: There is no workaround.

- CSCtn65060

  Symptoms: A Cisco device crashes.

Conditions: This symptom is observed with Cisco IOS Release 15.0M and Release 15.1T when configuring “snmp-server community A ro ipv6 IPv6_ACL IPv4_ACL.”

Workaround: Avoid using the **snmp-server community A ro ipv6 IPv6_ACL IPv4_ACL** command.

- CSCtn65655

  Symptoms: The applied QoS policy is not seen, after it is removed from the PVC and re-applied.

  Conditions: Both the input policy and the output policy must be applied. The issue was not seen with only one policy applied in the lab.

  1. Both service policies are applied to the OUT and IN directions on the ATM PVC.
  2. Remove the service policy applied to the OUT direction.
  3. Exit from ATM PVC mode, enter ATM PVC mode again, and confirm that the policy is removed.
  4. Re-apply the service policy and exit.
  5. The OUTBOUND policy is not applied (nothing shows up in “show policy-map int *target* out”) though upon “show run” the configuration is seen.

  Workaround 1: Perform a shut/no shut on the PVC in order for the policy map to be applied correctly.

  Workaround 2: (Affects both inbound and outbound policies):

  1. Remove both the input and output service policies from the PVC.
  2. Exit configuration mode.
  3. Make necessary changes to policy maps (for example, policing rates, WRED thresholds).
  4. Re-add both the input and output service polices to the PVC.
  5. Exit configuration mode.

  Workaround 3: (Affects only the outbound policy):

  1. Remove the output service policies from the PVC.
  2. Add the “junk” outbound service policy to the PVC.
  3. Exit configuration mode.
  4. Make necessary changes to policy maps (for example, policing rates, WRED thresholds).
  5. Remove the outbound “junk” service policy from the PVC.
  6. Re-add the original outbound service policy to the PVC.
  7. Exit configuration mode.

- CSCtn74169

  Symptoms: Crash by memory corruption occurs in the “EzVPN Web-intercept daemon” process

  Conditions: This symptom is observed when EzVPN server pushes a long banner to the client after HTTP authentication using HTTP intercept

  Workaround: Do not use long banner in HTTP intercept.

- CSCtn77090

  Symptoms: Gradual increase of CPU with CPU topping at 99% and increase in holding memory for IP SLA process may cause crash on routers that are running IP SLA probes, generally above 300 probes.

Conditions: This symptom is observed when there are more than 20 SNMP simultaneous probe restarts from IP SLA management software.

Workaround: Limit SNMP probe restarts to under 20 from IP SLA management software.

- CSCto02448

  Symptoms: On doing an inbound route refresh, the AS-PATH attribute is lost.

  Conditions: This symptom is observed with the following conditions:

  1. The neighbor is configured with soft-reconfiguration inbound.
  2. The inbound routemap is not configured for the neighbor
  3. The non-routemap inbound policy (filter-list) allows the path.

  Workaround: Instead of using the non-routemap inbound policy, use the routemap inbound policy to filter the prefixes.

- CSCto02997

  Symptoms: HSRP hangs in INIT state.

  Conditions: This symptom occurs after reloading a Cisco 7200 series router on Cisco IOS Release 12.4(15)T13b with HSRP configured on a LAN interface. The interface will come up, but HSRP will be stuck in INIT state.

  Workaround: Flap the hsrp enabled interface to correct the problem.

  In Cisco IOS Release 12.4(24)T and later releases, the code in this timer area is different so this caveat does not directly apply.

  In Cisco IOS Release 12.4(24)T and later releases, if the problem is observed, it should be possible to configure “standby delay reload” for 5 seconds to allow time for the interface notification to occur.

- CSCto08754

  Symptoms: The crypto VTI interface with ip unnumbered VTI may experience input queue wedge. When the interface becomes wedged, all incoming traffic from the tunnel drops.

  Conditions: This symptom occurs when the crypto VTI interface becomes wedged.

  Workaround: There is no workaround.

- CSCto88686

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities. Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.

  Cisco has released free software updates that address these vulnerabilities. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-sip.shtml.

- CSCtq07413

  Symptoms: A hardware crypto engine may fail to decrypt packets. An “invalid parameter” error is seen after decryption. Software encryption works fine.

  Conditions: This symptom is observed in Cisco IOS Release 12.4.15T6.

  Workaround: Use software encryption.

- CSCtq63838

  Symptoms: A Cisco 2921 router crashes, and the following traceback is seen:

  ```
  ASSERTION FAILED : ../voip/ccvtsp/vtsp.c: vtsp_cdb_assert: 1528: unkn -Traceback=
  0x24A19810z 0x24A5DC8Cz 0x24A4A560z 0x24DF6618z 0x24DF6BBCz 0x24A2DD5Cz 0x24A2E274z
  0x233DEA40z 0x233DEA24z

  ASSERTION FAILED : ../voip/ccvtsp/vtsp.c: vtsp_cdb_assert: 1528: unkn -Traceback=
  0x24A19810z 0x24A5DC8Cz 0x24A4A7E0z 0x24DF6618z 0x24DF6BBCz 0x24A2DD5Cz 0x24A2E274z
  0x233DEA40z 0x233DEA24z

  %SYS-3-MGDTIMER: Uninitialized timer, timer stop, timer = 315556E0. -Process= "DSMP",
  ipl= 0, pid= 306, -Traceback= 0x246EBB2Cz 0x24719984z 0x24A19810z 0x24A5DC8Cz
  0x24A4A7E0z 0x24DF6618z 0x24DF6BBCz 0x24A2DD5Cz 0x24A2E274z 0x233DEA40z 0x233DEA24z
  23:50:00 UTC Sun May 1 2011: TLB (load or instruction fetch) exception, CPU signal
  10, PC = 0x2581FB94
  ```

  Conditions: This symptom is observed with the DSMP process.

  Workaround: There is no workaround.

- CSCtr15891

  Symptoms: On-demand DPD is being sent on every IPsec SA even though a response is seen on at least one of them.

  Conditions: Periodic DPD is configured, and multiple IPsec SAs exist with the peer with outbound traffic flowing on each of them without any inbound traffic.

  Workaround: There is no workaround.

- CSCtr36023

  Symptoms: Traceback is printed on console when traffic is flowing through.

  Conditions: This symptom is seen with MPLS VPN setup with VRF-aware NAT configured.

  Workaround: There is no workaround.

- CSCtr49064

  The Secure Shell (SSH) server implementation in Cisco IOS Software and Cisco IOS XE Software contains a denial of service (DoS) vulnerability in the SSH version 2 (SSHv2) feature. An unauthenticated, remote attacker could exploit this vulnerability by attempting a reverse SSH login with a crafted username. Successful exploitation of this vulnerability could allow an attacker to create a DoS condition by causing the device to reload. Repeated exploits could create a sustained DoS condition.

  The SSH server in Cisco IOS Software and Cisco IOS XE Software is an optional service, but its use is highly recommended as a security best practice for the management of Cisco IOS devices. Devices that are not configured to accept SSHv2 connections are not affected by this vulnerability.

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

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-ssh

- CSCtr54327

  Symptoms: A Cisco router may crash due to a SegV exception or have a spurious access when a fax comes in.

  Conditions: The crash occurs on a voice gateway that is configured with transcoding and fax passthrough where a fax call comes in for a codec, but the fax is not configured for a codec, and the “a=silenceSupp:off” option is set in SDP.

  Workaround: There is no workaround.

- CSCtr56914

  Symptoms: Analog port on a Cisco VG224 gets in a hung state.

  Conditions: This symptom occurs under the following conditions:

  - IP Phone sources call to SCCP FXS port on VG224.
  - IP Phone goes onhook.
  - IP Phone sends new call prior to analog phone physically going on-hook.
  - Analog port is hung due timing issue.

  Workaround: Reload device to clear the DSP state.

- CSCtr70232

  Symptoms: An IP fragment that is received on dialer interface in CEF path may bypass virtual fragment reassembly (VFR) processing and create a VFR timeout, causing additional inner IP fragments to be dropped.

  This can cause problems where the first inner IP fragment was IPSec encapsulated and then IPSec fragmented, due to the fragmentation after encryption. The IPSec packets corresponding to the first inner IP fragment after decryption will be given to VFR for processing. The second inner IP fragment may be a smaller packet that does not require IPSec fragmentation and after decryption, may bypass VFR processing. This will result in dropping of the first inner ip fragment due to a VFR timeout as the second IP fragment bypasses VFR processing.

  Conditions: This symptom occurs under the following conditions:

  1. VFR is enabled on decryption side and on dialer interface with CEF turned on.
  2. Fragmentation after encryption is used on encryption side.
  3. The inner IP packet is fragmented when received by the encrypting router.

  Workaround: Perform fragmentation before encryption on the sending side and ensure that the proper IP MTU is used on the tunnel so that no fragmentation occurs after encryption.

- CSCtr83659

  Symptoms: GETVPN group members stop communicating with each other after a partial network outage.

  Conditions: This symptom is seen when a MPLS outage occurs with the following characteristics:

  - Traffic flow stops between KS-1 and KS-2.
  - KS-2 can send rekey to GM-1 and GM-2. However, ACKs from these two GMs cannot reach KS-2.

  Outage does not need to be MPLS related.

  Workaround: There is no workaround.

- CSCtr97640

  Symptoms: Start-up configuration could still be retrieved bypassing the “no service password-recovery” feature.

  Conditions: None.

  Workaround: There is no workaround. Physically securing the router is important.

  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 1.9/1.8:

https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:L/AC:M/Au:N/C:N/I:P/A:N/E:F/RL:U/RC:C CVE ID CVE-2011-3289

has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

Resolved Caveats—Cisco IOS Release 12.4(15)T15

Cisco IOS Release 12.4(15)T15 is a rebuild release for Cisco IOS Release 12.4(15)T. The caveats in this section are resolved in Cisco IOS Release 12.4(15)T15 but may be open in previous Cisco IOS releases.

- CSCdw49329

  Symptoms: A Cisco 3660 router may reload with a bus error.

  Conditions: The stack trace indicates that the CPU has attempted to access an invalid address while the router is executing Network Time Protocol (NTP) functions.

  Workaround: Disable NTP on the router.

- CSCsg31704

  Symptoms: CPU utilization spikes when the **show running-config** command is issued.

  Conditions: This symptom is observed when the **show running-config** command is issued.

  Workaround: There is no workaround.

- CSCsh64365

  Symptoms: A ping does not yield a 100-percent result after you have entered the **no set-overload-bit** command for an IS-IS configuration.

  Conditions: This symptom is observed on a Cisco 7200 series but is not platform-specific.

  Workaround: There is no workaround.

- CSCsj01961

  Symptoms: A router may not boot and may generate an "INSUFFICIENT MEMORY" error message.

  Conditions: This symptom is observed on a Cisco 7600 series that has an RSP720 when the ifIndex table is corrupt, preventing SNMP from initializing because SNMP attempts to use the ifIndex table from NVRAM.

  Workaround: There is no workaround.

- CSCsk48102

  Symptoms: A supervisor crashes at ru_transfer_buffer_allocation().

  Conditions: This symptom is a very rare random occurrence that occurs only in devices that have an uptime of over 1 year. In some cases, the devices were up for over 2 years before encountering this problem.

  Workaround: There is no workaround. Reloading resolves the issue; the device resumes normal operation after the crash.

- CSCsk98507

  Symptoms: Router crashes after IPX routing is enabled.

Conditions: Problem happens only if an interface which has IPX network configuration is deleted after disabling IPX routing.

Workaround: There is no workaround.

- CSCsr70963

  Symptoms: A Cisco 10000 PRE will reload unexpectedly when a radius server which is marked as dead is removed from the configuration during authentication of sessions.

  Conditions: The issue is seen when a RADIUS server is marked as dead. There are attempts to retry and access the server during its removal from the configuration.

  Workaround: There is no workaround.

- CSCsu31853

  Symptoms: TCP sessions in TIMEWAIT state cause buffer usage until they move to CLOSED state.

  Conditions: This symptom is observed with almost all TCP applications. It is mainly seen on low end switches.

  Workaround: There is no workaround.

- CSCsv03300

  Symptoms: Cisco 7200 NPEG2 router crashes while displaying the interface output for onboard Gigabit Ethernet using the **show interface gig0/x** command.

  Conditions: Occurs when a CBWFQ QoS policy is attached to the onboard Gigabit Ethernet interface.

  Workaround: There is no workaround.

- CSCsv38205

  Symptoms: Running a post-dial delay operation with reaction configuration may cause a router to crash after removing the operation.

  Conditions: The symptom is observed when using a post-dial delay operation with reaction configuration.

  Workaround: Do not use reaction configuration for post-dial delay.

- CSCsv97424

  Symptoms: A router will reload due to memory corruption in the I/O pool. As an indication for this bug, we will see the same caller PC in the output of the **show buffer pool Serial0/0/0** command.

  Conditions: This symptom is observed on Cisco routers that are running the adventerprisek9_ivs-mz feature set and when packets are being processed by an ATM interface.

  Frequency: Always.

  Workaround: We can overcome the reload issue by disabling hardware crypto using the following command in global configuration mode: **no crypto engine accelerator**.

  Note When hardware crypto is turned off, encryption and de-cryption will be done by software and not by hardware. This can slightly hike CPU utilization, which should not be an issue as long as we do not encounter a huge volume of traffic.

- CSCsy77298

  Symptoms: Option 82 is not appended in DHCP NAK packet by DHCP server.

  Conditions: Not any specific condition.

Workaround: There is no workaround.

- CSCsz07103

  Symptoms: A router crashes at nvgen_action when 500 IPSec tunnels are configured and the **write memory** command is issued.

  Conditions: This symptom is observed when 500 IPSec tunnels are configured and the **write memory** command is issued. The problem might be a scalability issue.

  Workaround: There is no workaround.

- CSCta38476

  Symptoms: When removing the tunnel interface with CDP enabled, tracebacks are generated. CDP does not come up in all interfaces.

  Conditions: The symptom is observed with large numbers of CDP neighbors in an MCP router.

  Workaround: Disable CDP before deleting the tunnel interface.

  Further Problem Description: CDP tries to send a packet over a deleted tunnel interface causing the issue.

- CSCta95295

  Symptoms: A Cisco router terminates 100+ VPN tunnels when using CRL checking for the Phase 1 authentication.

  Conditions: If IKE gets stuck for any reason, it might cause IOMEM to be depleted completely, which could lead to a router crash.

  Workaround: Disable CRL checking or use pre-shared keys.

- CSCtb17152

  Symptoms: A large packet drop may occur when FRF.12 is enabled.

  Conditions: This symptom is observed when FRF.12 is enabled.

  Workaround: There is no workaround.

- CSCtb34358

  Symptoms: Tunnel sources get mixed up when tunnel interfaces are configured with serial subinterfaces as sources and the router is reloaded.

  Conditions: The symptom occurs only after a reload or when a saved configuration is applied to the running configuration.

  Workaround: There is no workaround.

- CSCtc06935

  Symptoms:

  Packet loss occurs between two Cisco 3200 MAR routers that are connected over FESMIC Fast Ethernet ports via wireless radios after upgrading to Cisco IOS Release 12.4(22)T2.

  Conditions: The symptom is observed under the following conditions:

  - After a code upgrade.
  - On Cisco 3200 routers that are connected via wireless radios.
  - It does not occur on devices directly connected via fiber.

  Workaround: Use Cisco IOS Release 12.4(1a).

- CSCtc65347

  Symptoms: A Cisco 3845 may have a processor pool memory leak in the SNMP Engine.

  Conditions: This symptom is observed on a Cisco 3845 that is running Cisco IOS Release 12.4(20)T1 and polling specific VoIP MIBs.

  Workaround: Do not poll VoIP Peer CFG Entry MIBs or use an SNMP view to block the router from replying to said poll, such as:

  snmp-server view leak internet included
  snmp-server view leak cvVoIPPeerCfgEntry excluded
  snmp-server community <community name> view leak

  Further Problem Description: “Show proc mem <pid>” (where <pid> is the process ID for the SNMP ENGINE) should decode to VoIP Peer Cfg Entry MIBs being polled.

- CSCtd39579

  Symptoms: A router crashes when we try to remove a service policy/WAAS from an interface.

  Conditions: Traffic should be hitting the interface, CPU utilization should be high, and NAT should be applied on the interface.

  Workaround:

  1. Remove NAT from the interface.

  2. Remove the service policy.

  3. Re-apply NAT.

- CSCtd74470

  Symptoms: Voice ports on gateways configured for E1 R2 intermittently get stuck in the “clearfwd” state and can be returned to normal operation mode only by manual intervention.

  Conditions: When the issue occurs, the following states are observed by examining the stuck port with **show** commands:

```
Router# show vo po su | include clearfwd

0/3/0:1 24 r2-digital up up clearfwd idle y

Show voice trace 0/3/0.1.24 0/3/0:1 24

State Transitions: timestamp (state, event) -> (state, event) ...
3440023.272 (R2_Q421_IDLE, E_HTSP_SETUP_REQ) ->
3440023.380 (R2_Q421_OG_SEIZE, E_DSP_SIG_1100) ->
3440047.816 (R2_Q421_OG_SEIZE_ACK, E_R2_REG_ABORT_DIGIT_COLLECT) ->
3440047.816 (R2_Q421_OG_CLR_FWD, E_DSP_DIALING_DONE) ->
3440048.816 (R2_Q421_OG_CLR_FWD, E_HTSP_EVENT_TIMER) - >
3440050.816 (R2_Q421_WAIT_IDLE, E_HTSP_EVENT_TIMER) ->
3440050.816 (R2_Q421_WAIT_IDLE, E_DSP_SIG_1100) ->
3440050.820 (R2_Q421_BLOCKED, E_DSP_SIG_1100) ->
3440069.960 (R2_Q421_BLOCKED, E_HTSP_RELEASE_REQ) ->
3440113.512 (R2_Q421_BLOCKED, E_DSP_SIG_1000) ->) ->
```

Workaround: Perform a shut/no shut on the controller or busy-out the channel:

```
Router# sh vo po sum | include clearfwd

0/3/0:1 24 r2-digital up up clearfwd idle y
0/2/0:1 21 r2-digital up up clearfwd idle y
0/2/0:1 29 r2-digital up up clearfwd idle y
0/2/0:1 30 r2-digital up up clearfwd idle y
Router# conf term
Enter configuration commands, one per line. End with CNTL/Z:
Router(config)# control
Router(config)# controll
Router(config)# controller E1 0/2/0
Router(config-controller)# ds0 busyout 21,29,30,24
Router(config-controller)# no ds0 busyout 21,29,30,24
Router(config-controller)# end
Router# sh vo po sum | include clearfwd
Router#
```

- CSCtd75189

  Symptoms: Continuous error message similar to the one below are recorded on voice gateway:

  ```
  SYS-2-INPUTQ: INPUTQ set, but no IDB, ptr=6818DA34, -Traceback=
  ```

  Conditions: The symptom is observed on a voice gateway that is running Cisco IOS Release 12.4(24)T2.

  Workaround: There is no workaround.

- CSCte43663

  Symptoms: RTCP packets are not forwarded across the network.

  Conditions: This symptom is observed in an IPIPGW configuration.

  Workaround: There is no workaround.

- CSCte61495

  Symptoms: The following messages are seen with tracebacks:

  ```
  %SYS-3-CPUHOG: Task is running for (2004)msecs, more than (2000)msecs (4/4),process
  = Exec. %SYS-2-INTSCHED: 'suspend' at level 3 -Process= "Exec", ipl= 3, pid= 128,
  ```

  Conditions: The symptom is observed when a large ACL is configured for the service policy. This happens only under ATM subinterfaces.

  Workaround: Use small-sized ACLs for the service policy.

- CSCtf23298

  Symptoms: There is high CPU usage when a Terminal Access Controller Access- Control System (TACACS) server is configured with a single connection.

  Conditions: This symptom occurs when a Terminal Access Controller Access- Control System (TACACS) server is configured with a single connection.

  Workaround: Remove single connection option.

- CSCtf39455

  Symptoms: Router can hang when xconnect configuration is modified on a VLAN subinterface while data packets are being switched. The following error traceback is printed:

  ```
  %SYS-2-NOTQ: unqueue didn't find 0 in queue
  ```

  Conditions: The symptom is observed when the VLAN subinterface is still seeing data traffic and the main interface is not shut down, and when the xconnect configuration on the VLAN subinterface is being modified.

Workaround: Shut down the main ethernet interface when doing xconnect configuration changes on the subinterface.

- CSCtf56107

  Symptoms: A router processing a unknown notify message may run into a loop without relinquishing control, kicking off the watch dog timer and resulting in a software-based reload.

  Conditions: The symptom is observed when an unknown notify message is received.

  Workaround: There is no workaround.

- CSCtf75053

  Symptoms: DHCP Relay will send a malformed DHCP-NAK packet. The malformed packet will be missing the END option (255) and the packet's length will be truncated to 300. In effect, all the options after 300 bytes, if any, will be missing.

  Conditions: When a Cisco 10000 series router is configured as a relay and a DHCP request is sent from the CPE, the router will send a DHCP-NAK when client moves into a new subnet.

  Workaround: There is no workaround.

- CSCtf77047

  Symptoms: Ping ATM subinterface peer IP address has packet loss from Cisco 7206.

  Conditions: This symptom occurs with the following:

  1. NPE-G2+PA-MC-STM-1SMI+PA-A6-OC3SML.

  2. Enable EIGRP on ATM subinterface.

  Workaround: There is no workaround.

- CSCtf99622

  Symptoms: Web Cache Communications Protocol (WCCP) Generic Routing Encapsulation (GRE) returned packet gets dropped on Cisco 7200 series routers, when the interface has multiple sub-interfaces configured in more than one routing domain and is passing SSL/HTTPS traffic.

  Conditions: This symptom occurs when multiple subinterfaces are present on the same physical interface, out of which one subinterface is management and the other subinterfaces are for traffic. The GRE returned packet from the Wide-Area Application Engine (WAE) uses the wrong subinterface (mgmt instead of traffic) to route packet and hence the packet gets dropped no throughput is seen.

  Workaround 1: Use IP Routing Table Manager (RTM) instead of configuring WAE with GRE Routing Transit Number (RTN).

  Workaround 2: Use physical interfaces on the Cisco 7200 platform instead of sub-interfaces.

- CSCth03022

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities. Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.

  Cisco has released free software updates that address these vulnerabilities. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-sip.shtml.

- CSCth15268

  Symptoms: Cisco IOS stops forwarding LLC I frames but continues to respond to poll frames. Finally, Cisco IOS might disconnect the LLC session.

  Conditions: This symptom can happen if the remote client drops an LLC packet with the poll bit on.

  Workaround: Set “llc2 local-window” to 1.

- CSCth20696

  Symptoms: Address Error (load or instruction fetch) exception, CPU signal 10 on a Cisco 7204VXR (NPE-G1).

  Conditions: The symptom is observed with Cisco IOS Release 12.4(25c).

  Workaround: There is no workaround.

- CSCth26441

  Symptoms: Non-broadcast Ethernet frames are dropped by the Gig1/0 controller that connects to the NME module.

  Conditions: This symptom is observed when xconnect is configured on a subinterface and 802.1q trunking is used to connect to the NME module.

  Workaround: There is no workaround.

- CSCth69364

  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://www.cisco.com/warp/public/707/cisco-sa-20110928-dlsw.shtml.

- CSCth95192

  Symptoms: On a Cisco router loaded with Cisco IOS Release 12.0(33)S6, when LSP changes, the CEF table may become stuck with old label information.

  Conditions: This symptom occurs when there are two outgoing links to the BGP next hop for the prefix received via BGP.

  The following is a snapshot of how the CEF table will be during the time of the issue:

```
R1# show ip cef 10.150.150.150 detail

10.150.150.150/32, version 26, epoch 0, cached adjacency 10.1.15.5
0 packets, 0 bytes
  tag information from 10.100.100.0/30, shared, all rewrites owned
    local tag: 33
    fast tag rewrite with Et0/0.12, 10.1.1.1, tags imposed {16}
  via 10.100.100.2, 0 dependencies, recursive
    next hop 10.1.15.5, Ethernet0/0.15 via 10.100.100.0/30 (Default)
    valid cached adjacency
    tag rewrite with Et0/0.15, 10.1.15.5, tags imposed {502}
```

  Workaround: Issue the “clear ip route” command.

- CSCti03808

  Symptoms: A Cisco 7200 may crash with a fatal error.

  Conditions: This symptom is observed only when PA-POS-1OC3 and C7200-VSA port adapters are installed and the encrypted traffic is being sent through the POS interface. The problem is more likely as traffic load increases.

Workaround: Use a different POS port adapter or VAM module instead of the VSA encryption module.

Further problem description: During investigation the router would also occasionally hang instead of crash. With the fix for this symptom the hangs were not seen.

- CSCti25339

  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/en/US/products/products_security_vulnerability_policy.html

- CSCti54173

  Symptoms: A leak of 164 bytes of memory for every packet that is fragmented at high CPU is seen sometime after having leaked all the processor memory. This causes the router to reload.

  Conditions: The symptom is observed on a Cisco 7200 series router.

  Workaround: There is no workaround.

- CSCti62801

  Symptoms: When both Caller-ID (CID) and Call-Waiting (CW) features are enabled on SIP analog endpoint, repetitive Call-Waiting (CW) tone is not played every 10 seconds until call is answered.

  Conditions: The symptom is observed with a SIP analog endpoint on IAD243x, when the Device Service Application (DSAPP) is enabled on the gateway to provide supplementary features using SIP for the phone connected to the FXS port.

  Workaround: There is no workaround.

- CSCti66153

  Symptoms: A Cisco 7200 series router with VSA in GETVPN deployment is logging the following error:

  ```
  %VPN_HW-1-PACKET_ERROR: slot: 0 Packet Encryption/Decryption error, Selector checks.
  ```

  Conditions: The following conditions need to be met:

  - A Cisco 7200 series router with VSA in receive-only mode.
  - Keyserver in receive-only mode.
  - Other GM in passive mode (that is encrypting outbound traffic) sending traffic to the "inside" of the Cisco 7200.
  - Traffic matching a keyserver delivered crypto ACL matching L4 ports (e.g.: **permit tcp any any eq 23**).

  Workaround: Relaxing any of the conditions here above:

  1. Use VAM2+ instead of VSA.

2. Use GETVPN ACL without l4 ports (e.g.: **permit ip any any**).

3. Have the Cisco 7200 in passive mode as well.

4. Do not use receive-only mode on the keyserver.

- CSCti77879

  Symptoms: When the traffic to encrypt matches the first sequence of a crypto map, starting its crypto ACL with a deny statement, the traffic is dropped whether or not this deny statement is a subset of the permits contained in that crypto ACL or not.

  Also, the limitation of 14 denies in an ACL due to the jump behavior does not seem to be present.

  Conditions: The symptom is observed in a VSA installed in a Cisco 7200 series router that is running Cisco IOS Release 15.0(1)M3.

  Workaround: There is no workaround.

  Further Problem Description: As the configuration guide states, the **crypto ipsec ipv4-deny** {**jump | clear | drop**} command should help to avoid this problem, but this command is not available for the VSA, only for VPN SPA.

- CSCti90602

  Symptoms: The PPTP connection is not getting established when “ip nat outside” is configured on the NAT router. The NAT router is between the client and the server.

  Conditions: This symptom is observed only with the PPTP connection; all other traffic works fine.

  Workaround: There is no workaround.

- CSCtj07885

  Symptoms: A Cisco router may unexpectedly reload due to a bus error during an SNMP poll for the ccmeActiveStats MIB.

  Conditions: The router may crash when it is configured as SRST (call-manager-fallback) or CME-as-SRST with “srst mode auto-provision none”, when interworking with SNMP, using the MIB browser query ccmeActiveStats.

  Workaround:

  1) Configure CME-as-SRST with “srst mode auto-provision all”.

  2) Stop the ccmeActiveStats MIB from being polled on the router. There are three possible ways to do this:

  a) Stop the MIB on the NMS device that is doing the polling.

  b) Turn off SNMP polling on the device.

  c) Create a view to block the MIB and apply it to all SNMP communities.

- CSCtj21045

  Symptoms: Header compression decodes RTP timestamp incorrectly.

  Conditions: This issue occurs mainly with IPHC format compression interacting with older Cisco IOS releases.

  Workaround: Use IETF format compression.

- CSCtj86514

  Symptoms: An SNMP walk on Cisco AAL5 MIB may not return information for all PVCs configured on the device.

Conditions: An SNMP walk query on the Cisco AAL5 MIB may fail to return information of bundled PVCs that are in down state. Information about PVCs in UP state is returned correctly.

Workaround: To get information of bundled PVCs in down state, you need to poll with more specific OIDs. Instead of doing an snmpwalk on "1.3.6.1.4.1.9.9.66.1.1.1.1.3", do an snmpget on "1.3.6.1.4.1.9.9.66.1.1.1.1.3.<IfIndex>.<VPI>.<VCI>".

- CSCtj96915

  Symptoms: LNS router hangs up at interrupt level and goes into an infinite loop.

  Conditions: Unknown. See Further Problem Description below.

  Workaround: There is no workaround. Only power cycle can remove the symptom.

  Further Problem Description: This is a hypothesis based on analysis of the data provided for the failures experienced by the customer, together with an extensive code review. The issue can happen during L2TP session creation and removal, specifically where a session removal/addition is prevented from being completed by an interrupt, which is raised. We believe this is a timing issue. While this is a rare event, the probability of it occurring increases with load and number of sessions.

- CSCtj99288

  Symptoms: EIGRP neighborship over a DMVPN interface does not scale over approximately 500 neighbors.

  Conditions: The pacing time for EIGRP on the DMVPN (p2mp) interface increases proportionally with the number of peers on the interface.

  Workaround: There is no workaround.

- CSCtk74685

  Symptoms: When H225 messages for a call are sent out to the wrong TCP socket by a Cisco IOS gateway, they may sent to a completely different IP than the one that is aware of the call. When this occurs, the new socket gets paired to the call and the H323 stack tries to tear down the H245 socket for a call that is being disconnected. Instead, it erroneously tears down an unrelated calls H225 socket. This causes the unrelated call to drop.

  Observed with "debug cch323 all" and "debug ip tcp trans:"

  ```
  13090333: Dec 3 13:18:20.965: //137091/80C6B1F78F31/H323/run_h245_iwf_sm: received
  IWF_EV_H245_DISCONN while at state IWF_ACTIVE 13090334: Dec 3 13:18:20.965:
  //137091/80C6B1F78F31/H323/cch323_send_event_to_h245_connection_ sm: Changing to new
  event H245_DISCONNECT_EVENT 13090335: Dec 3 13:18:20.965:
  //137091/80C6B1F78F31/H323/cch323_h245_connection_sm: state=0, event=4,
  ccb=C5E442B8, listen state=2 13090336: Dec 3 13:18:20.965:
  //137091/80C6B1F78F31/H323/cch323_h245_connection_sm: H245_CONNECT: Received event
  H245_DISCONNECT_EVENT while at H245_NONE state 13090337: Dec 3 13:18:20.965: TCP0:
  state was ESTAB -> FINWAIT1 [24696 -> 192.0.2.100(1720)] 13090338: Dec 3 13:18:20.965:
  TCP0: sending FIN
  ```

  Conditions: This symptom occurs with all IOS images with the fix for CSCin76666.

  The cascade issue noted in this bug is triggered by an event where CM closes down an H225 or H245 TCP socket mid-call. Due to the cascading nature of CSCtk74685, identifying the root call that triggers this socket conflict may be extremely difficult, until the fix for CSCtk74685 is applied.

  Workaround: Use one of the following workarounds:

  1. Enable call preservation on CM, which does not prevent the socket from getting torn down, but minimizes user impact and does not drop audio on the call.

  voice service voip h323 call preserve

System > Service Parameters > (Select Publisher Node) > Cisco CallManager > Advanced > Allow Peer to Preserve H.323 Calls > False > Save

2. Run a Cisco IOS release that does not have the fix for CSCin76666.

3. Change the signaling protocol to SIP.

- CSCtk95992

  Symptoms: DLSw circuits to not come up when using peer-on-demand peers.

  Conditions: This symptom occurs when DLSw uses UDP for circuit setup.

  Workaround: Configure the **dlsw udp-disable** command.

  Further Problem Description: This symptom occurs in the following (and later) releases:

  - 12.4(15)T14
  - 12.4(24)T4
  - 15.0(1)M3
  - 15.1(1)S
  - 15.1(2)T
  - 12.2(33)SXI4
  - 12.2(33)SXI4a

- CSCtl21695

  Symptoms: An LNS configured for PPTP aggregation might stop accepting new PPTP connections after PPTP tunnels exceed one million. Debug vpdn l2x ev/er shows:

  PPTP _____:_____: TCP connect reqd from 0.0.0.0:49257

  PPTP _____:_____: PPTP, no cc in l2x

  Conditions: This symptom occurs when LNS is configured for PPTP aggregation and over one millions tunnels have been accepted (on VPDN level).

  Workaround: Reload LNS.

- CSCtl87879

  Symptoms: MGCP calls fail as the DTMF detection and reporting via NTFY message does not occur.

  Conditions: This symptom is observed in Cisco IOS Release 12.4(24)T5 but not in Cisco IOS Release 12.4(24)T4.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(15)T14

Cisco IOS Release 12.4(15)T14 is a rebuild release for Cisco IOS Release 12.4(15)T. The caveats in this section are resolved in Cisco IOS Release 12.4(15)T14 but may be open in previous Cisco IOS releases.

- CSCee93607

  Symptoms: A VPN client cannot connect to a router that functions as an EzVPN server.

  Conditions: This symptom is observed on a Cisco router that functions as an EzVPN server when the user name is not sent in the RADIUS authentication request for the VPN client, causing the authentication server to reject the VPN client.

Workaround: If this is an option, use local authentication.

Further Problem Description: The following error message appears in the debug output:

```
ISAKMP (0:1): FSM action returned error: 4
```

- CSCsc98835

  Symptoms: OSPF and BGP change their states unexpectedly.

  Conditions: This symptom is observed on a Cisco router when a modification of a shared access control list (ACL) that is called from more than 300 route maps causes a CPUHOG condition in the Virtual Exec Process.

  Workaround: There is no workaround.

- CSCsl64247

  Symptoms: A Cisco router crashes 20-30 minutes after configuring “mode route control.”

  Conditions: This symptom is observed when the router is configured as OER master.

  Workaround: There is no workaround.

- CSCsl85654

  Symptoms: A Cisco router acting as the main mode initiator fails to check peer identity against an ISAKMP profile; as a result, a peer with an incorrect id may successfully establish an IPSec tunnel.

  Conditions: This symptom is observed on a Cisco IOS router configured for IPSec and acting as the initiator of IKE (Internet Key Exchange) main mode.

  Workaround: There is no workaround.

- CSCsm51299

  Symptoms: CSCsl27236 did not address all of the issues that needed to be fixed due to code divergence.

  Conditions: The symptoms can be observed under stress conditions and when ipsec-isakmp is enabled.

  Workaround: There is no workaround.

- CSCso55072

  Symptoms: System traceback occurs during TCL code execution, which causes subsequent system reboot.

  Conditions: This symptom is observed when ESM is still processing events in the background and another syslog message is processed from the ESM logger queue.

  Workaround: Avoid ESM filters that execute background events such as CLI commands for an extended period of time (for example, in a loop with a high loop count).

- CSCso55451

  Symptoms: A memory leak occurs in an ipsec-isakmp process.

  Conditions: This symptom is observed with Cisco IOS Release 12.4(19.12)T.

  Workaround: There is no workaround.

- CSCsu26526

  Symptoms: Memory leak can be seen on the LNS.

  Conditions: The symptom is observed on the L2TP Network Server (LNS) when the PPP client does a renegotiation.

  Workaround: There is no workaround.

- CSCsu47486

  Symptoms: Cisco IOS Software configured with MGCP may reload.

  Conditions: This symptom is observed if an authenticated user repeatedly configures **mgcp block-new call**, **no mgcp block-new call** while active calls are being made.

  Workaround: Wait for all active calls to terminate before configuring **no mgcp block-new call**.

- CSCsv43385

  Symptoms: Connectivity from a Dynamic Multipoint VPN (DMVPN) hub router to spokes may be lost due to an invalid Cisco Express Forwarding (CEF) adjacency. If tunnel protection is configured on the hub, the traffic from hub to spokes will be dropped on the tunnel interface and the **show interface tunnels** command will show the "Total output drops" counter incrementing.

  This is intermittent and the problem will generally appear right after a router reloads. It may not occur after all reloads.

  Conditions: This symptom is observed in Cisco IOS Release 12.4(20)T and 12.4(22)T.

  Workaround: Disable, then enable the tunnel mode:

  ```
  interface Tunnel30
  no tunnel mode gre multipoint
  tunnel mode gre multipoint
  ```

  Alternate Workaround: Remove the tunnel configuration and re-add it:

  ```
  no interface Tunnel30
  interface Tunnel30
  ip address 192.168.50.1 255.255.255.0
  ip nhrp authentication cisco
  ip nhrp map multicast dynamic
  ip nhrp network-id 111
  ip nhrp holdtime 900
  tunnel source FastEthernet0/0
  tunnel mode gre multipoint
  ```

- CSCsv79584

  Symptoms: An 0.0.0.0 binding with a 0 minute lease gets created and subsequently removed on the DHCP unnumbered relay.

  Conditions: The DHCP client sends a DHCPINFORM with ciaddr set to its address, but giaddr is empty. The relay fills in giaddr with its IP address and the server replies to giaddr. Since the DHCPACK is in response to DHCPINFOM, the lease-time option is absent. Relay receives the DHCPACK and tries to process it normally leading to the route addition.

  Workaround: There is no workaround.

  Further Problem Description: This behavior can indirectly have a negative impact on the system by triggering other applications to be called because the routing table change is triggered by such DHCP requests. Examining "debug ip routing" for 0.0.0.0/32 reveals 0.0.0.0/32 route flapping.

- CSCsv86288

  Symptoms: A device configured with the NETCONF feature reloads.

  Conditions: This symptom is observed when a device configured for either NETCONF over SSH or NETCONF over BEEP receives a specially crafted packet.

  Workaround: There is no workaround.

  Further Problem Description: To be exploited, the session must first be authenticated.

  For further details on NETCONF over SSH, consult the "NETCONF over SSH" configuration guide at the following link:

http://www.cisco.com/en/US/docs/ios/12_2sr/12_2sra/feature/guide/srnetcon.html

For further details on NETCONF over BEEP, consult the "NETCONF over BEEP" configuration guide at the following link:

http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/htnetbe.html

- CSCsw40203

  Symptoms: A Cisco ASR 1000 may crash with certain malformed IKE packets.

  Conditions: This symptom is observed on a Cisco ASR 1000 that is configured for IPSec VPN with digital certificates.

  Workaround: There is no workaround.

- CSCsw52416

  Symptoms: Dynamic NAT entries are not timing out properly.

  Conditions: This symptom is observed even after the timer expires.

  Workaround: There is no workaround.

- CSCsx08019

  Symptoms: A crash may occur if a trustpoint is removed from a server at the same time as the server is trying to autoenroll.

  Conditions: This symptom is observed when the **no crypto pki trustpoint** *trustpointname* command is issued just as the autoenroll timer goes off.

  Workaround: Do not delete a trustpoint that is about to autoenroll. Either wait until it finishes, or turn autoenroll off before deleting the trustpoint.

- CSCsx83443

  Symptoms: ISKMP debug messages from all peers are shown in the terminal monitor enable tty/vty even though **debug crypto condition peer ipv4 x.x.x.x** is set.

  Conditions: Use peer IP-based debug condition.

  Workaround: There is no workaround.

- CSCsx93245

  Symptoms: A Cisco router may reload after issuing the **show gatekeeper zone prefix all** command.

  Conditions: This symptom is observed on a Cisco 3825 router running Cisco IOS Release 12.4(8a).

  Workaround: There is no workaround.

- CSCsy07953

  Symptoms: Any attempt to copy a file from a router to an FTP server will fail. The FTP error is "No such file or directory."

  Conditions: This is only a problem with FTP and only when transferring to an FTP server. Transfers from an FTP server work as expected.

  Workaround: Use a different file transfer protocol, such as TFTP.

- CSCsy76185

  Symptoms: The following traceback may be seen:

```
Local7.Critical 192.168.133.252 827681: %SYS-2-NOBLOCK: printf with blocking disabled.
Local7.Critical 192.168.133.252 827682: -Process= "IP Input", ipl= 0, pid= 61
Local7.Critical 192.168.133.252 827683: -Traceback= 0x11EF3E4 0x1203120 0x180214C
0x1209F54 0x120A0B8 0x179EF5C 0x19A1F94 0x19A270C 0x19A2930 0x19A2B0C 0x196B6FC
0x196EC44 0x197115C 0x1972F8C 0x17AC2F4 0x17AC87C
```

Conditions: The symptom is observed during basic function.

Workaround: There is no workaround.

- CSCsy88640

  Symptoms: There are two unrelated problems fixed by this bug:

  - Problem 1: A core dump may fail to write, with the following errors seen on the console:

```
current memory block, bp = 0x4B5400A0, memorypool type is Exception data check, ptr =
0x4B5400D0
bp->next(0x00000000) not in any mempool
bp_prev(0x00000000) not in any mempool
writing compressed ftp://10.0.0.1/testuncached_iomem_region.Z
[Failed]
writing compressed ftp://10.0.0.1/testiomem.Z
[Failed]
writing compressed ftp://10.0.0.1/test.Z
[Failed]
%No memory available
```

  - Problem 2: A nested crash might occur while generating a crashinfo. That means that this bug only helps the crashinfo to write properly. It does not fix the cause of the original crash, but will aid investigation.

  Conditions:

  - Problem 1: This is only seen for memory corruption crashes when “exception region-size” is configured to a value that is not divisible by 4.
  - Problem 2: BFD must be configured and sending hellos.

  Workaround:

  - Problem 1: The recommended setting for exception region-size is 262144 in newer images. In older images, where the maximum configurable value is 65536, use the maximum.
  - Problem 2: Disable BFD.

- CSCsz43987

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device when SIP operation is enabled.

  Cisco has released free software updates that address these vulnerabilities. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-sip.shtml.

  Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

  http://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

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

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

Cisco Unified Communications Manager (CUCM) is affected by the vulnerabilities described in this advisory. Two separate Cisco Security Advisories have been published to disclose the vulnerabilities that affect the Cisco Unified Communications Manager at the following locations:

http://www.cisco.com/warp/public/707/cisco-sa-20090826-cucm.shtml

http://www.cisco.com/en/US/products/products_security_advisory09186a0080b4a313.shtml

- CSCsz71787

  Symptoms: A router crashes when it is configured with DLSw.

  Conditions: A vulnerability exists in Cisco IOS software when processing UDP and IP protocol 91 packets. This vulnerability does not affect TCP packet processing. A successful exploitation may result in a reload of the system, leading to a denial of service (DoS) condition.

  Cisco IOS devices that are configured for DLSw with the **dlsw local- peer** command automatically listen for IP protocol 91 packets. A Cisco IOS device that is configured for DLSw with the **dlsw local-peer peer-id** <*IP- address*> command listen for IP protocol 91 packets and UDP port 2067.

  Cisco IOS devices listen to IP protocol 91 packets when DLSw is configured. However, it is only used if DLSw is configured for Fast Sequenced Transport (FST). A DLSw FST peer configuration will contain the following line:

  ```
  dlsw remote-peer 0 fst <ip-address>
  ```

  It is possible to disable UDP processing in DLSw with the **dlsw udp-disable** command. However, disabling UDP only prevents the sending of UDP packets; it does not prevent the device from receiving and processing incoming UDP packets.

  Workaround: The workaround consists of filtering UDP packets to port 2067 and IP protocol 91 packets. Filters can be applied at network boundaries to filter all IP protocol 91 packets and UDP packets to port 2067, or filters can be applied on individual affected devices to permit such traffic only from trusted peer IP addresses. However, since both of the protocols are connectionless, it is possible for an attacker to spoof malformed packets from legitimate peer IP addresses.

  As soon as DLSw is configured, the Cisco IOS device begins listening on IP protocol 91. However, this protocol is used only if DLSw is configured for Fast Sequenced Transport (FST). A DLSw FST peer configuration will contain the following line:

  ```
  dlsw remote-peer 0 fst <ip-address>
  ```

  If FST is used, filtering IP protocol 91 will break the operation, so filters need to permit protocol 91 traffic from legitimate peer IP addresses.

  It is possible to disable UDP processing in DLSw with the **dlsw udp-disable** command. However, disabling UDP only prevents the sending of UDP packets; it does not prevent the receiving and processing of incoming UDP packets. To protect a vulnerable device from malicious packets via UDP port 2067, both of the following actions must be taken:

  1. Disable UDP outgoing packets with the **dlsw udp-disable** command
  2. Filter UDP 2067 in the vulnerable device using infrastructure ACL.

  * Using Control Plane Policing on Affected Devices

  Control Plane Policing (CoPP) can be used to block untrusted DLSw 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 may be configured on a device to protect the management and control planes to minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic sent to infrastructure devices in accordance with existing security policies and configurations. The following example, which uses 192.168.100.1 to represent a trusted host, can be adapted to your network. If FST is not used, protocol 91 may be completely filtered. Additionally, if UDP is disabled with the **dlsw udp-disable** command, UDP port 2067 may also be completely filtered.

```
!--- Deny DLSw traffic from trusted hosts to all IP addresses
!--- configured on all interfaces of the affected device so that
!--- it will be allowed by the CoPP feature.
access-list 111 deny udp host 192.168.100.1 any eq 2067 access-list 111 deny 91 host
192.168.100.1 any
!--- Permit all other DLSw traffic sent to all IP addresses
!--- configured on all interfaces of the affected device so that it
!--- will be policed and dropped by the CoPP feature.
access-list 111 permit udp any any eq 2067 access-list 111 permit 91 any any
!--- Permit (Police or Drop)/Deny (Allow) all other Layer 3 and Layer 4
!--- 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-DLSw-class match access-group 111
!--- Create a Policy-Map that will be applied to the
!--- Control-Plane of the device.
policy-map drop-DLSw-traffic class drop-DLSw-class drop
!--- Apply the Policy-Map to the Control-Plane of the
!--- device.
control-plane service-policy input drop-DLSw-traffic
```

In the above CoPP example, the access control 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. Please note that in the Cisco IOS 12.2S and 12.0S trains, the policy-map syntax is different:

```
policy-map drop-DLSw-traffic class drop-DLSw-class police 32000 1500 1500
conform-action drop exceed-action drop
```

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

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

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlimt.html

* Using Infrastructure ACLs at Network Boundary

Although it is often difficult to block traffic transiting your network, it is possible to identify traffic that should never be allowed to target your infrastructure devices and block that traffic at the border of your network. 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 shown below should be included as part of the deployed infrastructure access-list that will protect all devices with IP addresses in the infrastructure IP address range. If FST is not used, protocol 91 may be completely filtered. Additionally, if UDP is disabled with the **dlsw udp-disable** command, UDP port 2067 may also be completely filtered.

```
!--- Permit DLSw (UDP port 2067 and IP protocol 91) packets
!--- from trusted hosts destined to infrastructure addresses.
access-list 150 permit udp TRUSTED_HOSTS MASK INFRASTRUCTURE_ADDRESSES MASK eq 2067
access-list 150 permit 91 TRUSTED_HOSTS MASK INFRASTRUCTURE_ADDRESSES MASK
!--- Deny DLSw (UDP port 2067 and IP protocol 91) packets from
!--- all other sources destined to infrastructure addresses.
access-list 150 deny udp any INFRASTRUCTURE_ADDRESSES MASK eq 2067 access-list 150
deny 91 any INFRASTRUCTURE_ADDRESSES MASK
!--- 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
interface serial 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. This white paper can be obtained at the following link:

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

Further Problem Description: This vulnerability occurs on multiple events to be exploited. It is medium complexity in order to exploit and has never been seen in a customer environment.

- CSCta04391

  Symptoms: Router with dynamic NAT for unicast and multicast traffic crashes after deleting **ip nat inside source list**.

  Conditions: This symptom is observed when there is unicast and multicast traffic and only when unicast and multicast traffic use the same NAT rule.

  Workaround: Use a separate NAT rule for unicast and multicast traffic.

- CSCta16724

  Symptoms: Users with level 15 privilege and a “view” cannot perform Secure Copy (SCP).

  Conditions: This symptom is observed when a user with a “view” attempts to perform an SCP on a router running Cisco IOS Release 12.4(24)T.

  Workaround: Remove the “view”.

- CSCta36701

  Symptoms: A group member with VSA runs out of memory and starts dropping traffic after 12 hours.

  Conditions: This symptom is observed when the packet size of the traffic sent is near mtu so that the packets get fragmented before encryption. Crypto map on a multilink interface with VSA as the crypto engine will cause memory leak for every packet decrypted.

  Workaround: Disable VSA.

  Further Problem Description: This is specific to Crypto map on a multilink interface with VSA as the crypto engine. This is not specific to a GETVPN config.

- CSCta37063

  Symptoms: NAT fails to translate H323 payload information.

  Conditions: This symptom occurs when NetMeeting is dialing from outside NAT to inside NAT.

  Workaround: Initiate NetMeeting again. Note that once this NAT entry is cleared or has timed-out, the issue will reappear.

- CSCta67965

  Symptoms: A Cisco 7200 NPE-G1 may crash.

  Conditions: The symptom is observed when “ip pim sparse-mode” is added to the port-channel configuration and an OIR is performed on the FA-PA.

  Workaround: There is no workaround.

- CSCta79704

  Symptoms: A Cisco router crashes with a breakpoint exception.

  Conditions: This symptom is observed on a Cisco router configured with any of the following features:

  – IP Transfer Point (ITP)

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122mb/122mb2/itp20/index.htm

- PRI Backhaul Using the Stream Control Transmission Protocol and the ISDN Q.921 User Adaptation Layer

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ft_0546.htm

- Reliable Export with SCTP

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124t/124t4/nfhtsctp.htm

Workaround: There is no workaround.

- CSCtb54422

  Symptoms: An MFR bundle moves from SW to HW mode and flaps after reload.

  Conditions: This symptom is observed on a Cisco 7200 router when an MFR is configured on CJ-PA, then one member is added from MCTE1 and the following commands are entered: **wr mem** and **reload**.

  Workaround: Create a new MFR after reload and add members to it.

- CSCtb60330

  Symptoms: SVTI tunnel flaps at phase 1 expiry when a DPD ACK is not received. The line protocol on the tunnel interface goes down.

  Conditions: The symptom is observed with SVTI tunnels and when DPDs are enabled.

  Workaround: Disable DPDs.

  Alternate workaround: Use the **no crypto isakmp keepalive** command.

  Further Problem Description: This may affect those scenarios where routing protocols like BGP are run over the tunnel. To diagnose this, the following debugs should be enabled on both sides:

  ```
  debug crypto isakmp
  debug crypto ipsec
  debug crypto kmi
  ```

  The following entry can be seen in debugs:

  ```
  DPD sent to 10.1.1.1:500 & waiting: But IKE sa expired. Killing IPSec sas.
  ```

- CSCtb73450

  Symptoms: Start-Control-Connection-Request (SCCRQ) packets may cause tunnel to reset after digest failure.

  Conditions: This symptom is observed when the SCCRQ packets are sent with an incorrect hash.

  Workaround: There is no workaround.

- CSCtc13344

  Symptoms: Cisco Optimized Edge Routing (OER) experiences a fatal error and is disabled:

  ```
  %OER_MC-0-EMERG: Fatal OER error <> Traceback %OER_MC-5-NOTICE: System Disabled
  ```

  Conditions: This symptom is observed when configuring OER to learn the inside prefixes within a network by using the **inside bgp** command.

  Workaround: Disable prefix learning by using the **no inside bgp** command.

- CSCtc59535

  Symptoms: The DSL link stops passing traffic. The issue does not get resolved by shut and no shut of ATM interface or reloading the router.

Conditions: The symptom is observed when the CU has a Cisco 2821 router that is running Cisco IOS Release 12.4(15)T8 with HWIC-2SHDSL.

Workaround: Unplug and plug back the cable.

- CSCtc73759

  The H.323 implementation in Cisco IOS Software contains two vulnerabilities that may be exploited remotely to cause a denial of service (DoS) condition on a device that is running a vulnerable version of Cisco IOS Software.

  Cisco has released free software updates that address these vulnerabilities. There are no workarounds to mitigate these vulnerabilities other than disabling H.323 on the vulnerable device.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-201

  -h323.shtml.

  Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

  http://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

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

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

- CSCtd33567

  The H.323 implementation in Cisco IOS Software contains two vulnerabilities that may be exploited remotely to cause a denial of service (DoS) condition on a device that is running a vulnerable version of Cisco IOS Software.

  Cisco has released free software updates that address these vulnerabilities. There are no workarounds to mitigate these vulnerabilities other than disabling H.323 on the vulnerable device.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-h323.shtml.

  Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

  http://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

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

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

- CSCtd43168

  Symptoms: A breakpoint exception crash occurs while configuring SNMP traps via Cisco Works after the following errors are displayed:

  ```
  %SNMP-5-WARMSTART: SNMP agent on host <host name> is undergoing a warm start
  %SYS-2-CHUNKFREE: Attempted to free nonchunk memory, chunk ########, data ########.
  -Process= "NAT MIB Helper", ipl= 0, pid= 277 -Traceback=
  ```

Conditions: This symptom is observed after unconfiguring snmp-server, then configuring it again. Commands used for this configuration could include **snmp-server enable traps** or **snmp-server community**.

Workaround: There is no workaround.

- CSCtd47338

  Symptoms: The following error message is constantly displayed:

  ```
  crypto_engine_ps_vec(): no subblock attached
  ```

  Conditions: This issue is observed on a Cisco 7200 series router with VSA cards running Cisco IOS Release 12.4(15)T (other releases may be affected as well) and with DLSw configuration.

  Workaround: Configure the command **dlsw udp-disable**.

- CSCtd59184

  Symptoms: A Cisco router may reload due to a bus error.

  Conditions: This symptom is observed when the router is switching a packet via CEF through a crypto tunnel, and the tunnel adjacency has been deleted prematurely. It may be necessary for a crypto map to be associated with the physical interface in order to trigger this.

  Workaround: Avoid using a crypto map in the configuration.

  Alternate Workaround: Upgrade to Cisco IOS Release 12.4(20)T or later. Later releases handle management of adjacencies and interactions with the crypto subsystem differently, and do not exhibit this issue.

- CSCtd63792

  Symptoms: Calls may fail to a particular B channel in a PRI with cause code #47 (resources unavailable).

  Conditions: This symptom is observed on a Cisco gateway with H323 and PRI and Cisco IOS Release 12.4(15)T10.

  Workaround: Busy-out the affected B channel.

- CSCtd78209

  Symptoms: A Cisco router crashes when crypto is configured with ip-multicast fast switching.

  Conditions: This symptom is observed with Cisco IOS Release 12.4(15)T12.

  Workaround: There is no workaround.

- CSCtd86472

  The Cisco IOS Software Network Address Translation functionality contains three denial of service (DoS) vulnerabilities. The first vulnerability is in the translation of Session Initiation Protocol (SIP) packets, the second vulnerability in the translation of H.323 packets and the third vulnerability is in the translation of H.225.0 call signaling for H.323 packets.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-nat.shtml.

  Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

  http://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

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

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

- CSCtd87788

  Symptom: Traceback is seen when serial from second CJ-PA controller is added and removed from multilink. This interface remains up/down until a reload.

  Conditions: This symptom is seen when serial from second controller in unchannalized mode is added to multilink.

  Workaround: Reload the box to bring up the interface.

- CSCte14603

  A vulnerability in the Internet Group Management Protocol (IGMP) version 3 implementation of Cisco IOS Software and Cisco IOS XE Software allows a remote unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition. Cisco has released free software updates that address this vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-igmp.shtml.

  Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

  http://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

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

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

- CSCte19478

  Symptoms: Entering the **crypto isakmp xauth timeout** command does not seem to have any effect.

  Conditions: This symptom is observed when the command is needed for a specific scenario where user input at xauth requires more time than the default timeout value--for example, for rsa authentication (in new pin mode).

  Workaround: There is no workaround.

- CSCte49283

  Symptoms: Sometimes the LNS router sends an incorrect NAS-Port value.

  Conditions: The symptom is observed when the LNS router sends a stop accounting-request to the RADIUS server.

  Workaround: There is no workaround.

- CSCtf04954

  Symptoms: When the **cns config notify** command exists, some CLIs might misbehave or cause unexpected crashes during the configuration change.

  Conditions: The symptom is observed with the **cns config notify** command.

  Workaround: Remove all **cns config notify** CLIs from the configuration.

- CSCtf17624

  The Cisco IOS Software Network Address Translation functionality contains three denial of service (DoS) vulnerabilities. The first vulnerability is in the translation of Session Initiation Protocol (SIP) packets, the second vulnerability in the translation of H.323 packets and the third vulnerability is in the translation of H.225.0 call signaling for H.323 packets.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-nat.shtml.

  Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

  http://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

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

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

- CSCtf19461

  Symptoms: IP address is not leased out to the client from server.

  Conditions: The symptom is observed when configuring the VPN sub-option at the interface level on the relay.

  Workaround: There is no workaround.

- CSCtf36117

  Symptoms: Crash occurs when executing the **show crypto session brief** command with multiple IKEv2 tunnel connections.

  Conditions: The symptom is observed when setting up as many as 500 IKEv2 tunnels employing symmetric RSA-Sig based authentication with CRL check enabled. This crash occurs when there are about 450 tunnels established and the command is trying to list down the sessions.

  Workaround: There is no workaround.

- CSCtf47929

  Symptoms: Tracebacks are seen on a Cisco router when creating a udp-jitter operation with request-data size of more than 17000 bytes (super jumbo packet).

  Conditions: This symptom is observed with a large request-data size.

  Workaround: Use a request-data size value less than 17000.

- CSCtf70959

  Symptoms: EzVPN client is trying to negotiate the connection with a NULL address when the outside interface is a profile-based dialer interface.

  Conditions: This situation is a corner condition. The IP address on the dialer interface will be installed as soon as the dialer negotiation completes and the dialer interface comes up. But in this case, even though the IP address is not installed the dialer interface, the API is returning TRUE and proceeds further with the EzVPN connection.

  Workaround: Use a non profile-based dialer interface.

- CSCtf72678

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device when SIP operation is enabled.

  Cisco has released free software updates that address these vulnerabilities. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-sip.shtml.

  Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

  http://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

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

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

  Cisco Unified Communications Manager (CUCM) is affected by the vulnerabilities described in this advisory. Two separate Cisco Security Advisories have been published to disclose the vulnerabilities that affect the Cisco Unified Communications Manager at the following locations:

  http://www.cisco.com/warp/public/707/cisco-sa-20090826-cucm.shtml

  http://www.cisco.com/en/US/products/products_security_advisory09186a0080b4a313.shtml

- CSCtf78252

  Symptoms: Packets of more than 1500 bytes are dropped 50% of the time when decrypted by VSA.

  Conditions: This symptom is observed with Crypto with Cisco IOS Release 12.4 (15)T with flow switching enabled on the interface, crypto applied, and DF bit set.

  Workaround: Upgrade to Cisco IOS Release 12.4(22)T4 or higher.

  Alternate Workarounds:

  - Tune MTU of LAN-facing interfaces to 1600 bytes
  - Turn off flow switching as follows:

```
interface GigabitEthernet0/2 mtu 1600 ip address x.x.x.x ip route-cache flow duplex
auto speed auto media-type rj45 negotiation auto crypto map vpn end
```

  - Remove the ip route-cache flow from the interface configuration.

- CSCtf84237

  Symptoms: A router may reload with the following crash decode (traceback summary):

```
0x123d7e24 is in vpdn_apply_vpdn_template_pptp 0x1239c100 is in l2x_vpdn_template_find
0x123d81dc is in vpdn_apply_l2x_group_config 0x123cfedc is in
vpdn_mgr_call_initiate_connection 0x123cce68 is in vpdn_mgr_event 0x123ce974 is in
vpdn_mgr_process_client_connect 0x123cf248 is in vpdn_mgr_process_message 0x123cf368
is in vpdn_call_manager
```

  Conditions: The symptom is observed when an invalid tunnel-type VSA is configured, for example:

```
vsa cisco generic 1 string "vpdn:tunnel-type=l2tp_bad"
```

  Workaround: Configure a correct tunnel-type VSA in Radius.

- CSCtf87039

  Symptoms: Device crashes at crypto_ikmp_process_xauth_reply.

  Conditions: The symptom could occur while processing the xauth response received from the client. The PPC platform crashes (the MIPS64 platform does not crash).

  Workaround: There is no workaround.

- CSCtf87559

  Symptoms: HWIC-4ESW drops some of the multicast packets while transmitting due to output errors.

  Conditions: This symptom is observed when multicast packets are received on an onboard FE port and transmitted via the HWIC-4ESW to the LAN using a VLAN interface. As the multicast traffic rate increases, the drop rate of the HWIC- 4ESW increases. Show controller for the HWIC-4ESW port shows “MAC IDB Tx Errors: output_drops” incrementing. The issue is not seen with unicast traffic.

  Workaround: There is no workaround.

- CSCtf91428

  The Cisco IOS Software Network Address Translation functionality contains three denial of service (DoS) vulnerabilities. The first vulnerability is in the translation of Session Initiation Protocol (SIP) packets, the second vulnerability in the translation of H.323 packets and the third vulnerability is in the translation of H.225.0 call signaling for H.323 packets.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-nat.shtml.

  Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

  http://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

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

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

- CSCtg06045

  Symptoms: A Cisco router may reload with traceback from a crypto ACL configuration.

  Conditions: This symptom is observed on a Cisco router running Cisco IOS Release 12.4(15)T12 and experiencing a high CPU stress load while the ACEs are being changed periodically. This symptom is specific to the ACE entries in crypto ACL downloaded from KS.

  Workaround: Simplify and consolidate the ACE entries in the crypto ACL. In addition, reducing the CPU stress level may help.

- CSCtg21685

  Cisco IOS Software contains a vulnerability when the Cisco IOS SSL VPN feature is configured with an HTTP redirect. Exploitation could allow a remote, unauthenticated user to cause a memory leak on the affected devices, that could result in a memory exhaustion condition that may cause device reloads, the inability to service new TCP connections, and other denial of service (DoS) conditions.

Cisco has released free software updates that address this vulnerability. There is a workaround to mitigate this vulnerability.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-sslvpn.shtml.

Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

http://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

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

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

- CSCtg23115

  Symptoms: A memory leak occurs in the Pool Manager process.

  Conditions: This symptom is observed with Cisco IOS Release 12.4(24)T. It is not yet known what other IOS releases may be affected. This symptom is seen with multicast enabled.

  Workaround: There is no workaround to prevent the leak. Once the memory has leaked, reloading the router will temporarily free the memory.

- CSCtg27206

  Symptoms: Static route not seen in the receiver end after a link flap.

  Conditions: The symptom is observed if the leachability of the same subnet to static routes nexthop is being learnt from another interface during link down and, before link flap, RIP protocol is removed and reconfigured.

  Workaround: Do a **clear ip route <ip-address>** on the sender side.

- CSCtg41733

  Symptoms: Certain crafted packets may cause memory leak on a Cisco IOS router.

  Conditions: This symptom is observed on a Cisco IOS router configured for SIP processing.

  Workaround: Disable SIP if it is not needed.

- CSCtg42179

  Symptoms: High CPU utilization occurs under interrupt. CPU profiling indicates that this is due to QoS.

  Conditions: This symptom is observed on Cisco ISR 3800 routers with Cisco IOS Release 12.4(15)T10. It is not yet known what other platforms and/or versions are affected.

  Workaround: There is no workaround. A lower traffic rate may lower the CPU utilization.

- CSCtg71332

  Symptoms: On a Cisco 3800 ISR that is using NM-1T3/E3 module, the controller will be down/down should following condition be true.

  Conditions: This symptom has been noticed on the router that is running Cisco IOS Release 12.4(15)T8 with advanced IP services or IP services feature set.

  Workaround:

  1. Use SP services feature set.

2. Upgrade router to Cisco IOS Release 12.4(24)T.
3. Install one or more PVDM sLOTS.

- CSCtg73604

  Symptom: E1R2-compelled signaling calls fail.

  Conditions: This symptom is observed when a call is made using E1R2-compelled signaling.

  Workaround: There is no workaround.

- CSCtg88766

  Symptoms: HWIC-SHDSL does not train up in 4-wire standard mode.

  Conditions: The symptom is observed when CPE is in 4-wire standard mode and the DSLAM linecard is GSPN-based and configured in 4-wire standard mode.

  Workaround: There is no workaround.

- CSCth01939

  Symptoms: IPsec packets are dropped on the router and an error is displayed on the console.

  Conditions: This symptom is observed on a Cisco IAD2430 with VPN/GRE tunnel configuration and AES256 encryption.

  Workaround: There is no workaround.

- CSCth89668

  Symptoms: NAS port ID is 0 while testing idbless VLAN for PPPoE.

  Conditions: This symptom is observed on a Cisco 7200 router running Cisco IOS Release 12.4(15)T14.

  Workaround: There is no workaround.

- CSCti15990

  Symptoms: EzVPN will not come up if the dialer interface flaps.

  Conditions: This symptom is observed when the dialer interface is profile-based.

  Workaround: Change the dialer interface to non-profile-based.

Resolved Caveats—Cisco IOS Release 12.4(15)T13

Cisco IOS Release 12.4(15)T13 is a rebuild release for Cisco IOS Release 12.4(15)T. The caveats in this section are resolved in Cisco IOS Release 12.4(15)T13 but may be open in previous Cisco IOS releases.

- CSCsg39977

  Symptom: When dialer interfaces are used in conjunction with Multilink PPP (MLP), a router may crash because of a corrupted program counter.

  Conditions: This symptom is observed on a Cisco router when a dialer interface, including interfaces such as ISDN BRI and PRI interfaces, is configured to use MLP and when the queueing mode on the dialer interface is configured for Weighted Fair Queuing (WFQ). Note that WFQ is the default for some types of dialer interfaces.

  Workaround: There is no workaround.

- CSCsj64222

  Symptoms: A Cisco router configured with Dynamic Multipoint VPN (DMVPN) may crash when the tunnel interface is shut down and then later **no shut**, or if the tunnel protection configuration is changed.

  Conditions: This occurs with a DMVPN configuration where a spoke router has more than one tunnel interface that shares the same tunnel source interface.

  Workaround: There is no workaround.

- CSCsu22952

  Symptoms: Cisco 7600 RP crashes when the traffic crosses ATM dLFI interfaces.

  Conditions: This could happen when all the following met:

  1. MLP over ATM is configured.
  2. QoS queuing policy applied on the MLP bundle.
  3. The MLP link goes down.

  Workaround: There is no workaround.

- CSCsu73970

  Symptoms: Applying a service policy to an outbound interface causes CPUHOG messages of the following nature, and then it triggers a software-forced crash:

  ```
  %SYS-3-CPUHOG: Task is running for (128004)msecs, more than (2000)msecs (25/1),process
  = IP Input.
  %SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = IP Input.
  %Software-forced reload
  Preparing to dump core... *Sep 23 22:44:39.275 AWST: %SYS-3-CPUYLD: Task ran for
  (128072)msecs, more than (2000)msecs (25/1),process = IP Input
  22:44:42 AWST Tue Sep 23 2008: Breakpoint exception, CPU signal 23, PC = 0x4004FE88
  ```

  Conditions: This symptom is observed when a service policy is applied to an outbound interface. The service policy should have similar ICMP permit statements:

  ```
  permit icmp any 172.16.156.16 0.0.0.15 echo-reply
  permit icmp any 172.16.156.16 0.0.0.15 echo
  ```

  The hang occurs when both of these statements are configured at the same time.

  Workaround: There is no workaround.

- CSCsx23602

  Symptoms: Catalyst 6000 running modular Cisco IOS 12.2(33)SXH4 may crash with NAT configuration.

  Conditions: Occurs when running modular IOS with NAT deployment. Crash only happening in production, and NAT translation is required for crash to occur.

  Workaround: Run non-modular Cisco IOS Release 12.2(33)SXH4.

- CSCsx26025

  Symptoms: Wireless clients are not able to ping each other after a few minutes.

  Conditions: Can occur on any of the following routers with 802.11 wireless interfaces:

  ```
  UC500, 85x, 87x, 1811, HWIC-AP
  ```

  Workaround: There is none.

- CSCsy20998

  Symptoms: A buffer leak is observed when a high volume of SSLVPN traffic flows through the router.

Conditions: This symptom occurs under stress conditions and also when SSL negotiation fails during handshake.

Workaround: There is no workaround.

- CSCsy61321

  Symptoms: Accounting requests sent to the TAC server do not fail over to the second server.

  Conditions: This symptom is observed when two TACACS servers are configured, the first without TACACS, the second with TACACS, and authentication is configured as “none”.

  Workaround: Use a single working server, or ensure that the first group uses a valid server.

- CSCsz05783

  Symptoms: Voice/SIP (ef) packets are not marking in the ingress/egress when NAT is enabled on the interface.

  Conditions: Occurs when NAT is enabled.

  Workaround: Remove NAT from the configuration.

- CSCsz70049

  Symptoms: A VIC2-2BRI port may go down suddenly by not detecting the RR command/response from the telco side, and it stays in a down state. As a result, this BRI port does not send/receive a voice call.

  Conditions: The symptom is observed on a Cisco 3825 router with VIC2-2BRI.

  Workaround: Issue the **clear interface bri** command to restore this state.

- CSCta20590

  Symptoms: A group member (GM) pseudotime may desynchronize after re- registering or at initial registration.

  Conditions: This symptom is observed when GETVPN with time-based anti-replay (TBAR) is enabled.

  Workaround: Disable TBAR or use a very large window (> 30 seconds).

  Further Problem Description: After establishing phase I, the GM is supposed to obtain the KEK and TEKs. If a packet drop occurs (usually, this message is fragmented across multiple frames], then the router is not able to reassemble the packet. IKE will later resend this message, but if the pseudotime has not been recalculated the symptom will reoccur.

- CSCta62678

  Symptoms: A router hangs when an access-control service policy is reconfigured.

  Conditions: This symptom is observed on a Cisco 7200 router.

  Workaround: There is no workaround.

- CSCta86675

  Symptoms: A Cisco router may crash reporting a bus error.

  Conditions: This symptom occurs when stress traffic passes through a Cisco router that is configured with QOS policies, cryptomap, and access-lists.

  Workaround: There is no workaround.

- CSCtb39756

  Symptoms: New GM is not able to communicate to existing GMs.

Conditions: The symptom is observed under the following conditions:

1. Primary keyserver reloads.
2. Secondary keyserver takes over role as primary and removes the old TEK and creates a new TEK2.
3. During the period where the existing GMs have both old and new TEK keys, any new GM that registers will only get the new TEK. This new GM will not be able to communicate to the existing GMs until the old TEK expires.

Workaround: There is no workaround.

- CSCtb98080

  Symptoms: When you attempt to browse to a WebVPN portal you only see a blank page. The router does not send the browser a certificate and the portal login page is not displayed. The command **debug webvpn sdps** logs the following error message:

  ```
  WV-SDPS: Sev 4:sslvpn_tcp_read_notify(),line 1569:No to notify read: already queued[1]
  004549:
  ```

  Conditions: The symptom is observed when the SSLVPN process is waiting for an HTTP REQUEST from a client on the port configured using the **http-redirect** *port no* command but the process does not wake up. This can happen because of an unexpected IPC message to the SSLVPN process by another IOS process.

  Workaround: Remove **http-redirect** from the WebVPN gateway and reload the device.

- CSCtc40477

  Symptoms: A Cisco router may crash after disabling then re-enabling NBAR on an interface.

  Conditions: This symptom is observed when policy-map classification based on NBAR and NAT is configured on the router.

  Workaround: Create a dummy subinterface and enable NBAR using the **ip nbar protocol-discovery** command.

  Alternate workaround: While migrating on the subinterface, disable NBAR using the **no ip nbar protocol-discovery** command on the old interface only after enabling NBAR on the newly-migrated interface.

- CSCtc51539

  Symptoms: A Cisco router crashes with a “Watch Dog Timeout NMI” error message.

  Conditions: This symptom is observed only on devices configured with Bidirectional Forwarding Detection (BFD). For further information on BFD, consult the following link:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fs_bfd.html

  Workaround: Disable BFD.

- CSCtc90459

  Symptoms: Inbound ACL is not working properly. It does not allow packets to pass that should.

  Conditions: The symptom is observed when you configure “input access list” to allow voice packets (SIP protocol). If you apply the following configuration on the router the voice packets will get dropped:

  ```
  access-list 101 permit udp host 85.38.230.34 eq 5060 host 85.34.23.74
  access-list 101 permit udp host 85.38.230.34 host 85.34.23.74 range 16384 32767
  ```

  Workaround: Use “log” keyword at the end of the ACL.

- CSCtd21666

  Symptoms: Prefixes are not advertised from an MPLS VPN PE router to a group of CEs (all belonging to an update-group).

  Conditions: The issue toggles between two update-groups. The only difference between the two update-groups is that one of the update-groups has the “4 octets ASN capable” set.

  Workaround: Clearing the leader of the update-group that is not advertising any routes works most of the time.

- CSCtd75033

  Symptoms: Cisco IOS Software is affected by NTP mode 7 denial-of-service vulnerability.

  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 Reference Guide" at the following link:

http://www.cisco.com/warp/public/620/1.html

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

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

* NTP Access Group

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

```
!--- Configure trusted peers for allowed access

access-list 1 permit 171.70.173.55

!--- Apply ACE to the NTP configuration

ntp access-group peer 1
```

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

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

* Infrastructure Access Control Lists

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

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

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

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

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

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

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

!--- Note: If the router is acting as a NTP multicast client
!---   via the interface command "ntp multicast client"
!---   then multicast IP packets to the mutlicast group must
!---   be filtered as well.  The following example covers
!---   a NTP multicast group of 239.0.0.1 (Default is
!---   224.0.1.1)

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

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

access-list 150 deny udp any
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 123

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

access-list 150 permit ip any any

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

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

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

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

* Control Plane Policing

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

- Filtering untrusted sources to the device.

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

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

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

access-list 150 deny udp TRUSTED_SOURCE_ADDRESSES WILDCARD
     any eq 123

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

access-list 150 permit udp any any eq 123

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

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

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

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

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

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

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

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

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

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

access-list 150 permit udp any any eq 123

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

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

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

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

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

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

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

http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html and
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlimt.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.

- CSCte03142

  Symptoms: Enhancement allows user to configure MAC address for ATM p2p subinterface.

  Conditions: This enhancement is to be used for RBE case to use the configured MAC on ATM p2p subinterface.

  Workaround: There is no workaround.

- CSCte03209

  Symptoms: On a Cisco 7206/NPE-G2 configured for IRB and L2TP, ingress ARP requests and replies may fail with this message according to “debug arp”:

  ```
  IP ARP: sent req src 10.10.10.2 0000.0c4d.4a20,dst 10.10.10.1 0000.0000.0000 BVI1
  IP ARP rep filtered src 10.10.10.1 000c.85ae.2e00, dst 10.10.10.2 0000.0c4d.4a20 wrong
  cable, interface Virtual-Access5.
  ```

Conditions:

```
bridge irb
 bridge 1 protocol ieee
 bridge 1 route ip

 interface BVI1
  ip address 10.10.10.2 255.255.255.0
  ip directed-broadcast

 interface Virtual-Template1
  no ip address
  no peer default ip address
  ppp authentication pap chap
  bridge-group 1
  bridge-group 1 spanning-disabled
 end

 interface Virtual-Access5
  no ip address
  no peer default ip address
  ppp authentication pap chap
  bridge-group 1
  bridge-group 1 spanning-disabled
```

This symptom is observed on Cisco IOS Release 12.4(15)T7, Release 12.4(15) T9, and Release 12.4(24)T2.

Workaround: There is no workaround.

- CSCte12104

  Symptoms: Crash at startup with the following error message:

  ```
  %SYS-6-STACKLOW: Stack for process ATM Periodic running low, 0/9000
  ```

  Conditions: The symptom is observed when QoS policy is applied on an ATM interface. There is no specific trigger.

  Workaround: There is no workaround.

  Further Problem Description: This issue may not be widely hit as it is difficult to reproduce.

- CSCte15982

  Symptoms: When a Cisco 877 DSL router that is running Cisco IOS Release 12.4(24)T2 is connected to a third-party DSLAM that is running in 4-wire mode, entering the **clear pppoe all** command may result in a PADS received on one PVC being incorrectly processed on a subinterface associated with a different PVC, which results in two PPPoE sessions transmitting data packets on the same PVC.

  Conditions: This symptom is observed under the following working scenario:

  ```
  CPE# show pppoe session 2 client sessions

  Uniq ID PPPoE RemMAC Port Source VA State SID LocMAC VA-st N/A 7 xxxx.xxxx.xxxx
  ATM0.38 Di0 Vi1 UP
  xxxx.xxxx.xxxx VC: 0/38 UP N/A 8 xxxx.xxxx.xxxx ATM0.40 Di1 Vi2 UP
  xxxx.xxxx.xxxx VC: 0/40 UP
  ```

  After the **clear pppoe all** command is entered:

  ```
  CPE# clear pppoe all
  CPE# show pppoe session 2 client sessions

  Uniq ID PPPoE RemMAC Port Source VA State SID LocMAC VA-st N/A 9 xxxx.xxxx.xxxx
  ATM0.40 Di0 Vi1 UP
  ```

```
xxxx.xxxx.xxxx VC: 0/40 UP N/A 10 xxxx.xxxx.xxxx ATM0.40 Di1 Vi2 UP
xxxx.xxxx.xxxx VC: 0/40 UP
controller DSL 0 mode atm line-mode 4-wire enhanced dsl-mode shdsl symmetric annex B
interface ATM0.38 point-to-point pvc data 0/38 pppoe-client dial-pool-number 1
interface ATM0.40 point-to-point pvc voip 0/40 pppoe-client dial-pool-number 2
interface Dialer0 ip address negotiated encapsulation ppp dialer pool 1 keepalive 60
ppp pap sent-username data@data.com password 0 data
interface Dialer1 ip address negotiated encapsulation ppp dialer pool 2 keepalive 60
ppp pap sent-username voip@voip.com password 0 voip
```

1. This symptom is not reproducible when running in 2-wire G.SHDSL mode. It is reproducible only when running the **line-mode 4-wire enhanced** command.
2. The symptom is reproducible running the following Cisco IOS Releases:
   - 12.4(15)T7
   - 12.4(15)T10
   - 12.4(20)T
   - 12.4(22)T
   - 12.4(22)T1
   - 12.4(24)T
   - 12.4(24)T1
   - 12.4(24)T2
   - 15.0(1)M
3. The symptom can be triggered three ways:

   3A. “reload”

   3B. If “reload” results in correct behavior, “clear pppoe all”.

   3C. If “reload” results in correct behavior, any subsequent event that results in both PPPoE sessions being torn down simultaneously.
4. The symptom is not reproducible if any packet-layer debugs are enabled, such as “debug pppoe packet” or “debug atm packet”.

Workaround:

1. Reload the router.
2. After every reload, if the problem is not occurring, configure “debug pppoe packet” on the Cisco 878 router.
3. After every reload, if the problem is occurring, reload the router until it is not occurring, and then follow Workaround 1.

- CSCte23299

  Symptoms: A Cisco 877W router is not responding to IPv6 neighbor solicitation.

  Conditions: This symptom is observed under normal conditions.

  Workaround: There is no workaround.

- CSCte34718

  Symptoms: Network Time Protocol (NTP) may lose synchronization.

  Conditions: This symptom is observed on a Cisco 871 router with board Rev. C0.

  Workaround: Revert to Cisco IOS Release 12.4(15)T3.

- CSCte39250

  Symptoms: Router crashes at ipv6_show_interface while executing the **show ipv6 interface brief** command after a link-local has been explicitly configured, and an invalid deletion command has been executed to remove it. In all other scenarios the **show ipv6 interface brief** command has no issues.

  Conditions: This symptom only happens on a Cisco 7200 router that is running Cisco IOS Release 12.4(15)T12. The steps to follow are:

  – onfigure explicitly a link-local address on an interface:

    ipv6 address FE80::A8BB:CCFF:FE03:2001 link-local

  – Try to remove a non-existent and invalid address which has the same prefix as the previously configured link-local address:

    no ipv6 address FE80::A8BB:CCFF:FE03:2001/64

  – Try to display the addresses on that interface:

    do **show ipv6 interface** command

  Workaround: Use the appropriate delete command to delete the link-local address. For example, see the following:

  no ipv6 address FE80::A8BB:CCFF:FE03:2001 link-local

- CSCte64544

  Symptoms: Calls fail following hook flash on a T1-CAS circuit.

  Conditions: The symptom is observed following outbound calls over a T1-CAS E&M, and after a hookflash.

  Workaround 1: Reorder circuits in CUCM RG.

  Workaround 2: Perform a shut/no shut on the T1-CAS controller.

- CSCte81027

  Symptoms: Incoming packets are dropped because route lookup fails after packets have been passing through for a while. Ping to default gateway fails, but extended ping works fine with “record” option.

  Conditions: This symptom occurs when the incoming interface has crypto and VRF configured, and CEF is turned on. There is at least one packet sent with TTL 1 or the IP options set. This problem is seen in Cisco IOS Release 12.4 (15)T8 and later releases.

  Workaround: Any one of the following steps will fix the issue:

  1. Reload the router.
  2. Remove the **crypto map** command under the interface and add it back.
  3. Bounce the interface.
  4. Turn CEF off and turn it back on.

- CSCte81855

  Symptoms: The following symptoms occur when a Cisco Voice XML (VXML) gateway reaches 2048 open sockets:

  – Dead air on call and call drops

  – If customer has survivability TCL enabled in ingress gateway, the call will go to survivability

  - Agents can be reserved but voice calls do not reach the agent. Calls to the agent are placed after the original call failed and the call is handled by survivability TCL.
  - Errors displayed in the VXML gateway are related to Network Out of Order cause code 38 and ip transfer to 0.0.0.0 ip address failed

  Conditions: This symptom is observed in any Cisco gateway, specifically Cisco 2800, Cisco 3800, and Cisco AS53. The symptom occurs in Cisco IOS Release 12.4 (15)T6, Release 12.4(15)T7, Release 12.4(15)T8, Release 12.4(15)T9, Release 12.4 (15)T10, Release 12.4(15)T11, and Release 12.4(15)T12.

  Workaround:

  - Make sure the media server and VXML server are reachable
  - Make sure all media files requested exist in the media server and that the path to the media file is correct
  - Make sure media server backup is configured in the VXML gateway (for example, ip host mediaserver-backup)
  - Check the http client process with: show proc cpu | include http client show socket X --> Where X is the id of the http client process showing with the previous command.

  If the TCP sockets are getting closed to 2048, shutdown the voice service VoIP and wait for all the IP calls to finish to reboot the gateway. If this is also an ingress gateway, you will have to re-route the calls to another ingress gateway.

- CSCtf05490

  Symptoms: There is dead air on call between ingress and VXML gateway.

  Conditions: The symptom is observed when a CVP is used between the gateway and the VXML gateway. The CVP sends a late TCS to VXML gateway. The TCS is sent after the received VXML TCS and a TCS-ACK is replied. The VXML gateway is unable to handle the late TCS and disconnects the call with disconnect cause code 65. When the call is dropped from VXML gateway, CVP will retry to send the call to a post-survey DNIS, but it will not forward code 65 to ingress gateway at any time.

  Workaround: Configure “call start slow”.

Resolved Caveats—Cisco IOS Release 12.4(15)T12

Cisco IOS Release 12.4(15)T12 is a rebuild release for Cisco IOS Release 12.4(15)T. The caveats in this section are resolved in Cisco IOS Release 12.4(15)T12 but may be open in previous Cisco IOS releases.

- CSCsc62963

  Symptoms: The interface MTU is not user configurable. When you attempt to configure “interface level command mtu”, the following message is printed:

  ```
  % Interface {Interface Name} does not support user settable mtu.
  ```

  Conditions: The symptom is observed with a 2-Port FE on a Cisco 7200 series router.

  Workaround: There is no workaround.

  Further Problem Description: The Cisco.com document entitled “MPLS MTU Command Changes” further discusses this enhancement.

- CSCsg38088

  Symptoms: A Cisco router may crash.

Conditions: This symptom is observed under the following conditions:

1. AAA authentication must be enabled.
2. Use the **cns aaa authentication** *authentication method* command to enable CNS authentication
3. Repeat step 2 multiple times with different invalid authentication method arguments.

Workaround: To change the method associated with CNS authentication, enter the **no cns aaa authentication** command, then reconfigure CNS authentication with a valid authentication method argument.

- CSCsk53318

  Symptoms: An ATM interface may lose its IP address after a graceful stop and start of the interface.

  Conditions: This symptom is observed after online insertion and removal (OIR) of the ATM port adapter.

  Workaround: Reconfigure the IP address, then enter the **no shutdown** command followed by the **shutdown** command on the main ATM interface.

- CSCsq99299

  Symptoms: Router crashes during traceback generation with a bus error.

  Conditions: When CPUHOG occurs, traceback is generated. In some cases, it may lead to crash due to uninitialized internal data.

  Workaround: There is no workaround.

- CSCsu05306

  Symptoms: A Cisco device might report a crash because of a software-forced crash and/or bus error. The root cause for the crash: Refcount becomes -1 as the chunk was already freed.

  Conditions: This symptom is observed on a Cisco device only when an application firewall for HTTP inspection is turned on.

  Workaround: There is no workaround.

- CSCsv40924

  Symptoms: A Cisco router that is running NAT may corrupt the IP header checksum for some RTSP packets.

  Conditions: This symptom is observed when the RTSP connection goes through NAT, “OPTION” or “DESCRIBE” messages are sent, and the NAT translation used has a differing number of characters for the private and public IP addresses of the server.

  Workarounds:

  1) Configure the **no-payload** command for the NAT translation. This will stop the corruption, but will also cause all deep packet NATing to stop, which can cause other issues.

  2) Use a port other than 554 for the RTSP steam. This will stop the corruption, but will also stop the router from NATing the embedded IP addresses in the RTSP packets. Depending on the specific implementation of RTSP, this may or may not stop the stream from working.

  3) Change your NAT translation such that the private and public IP addresses have the same number of characters. For instance 192.168.0.1 has 11 characters, and 172.16.100.200 has 14 characters.

- CSCsv81176

  Symptoms: Router crashes with syslog CHUNKBADMAGIC.

Conditions: The symptom is observed with an ATM interface and NAT outside interface on a Cisco 3845 platform. It has been seen with a large number of flows from thousands of source addresses and with thousands of translated source addresses in a short period of time.

Workaround: Limit the number of source addresses available for NAT translation to less than 2000 or increase traffic slowly.

- CSCsw39413

  Symptoms: The following sequence of steps used to reset all the C5510 DSPs on a Cisco C1861 voice gateway will leave DSP 1 in an unusable state, and all analog voice ports tied to this DSP for signaling channels will be forced into a shutdown state.

  1. Invoke “test voiceport driver” for slot 0.
  2. Choose the “2 - 5510 DSP test” option.
  3. Select “1 - Reset ALL DSPs”.

  Conditions: This behavior is observed on Cisco C1861 voice gateways installed with any Cisco IOS release that supports these products, namely 12.4T and 12.4T-based Cisco IOS releases that support voice features.

  Workarounds: The following alternate methods to reset all the C5510 DSPs have been observed to correctly bounce and recover both of the DSPs and all analog voice ports tied to DSP 1.

  Alternative 1:

  a. Invoke “test voiceport driver” for slot 0.
  b. Choose the “2 - 5510 DSP test” option.
  c. Select “2 - Reset 1 DSP” twice, and each time specify DSP ID 1 or 2.

  Alternative 2:

  a. Invoke “test voiceport driver” for slot 0.
  b. Choose the “2 - 5510 DSP test” option.
  c. Select “14 - faked dsp crash” twice, and each time specify DSP ID 1 or 2.

  Alternative 3: At the EXEC prompt, issue the “test dsp device all all reset” command.

- CSCsx10028

  Symptoms: A core dump may fail to write or write very slowly (less than 10KB per second).

  Conditions: The symptom is observed when the cause of the crash is processor memory corruption. When this occurs, the corrupted memory pool cannot be used to write the core dump so it will likely fail. (IO memory corruption crashes should not have this problem.)

  Workaround: There is no workaround.

- CSCsx33622

  Symptoms: Flapping BGP sessions are seen in the network when a Cisco IOS application sends full-length segments along with TCP options.

  Conditions: This issue is seen only in topologies where a Cisco IOS device is communicating with a non-Cisco-IOS peer or with a Cisco IOS device on which this defect has been fixed. The router with the fixed Cisco IOS software must advertise a lower maximum segment size (MSS) than the non-fixed Cisco IOS device. ICMP unreachables toward the non-fixed Cisco IOS router must be turned off, and TCP options (for example, MD5 authentication) and the **ip tcp path-mtu-discovery** command must be turned on.

  Workaround: Any value lower than the advertised MSS from the peer should always work.

Setting the MSS to a slightly lower value (-20 to -40) is sufficient to avoid the issue. This number actually accounts for the length of TCP options present in each segment. The maximum length of TCP option bytes is 40.

If the customer is using MD5, Timestamp, and SACK, the current MSS should be decreased by 40 bytes. However, if the customer is using only MD5, the current MSS should be decreased by 20 bytes. This should be enough to avoid the problem. For example:

1. If the current MSS of the session is 1460, New MSS = 1460 - 40 = 1420 (accounts for maximum TCP option bytes; recommended).
2. If the current MSS of the session is 1460, New MSS = 1460 - 20 = 1440 (accounts for only the MD5 option).

- CSCsy29533

  Symptoms: A T.38 fax relay call may fail.

  Conditions: The symptom is observed with an MGCP-controlled T.38 fax relay call when the gateway is configured for CA control T.38. The output of the **debug voip vtsp all** command shows fax relay as "DISABLED."

  Workaround: Use Cisco IOS Release 12.4(15)T7 or Release 12.4(22)T.

- CSCsy86078

  Symptoms: Router crashes with memory corruption.

  Conditions: This symptom is observed when BFD is configured

  Workaround: There is no workaround.

- CSCsy95844

  Symptoms: Multicast traffic destined for a dialer interface configured with PPPoA is not forwarded, although the counters in the output of the **sh ip mroute count** command and all multicast state information seems correct.

  Conditions: This symptom is observed

  – on a Cisco 1800 series integrated services router (ISR) configured with PPPoA over DSL link while running Cisco IOS Release 12.4(24)T
  – when the multicast traffic originates on the LAN and is transmitted over the dialer interface toward the receivers/PIM RP. Initial packets may be correctly sent while the multicast group is in registering state, but once the source is registered with the RP, sending the multicast traffic fails
  – when CEF is globally enabled on all interfaces.

  Workaround: Disable CEF on the dialer interface using the **no ip mroute-cache** command.

- CSCsz39167

  Symptoms: If a tunnel is configured over the 880-3G cellular interface, traffic forwarding stops when the packet size is greater than the tunnel MTU.

  Conditions: The symptom is observed when a tunnel is configured over a cellular interface and running Cisco IOS Release 12.4(24)T.

  Workaround: Disable "ip cef".

- CSCsz48614

  Devices running Cisco IOS Software and configured for Cisco Unified Communications Manager Express (CME) or Cisco Unified Survivable Remote Site Telephony (SRST) operation are affected by two denial of service vulnerabilities that may result in a device reload if successfully exploited. The vulnerabilities are triggered when the Cisco IOS device processes specific, malformed Skinny Call Control Protocol (SCCP) messages.

  Cisco has released free software updates that address these vulnerabilities.

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

- CSCsz68709

  Symptoms: A console may lock when using the **scripting tcl init** *init-url* command.

  Conditions: This symptom is observed when using the **scripting tcl init** *init-url* command where the *init-url* is invalid or inaccessible, then entering the **tclsh** command and appending a file name.

  Workaround: Ensure that the *init-url* argument used in the **scripting tcl init** command is valid and accessible.

  Alternate workaround: Enter the **tclquit** command to end the Tcl shell and return to privileged EXEC mode, then enter the **tclsh** command to enable the Tcl shell again.

- CSCsz72138

  Symptoms: A POS interface on a PA-POS-2OC3 may experience a stuck issue. All packets will be dropped after hitting the stuck scenario:

  ```
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops:
  72048413<<<<<<<<<<<<<<<<<<<<all packets are getting dropped Queueing strategy:
  Class-based queueing Output queue: 197/1000/0 (size/max total/drops)<<<<<<<<<<output
  queue remains stuck at 197
  ```

  Conditions: This issue is common to different platforms such as the Cisco 7300, Cisco 7304, and Cisco 7200. Stuck can happen with and without service policy also.

  Workarounds:

  1. Do a “shut”/”no shut” of affected interface.
  2. Do a soft OIR of affected slot.

- CSCsz72591

  Symptoms: A router crashes with an Address Error (load or instruction fetch) exception.

  Conditions: The router must be configured to act as a DHCP client.

  Workaround: There is no workaround.

- CSCsz72701

  Symptoms: DSP crashes are recorded.

  Conditions: This symptom is observed with a large volume of calls.

  Workaround: Reboot.

  Further Problem Description: The crash dump files indicate that some large packets are sent to DSP.

- CSCta17774

  Symptoms: An abnormal/high interarrival jitter time is reported in RTCP from a Cisco AS54xx when Nextport DSPs are used.

  Conditions: This symptom is observed under the following conditions:

  – Nextport DSPs are used on a Cisco AS54xx.

- RTCP is used to measure interarrival jitter values.

Workaround: There is no workaround.

- CSCta19962

  The H.323 implementation in Cisco IOS Software contains two vulnerabilities that may be exploited remotely to cause a denial of service (DoS) condition on a device that is running a vulnerable version of Cisco IOS Software.

  Cisco has released free software updates that address these vulnerabilities. There are no workarounds to mitigate these vulnerabilities other than disabling H.323 on the vulnerable device if H.323 is not required.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100324-h323.shtml.

- CSCta20040

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device when SIP operation is enabled.

  Cisco has released free software updates that address these vulnerabilities. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-sip.shtml.

  Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

  http://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

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

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

  Cisco Unified Communications Manager (CUCM) is affected by the vulnerabilities described in this advisory. Two separate Cisco Security Advisories have been published to disclose the vulnerabilities that affect the Cisco Unified Communications Manager at the following locations:

  http://www.cisco.com/warp/public/707/cisco-sa-20090826-cucm.shtml

  http://www.cisco.com/en/US/products/products_security_advisory09186a0080b4a313.shtml

- CSCta32825

  Symptoms: A Cisco 7206VXR may crash with a bus error after configuring a class-map or modifying a class-map.

  Conditions: This symptom is observed when using the **class- map** command in global configuration mode and the **match** command in class-map configuration mode. For example, entering the following commands may result in a crash:

```
router(config)#class-map match-any PRIO
router(config-cmap)#match dscp cs4
router(config-cmap)#match dscp cs4 af4
router(config-cmap)#match dscp cs4 af41 af42
router(config-cmap)#match dscp cs4 af41 af42 af43
router(config-cmap)#match dscp cs4 af41 af42 af43 ef
router(config-cmap)#match dscp cs4 af41 af42 af43 ef cs5 <---device crashes here
```

Workaround: Configure QoS changes when no traffic is passing through the router.

- CSCta39763

  Symptoms: A Cisco router may experience a memory leak in the "ISDN Call Table" process, as seen in the output below:

```
Router# show memory all totals
Allocator PC Summary for: Processor Displayed first 2048 Allocator PCs only
PC Total Count Name 0x6010B9E8 9891336 513 ISDN Call Tabl
```

  Conditions: This has been experienced on a Cisco 3845 router running Cisco IOS Release 12.4(22)T with ISDN configured.

  Workaround: There is no workaround.

- CSCta45976

  Symptoms: A BFD session cannot be established to the peer if the same IP address is configured on the device in a different VRF.

  Conditions: The symptom is observed when BFD sessions stay in a down state.

  Workaround: Remove the locally-configured IP address.

- CSCta49840

  Symptoms: GGSN may encounter a fatal error in VPDN/L2TP configurations.

  Conditions: The symptom is observed in rare race conditions when physical connectivity on the interface to LNS is lost while there are active sessions and traffic.

  Workaround: There is no workaround.

- CSCta56762

  Symptoms: A Cisco router acting as an IP SLA Responder may leak memory in the chunk manager.

  Conditions: The symptom is seen when the router is responding to VoIP RTP probes.

  Workaround: Stop the probes.

- CSCta66499

  Symptoms: The Cisco IOS MGCP gateway may experience a software-forced reload.

  Conditions: This symptom is observed with Cisc IOS Release 12.4(20)T4 or a later release when reenabling MGCP with version 1.0 after testing fgdos calls with MGCP version 0.1.

  Workaround: There is no workaround.

- CSCta77960

  Symptoms: TCP/TCB leak may occur on a Cisco voice gateway with an increasing number of sessions hung in CLOSEWAIT state.

  Conditions: This symptom occurs when the voice gateway is under normal use.

  Workaround: There is no workaround.

- CSCta85026

  Symptoms: CLI does not accept white spaces in the DHCP option 60 Vendor Class Identifier (VCI) ASCII string, and shows the following error message:

```
Router(dhcp-config)#option 60 ascii Cisco AP c1240
% Invalid input detected at '^' marker.
Router(dhcp-config)#
```

  Conditions: The symptom is observed with Cisco IOS Release 12.4(24)T1 and later.

  Workaround: There is no workaround.

- CSCta93129

  Symptoms: An IP fragment may bypass virtual fragment reassembly (VFR) processing and create a VFR timeout, causing additional inner IP fragments to be dropped.

  Conditions: This symptom is observed when encrypted IPSEC packets are fragmented by the remote device (fragmentation after encryption) or somewhere in the network between the VPN termination routers. When the fragmented IPSEC packets are reassembled and decrypted, if the decrypted inner packet is also an IP fragment, the IP fragment bypasses VFR processing. The following conditions may cause this symptom to occur:

  1. VFR is enabled on the decryption side
  2. Fragmentation happens after encryption on the encrypting router, or in the path
  3. The inner IP packet is fragmented when received by the encrypting router.

  Workaround: Perform fragmentation before encryption on the sending side, and ensure that the proper IP MTU is used on the tunnel so that no fragmentation occurs after encryption.

  Further Problem Description: When IPSEC packets corresponding to the first inner IP fragment bypass VFP processing, the second inner IP fragment, even if too small to require IPSEC fragmentation, is decrypted and then sent for VFR processing. Due to the timeout created when the first IP fragment bypasses VFR processing, the second inner IP fragment is dropped.

- CSCtb13421

  Symptoms: The GM may not register on a Cisco ASR 1000 series router.

  Conditions: This symptom is observed when a crypto map with local-address configured is applied on multiple interfaces, and one of these interfaces is then shut.

  Workaround: Disable local-address for the crypto map.

- CSCtb25549

  Symptoms: Router crashes.

  Conditions: The symptom is observed with the following sequence:

  1. Use the command **debug condition username**
  2. Bring up a VPDN session
  3. Clear the VPDN tunnel on LAC. 4
  4. Remove the conditional debug.

  Workaround: There is no workaround.

- CSCtb26396

  Symptoms: HTTPS connections suddenly fail with the following error:

  ```
  //-1//HTTPC:/httpc_ssl_connect: EXIT err = -3, hs_try_count=1
  //394376//HTTPC:/httpc_process_ssl_connect_retry_timeout: SSL socket_connect failed
  fd(0)
  ```

  Conditions: The symptom is observed with CVP Standalone deployment running with HTTPS and with Cisco IOS Release 12.4(22)T1 or Release 12.4(24)T1.

  Workaround: Reload the gateway.

- CSCtb45057

  Symptoms: A fax through a Cisco IOS gateway configured for Fax Relay to a Cisco fax server fails.

  Conditions: When there is an incoming fax call on the Cisco IOS gateway that is configured for Fax Relay, the fax call setup between the gateway and the Cisco fax server fails. This symptom occurs when the Cisco fax server is configured to receive calls on an H.323 call control module.

Workaround: There is no workaround. Configure SIP between the Cisco IOS gateway and the Cisco fax server if that is an acceptable workaround.

- CSCtb48397

  Symptoms: A Cisco ISR router may experience performance degradation due to corrupted TCP headers.

  Conditions: This symptom is observed on a Cisco ISR router with Cisco IOS Release 12.4 or Release 12.4T running interface-based TCP header compression on any data link. Corrupted TCP headers may occur when all of the following are true:

  1. Frame-Relay, PPP, or HDLC is configured with “ip tcp header-compression”
  2. The queueing mechanism is fair-queue (either interface-based or in map- class frame-relay)
  3. >1 TCP sessions are traversing the compressing mechanism
  4. The packets are in the hardware (CEF) switching path.

  Workarounds:

  1. Do not configure an interface to carry compressed TCP/IP headers using the **frame-relay ip tcp header-compression** command.
  2. Disable hardware switching for all interfaces on the Cisco ISR using the **no ip route-cache** command.
  3. Do not use any form of fair-queue on interfaces configured with the **frame-relay ip tcp header-compression** command. To remove fair-queue, use the **no fair-queue** command in policy-map class configuration mode.

  Further Problem Description: With exactly two MS Remote Desktop Protocol TCP sessions, when the UUT’s serial transmit-ring (or frame-relay shaper Bc) congests and the fair-queue invokes, the compressed header from the second- established TCP flow is erroneously written into headers of some packets from the first-established TCP flow, resulting in post-decompression frames erroneously added to the first-established TCP flow and erroneously removed from the second-established TCP flow, thereby causing a performance degradation.

- CSCtb51922

  Symptoms: Chunk leak of list element when a host-address under a PfR API provider is configured or unconfigured.

  Conditions: This symptom is observed when the following occur:

  - PfR MC is configured
  - API provider with a host address is configured
  - Host address is unconfigured, or the MC process is shut/no shut.

  Workaround: There is no workaround.

- CSCtb57180

  Symptoms: A router may crash with a software-forced crash.

  Conditions: Under certain conditions, multiple parallel executions of the **show users** command will cause the device to reload.

  Workarounds: It is possible to limit the exposure of the Cisco device by applying a VTY access class to permit only known, trusted devices to connect to the device via telnet, reverse telnet, and SSH.

  For more information on restricting traffic to VTYs, please consult:

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1818/products_configuration_example09186a0080204528.shtml

The following example permits access to VTYs from the 192.168.1.0/24 netblock and the single IP address 172.16.1.2 while denying access from everywhere else:

```
Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255 Router(config)# access-list
1 permit host 172.16.1.2 Router(config)# line vty 0 4 Router(config-line)#
access-class 1 in
```

For devices that act as a terminal server, to apply the access class to reverse telnet ports, the access list must be configured for the aux port and terminal lines as well:

```
Router(config)# line 1 <x> Router(config-line)# access-class 1 in
```

Different Cisco platforms support different numbers of terminal lines. Check your device's configuration to determine the correct number of terminal lines for your platform.

Setting the access list for VTY access can help reduce the occurrences of the issue, but it cannot completely avoid the stale VTY access issue. Besides applying the access list, the following is also suggested:

1. Avoid nested VTY access. For example, RouterA->RouterB->RouterA->RouterB.
2. Avoid issuing the **clear vty** command or the **clear line** command when there is any nested VTY access.
3. Avoid issuing the **clear vty** command or the **clear line** command when there are multiple VTY accesses from the same host.
4. Avoid issuing the **clear vty** command or the **clear line** command when router CPU utilization is high.
5. Avoid issuing the **show users** command repetitively in a short period of time.

Again, the above can help reduce the occurrences of the issue, but it cannot completely avoid the issue.

- CSCtb62177

  Symptoms: Downspeeding stops based on Voice and 4-second silence.

  Conditions: This symptom is observed on a Cisco AS5400.

  Workaround: An image with a partial short-term solution was released on 08-09-2009. With this image, module changes are done, and the CLI is implemented to drop 4-second silence events and voice packets.

- CSCtb66925

  Symptoms: A router may crash during a port scan to TCP port 53.

  Conditions: DNS functionality must be configured on the device.

  This crash has been observed only in Cisco IOS Release 12.4(24)T, Release 12.4(24)T1, and Release 12.4(22)T. It is a timing condition on processing DNS TCP traffic.

  Workaround: Create an ACL to deny traffic to the device on TCP port 53.

  The following mitigations have been identified for this Cisco bug ID, which may help protect an infrastructure until an upgrade to a fixed version of Cisco IOS software can be scheduled:

  – Infrastructure Access Control Lists (iACLs)

    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 Access Control Lists (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 these specific vulnerabilities. The iACL example below should be included as part of the deployed infrastructure access list, which will protect all devices with IP addresses in the infrastructure IP address range:

```
!--- !--- Feature: DNS over TCP !---
access-list 150 permit tcp TRUSTED_HOSTS WILDCARD INFRASTRUCTURE_ADDRESSES
WILDCARD eq 53
!--- !--- Deny DNS TCP traffic from all other sources destined !--- to
infrastructure addresses. !---
access-list 150 deny tcp any INFRASTRUCTURE_ADDRESSES WILDCARD eq 53
!--- !--- 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 serial 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. This white paper can be obtained at the following link:

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a0080 1a1a55.shtml

- Receive ACLs (rACLs)

  For distributed platforms, Receive ACLs may be an option starting in Cisco IOS Software Release 12.0(21)S2 for the Cisco 12000, Release 12.0(24)S for the Cisco 7500, and Release 12.0(31)S for the Cisco 10720. The Receive ACL protects the device from harmful traffic before the traffic can impact the route processor. Receive ACLs are designed to protect only the device on which they are configured. On the Cisco 12000, Cisco 7500, and Cisco 10720, transit traffic is never affected by a Receive ACL. Because of this, the destination IP address "any" used in the example ACL entries below refer only to the router's own physical or virtual IP addresses. Receive ACLs are considered 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 white paper entitled "Protecting Your Core: Infrastructure Protection Access Control Lists" presents guidelines and recommended deployment techniques for infrastructure protection access lists. This white paper can be obtained at the following link:

  http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a0080 1a0a5e.shtml

  The following is the receive path ACL written to permit this type of traffic from trusted hosts:

```
!--- !--- Permit DNS over TCP traffic from trusted hosts allowed to the RP. !---
access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD any eq 53
!--- !--- Deny DNS over TCP traffic from all other sources to the RP. !---
access-list 150 deny tcp any any eq 53
!--- Permit all other traffic to the RP according !--- to security policy and
configurations.
access-list 150 permit ip any any
!--- Apply this access list to the 'receive' path.
ip receive access-list 150
```

- Control Plane Policing

  Control Plane Policing (CoPP) can be used to block the affected features TCP traffic access 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 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 that will protect all devices with IP addresses in the infrastructure IP address range.

```
!--- !--- Feature: DNS over TCP !---
access-list 150 deny tcp TRUSTED_HOSTS WILDCARD any eq 53
!--- !--- Permit DNS over TCP traffic sent to all IP addresses !--- configured on
```

```
all interfaces of the affected device so !--- that it will be policed and dropped
by the CoPP feature. !---
access-list 150 permit tcp any any eq 53
!--- !--- Permit (Police or Drop)/Deny (Allow) all other Layer 3 and !--- Layer 4
traffic in accordance with existing security policy !--- configurations for
traffic that is authorized to be sent !--- and to infrastructure devices. !---
Create a class map for traffic to be policed by !--- the CoPP feature. !---
class-map match-all drop-tcp-class match access-group 150
!--- !--- Create a policy map that will be applied to the !--- control plane of
the device. !---
policy-map drop-tcp-traffic class drop-tcp-class drop
!--- !--- Apply the policy map to the !--- control plane of the device. !---
control-plane service-policy input drop-tcp-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. Please note that the policy-map syntax is different in the 12.2S and 12.0S Cisco IOS trains:

```
policy-map drop-tcp-traffic class drop-tcp-class police 32000 1500 1500
conform-action drop exceed-action drop
```

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

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

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlimt.html

- CSCtb71889

  Symptoms: DNS A-answer from IPv4 DNS server (which is supposed to be forwarded to IPv6 side as AAAA-answer) is dropped on NAT-PT routers.

  Conditions: The symptom is observed when DNS NAT-ALG is enabled.

  Workaround: There is no workaround.

- CSCtb89424

  Symptoms: In rare instances, a Cisco router may crash while using IP SLA udp probes configured using SNMP and display an error message similar to the following:

  ```
  hh:mm:ss Date: Address Error (load or instruction fetch) exception, CPU signal 10, PC
  = 0x424ECCE4
  ```

  Conditions: This symptom is observed while using IP SLA.

  Workaround: There is no workaround.

- CSCtb93855

  The H.323 implementation in Cisco IOS Software contains two vulnerabilities that may be exploited remotely to cause a denial of service (DoS) condition on a device that is running a vulnerable version of Cisco IOS Software.

  Cisco has released free software updates that address these vulnerabilities. There are no workarounds to mitigate these vulnerabilities other than disabling H.323 on the vulnerable device if H.323 is not required.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100324-h323.shtml.

- CSCtc04016

  Symptoms: A Cisco IOS VoIP gateway configured for IPIPGW/CUBE may experience high CPU utilization, which causes additional calls through the router to fail.

Conditions: This symptom is observed under rare conditions when SIP- associated processes on the Cisco IOS gateway (as seen when the **show process cpu** command is entered) cause extremely high CPU utilization, which causes further calls through the router to fail.

Workaround: There is no workaround.

Further Problem Description: This symptom occurs due to a SIP "491 Request Pending" and ACK loop between the gateway and a third-party device. This loop most often occurs in environments with a large number of SIP REFER transfers. To determine whether the loop is occurring, enter the **show sip statistics** command and look for the RequestPending value; a high and increasing output count could indicate the SIP loop.

- CSCtc17162

  Symptoms: A Cisco router may crash due to a SegV exception.

  Conditions: This symptom is observed on a Cisco 2650XM router running Cisco IOS Release 12.4(15)T10 when VTI is configured inside the EzVPN.

  Workaround: Remove the VTI inside the EzVPN.

- CSCtc18562

  Symptoms: When Network Address Translation (NAT) of the outside source address is enabled, the static route to the local IP address is installed in the global RIB instead of the VRF RIB.

  Conditions: This symptom is observed when enabling NAT of the outside source address using the **ip nat outside source static** *global-ip local-ip* **vrf** *vrf name* **add-route extendable match-in-vrf** command.

  Workaround: Configure a static route within the VRF.

- CSCtc32374

  Symptoms: ISDN Layer 1 is deactivated after a reload, and calls fail with a cause code 47 (Resource Unavailable).

  Conditions: This symptom is observed when **busyout monitor** is configured and the TEI controller comes up before the monitored interface.

  Workaround: Remove the busyout monitor configuration using the **no busyout monitor** command in voice-port configuration mode.

  Further Problem Description: Entering the **shutdown** command followed by the **no shutdown** command will bring the PRI Layer 1 to Active and Layer 2 to a MULTIFRAME-ESTABLISHED connection status, but calls still fail with cause code 47.

- CSCtc68705

  Symptoms: A router may crash with a bus error.

  Conditions: This symptom is observed when a Cisco firewall withdraws a default route and the Cisco IOS router has another default route as a backup. This symptom is observed only when peering with a firewall, not a Cisco IOS router.

  Workaround: There is no workaround.

- CSCtc70490

  Symptoms: A Cisco IOS VoIP gateway may intermittently experience dropped calls and loss of audio.

  Conditions: This symptom is observed when the DSP used in the call fails to respond. When this occurs, the following error messages may be displayed:

```
%C5510-1-C5510_CHPI_ERROR: cHPI error for pa_bay 1 pump 1 dsp 9.
%C5510-1-NO_RING_DESCRIPTORS: No more ring descriptors available on slot 1 dsp 9.
%C5510-1-NO_RING_DESCRIPTORS: No more ring descriptors available on slot 1 dsp 9.
```

This symptom is observed only in DSPware 9.4.811. To determine the DSPware version residing on the gateway, enter the **show voice dsp group all** command in global configuration mode.

Workaround: Use a Cisco IOS Release prior to 12.4(15)T10, or load another version of DSPware by working with the TAC. See the following for more information about DSPware:

http://www.cisco.com/en/US/tech/tk652/tk698/technologies_tech_note09186a0080a7 af82.shtml

- CSCtc73441

  Symptoms: A CPUHOG message is observed on the key server (KS) when the **show crypto gdoi ks members** command is executed. As a result of the CPUHOG, the BGP session goes down between the KS and the iBGP neighbor.

  Conditions: The symptom is observed on primary or secondary key servers that have more than 1000 group members.

  Workaround: There is no workaround.

- CSCtd03835

  Symptoms: ISR stops forwarding any kind of traffic received from the wireless client to other APs even though the client entry is present in ISR dot11 association table.

  Conditions: Sometimes clients flush out the ARP cache while roaming. In such cases, the symptom is observed when a client resends a request after roaming.

  This issue is observed with IOS 12.4.11T2. It is also present in IOS 12.4.24T, but the issue is less observed.

  Workaround: Clearing association table of the router resolves the issue.

- CSCtd15454

  Symptoms: A Cisco router may crash while performing online insertion and removal (OIR).

  Conditions: This symptom is observed on a Cisco 7200 NPE-G1 router on PA-GIG in an MPLS environment with traffic.

  Workaround: There is no workaround.

- CSCtd18510

  Symptoms: A Cisco router may crash and display a SegV exception error.

  Conditions: This symptom is observed on a Cisco router when OSPF connects the CE and PE routers in an MPLS VPN configuration, and when none of the interfaces are in area 0. This symptom is seen only in Cisco IOS Software versions with the OSPF Local RIB feature.

  Workaround: Enter the **no capability transit** command in the OSPF routing processes.

- CSCtd59174

  Symptoms: PfR MC logs an Exit Mismatch after controlling a traffic class using policy based routing (PBR). At this point, PfR uncontrols the traffic class because it appears that traffic is not flowing over the exit interface that is expected.

  Conditions: This condition is observed under the following conditions:

  – At least one Cisco Catalyst 6000 PfR BR must by configured.

  – Monitor mode must include passive monitoring such as mode monitor both or mode monitor passive.

Workaround: Apply mode monitor active policy to the traffic classes controlled by PBR. Note, however, that this will prevent these traffic classes from being used for load, range, or cost policies.

- CSCte21958

  Symptoms: A Cisco router may reload when an L2TP xconnect pseudowire is configured using a pseudowire class that has not yet been defined.

  ```
  Conditions: This symptom is observed when the following sequence of commands is
  entered: configure terminal
  interface Ethernet0/0.1
  encapsulation dot1Q 400
  xconnect 10.0.0.1 555 encapsulation l2tpv3 pw-class test
  pseudowire-class test
  encapsulation l2tpv3
  protocol l2tpv3 test
  ip local interface Loopback0
  vpdn enable
  ```
  This symptom affects all platforms.

  Workaround: Define the pseudowire class using the **pseudowire- class** configuration command before referencing that pseudowire class in an xconnect configuration.

- CSCte54823

  Symptoms: Router reloads while unconfiguring the **isdn calling-number** command.

  Conditions: This symptom is observed while unconfiguring the **isdn calling-number** command. This issue is observed only with the Cisco IOS Release 12.4(15)T12.fc2 image, whereas it is not observed with Cisco IOS Release 12.4(15)T12 and Release 12.4(15)T11 images.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(15)T11

Cisco IOS Release 12.4(15)T11 is a rebuild release for Cisco IOS Release 12.4(15)T. The caveats in this section are resolved in Cisco IOS Release 12.4(15)T11 but may be open in previous Cisco IOS releases.

- CSCsy29533

  Symptoms: A T.38 fax relay call may fail.

  Conditions: The symptom is observed with an MGCP-controlled T.38 fax relay call when the gateway is configured for CA control T.38. The output of the **debug voip vtsp all** command shows fax relay as “DISABLED.”

  Workaround: Use Cisco IOS Release 12.4(15)T7 or Release 12.4(22)T.

- CSCta17774

  Symptoms: An abnormal/high interarrival jitter time is reported in RTCP from a Cisco AS54xx when Nextport DSPs are used.

  Conditions: This symptom is observed under the following conditions:

  – Nextport DSPs are used on a Cisco AS54xx.
  – RTCP is used to measure interarrival jitter values.

  Workaround: There is no workaround.

- CSCtb62177

  Symptoms: Downspeeding stops based on Voice and 4-second silence.

Conditions: This symptom is observed on a Cisco AS5400.

Workaround: An image with a partial short-term solution was released on 08-09-2009. With this image, module changes are done, and the CLI is implemented to drop 4-second silence events and voice packets.

Resolved Caveats—Cisco IOS Release 12.4(15)T10

Cisco IOS Release 12.4(15)T10 is a rebuild release for Cisco IOS Release 12.4(15)T. The caveats in this section are resolved in Cisco IOS Release 12.4(15)T10 but may be open in previous Cisco IOS releases.

- CSCsd34595

  Symptoms: LDP session between two LSRs cannot be established. “show mpls ldp discovery” shows normal output, both LSRs discovered peer. “show mpls ldp neighbor” does not show session with the peer. “show tcp brief all” shows that a TCP listen port on port 646 is opened for the peer on both sides, like the following:

```
PE6#show tcp brief all
TCB       Local Address               Foreign Address             (state)
03F32918  0.0.0.0.646                 10.0.0.7.*                  LISTEN

PE7#show tcp brief all
TCB       Local Address               Foreign Address             (state)
037B5D58  0.0.0.0.646                 10.0.0.6.*                  LISTEN
```

  Conditions: This problem can occur only if the following conditions are met:

  1. User changes the LDP transport address when LDP is trying to bring up an LDP session;
  2. Before changing LDP transport address, the local LDP transport address is smaller than the peer transport address;
  3. After changing LDP transport address, the local LDP transport address is bigger than the peer transport address;
  4. The transport address changing happens after LDP started listening to the peer based on old transport address but before sending another LDP hello.

  Workaround: Flapping “mpls ip” interface configuration on the router that changed LDP transport address.

- CSCsg00836

  Symptoms: The command **no crypto ipsec nat-transparency udp-encaps** is getting enabled by default on a freshly-reloaded router. Also, even after enabling the command **no crypto ipsec nat-transparency udp-encaps** and then using the **write memory** command, **no crypto ipsec nat-transparency udp-encaps** gets enabled once the router is reloaded.

  Conditions: The symptoms are observed when the router is reloaded and the command **show run | inc nat** is issued at the console prompt:

```
ireg2-02#sh run | inc nat
 destination address cat6k-auto-notify@cisco.com
 no crypto ipsec nat-transparency udp-encaps
```

  Workaround: Enable the command **no crypto ipsec nat-transparency udp-encaps** and run the test. After enabling this command the routers are NOT reloaded because if the routers are reloaded then the **no crypto ipsec nat-transparency udp-encaps** command would be enabled.

- CSCsh60033

  Symptoms: CPU hog seen on router console.

Conditions: The symptom is observed with a large number of ISIS neighbors for each session of ISIS.

Workaround: There is no workaround.

- CSCsi33626

  Symptoms: One may intermittently see a traceback from the Transport Port Agent because of timing of subsystem initialization in the router. The traceback is nonimpacting to the actual functional performance of the router.

  Conditions: This symptom is observed at bootup.

  Workaround: There is no workaround.

- CSCsi47359

  Symptoms: A router crashes when a PSTN call is forwarded.

  Conditions: The symptom is observed when a PSTN call is forwarded to another PSTN line number.

  Workaround: There is no workaround.

- CSCsj17977

  Symptoms: The GETVPN rekey fails. The following error message shows in the syslog:

  ```
  %GDOI-3-GM_NO_IPSEC_FLOWS: IPSec FLOW limit possibly reached
  ```

  The **show crypto engine connections flow** will show that all flows are used. For hardware-accelerated platforms, use the **show crypto eli** command to see how many Phase IIs are supported.

  Conditions: This problem is seen when the registration is not successful on a group member and then the flow IDs allocated for that incomplete registration are not cleaned up.

  Workaround: Reload the router, if the all the flow IDs are leaked.

- CSCsj36133

  Symptoms: A BGP neighbor may send a notification reporting that it received an invalid BGP message with a length of 4097 or 4098 bytes.

  Conditions: The problem can be seen for pure IPv4 BGP sessions (no MP-BGP in use) when the router that is running the affected software generates a large number of withdraws in a short time period and fills an entire BGP update message (up to 4096 bytes normally) completely with withdraws. Because of a counting error, the router that is running the affected software can generate an update message that is 1 or 2 bytes too large when formatting withdraws close to the 4096 size boundary.

  Workaround: The issue is not seen when multiple address families are being exchanged between BGP neighbors.

- CSCsk17498

  Symptoms: When per port storm control is configured and traffic is bursted on the port, the router crashes.

  Conditions: This symptom occurs when the port is controlled by storm control and configured for some value. If the traffic bursts on the interface, the port shuts and the router crashes.

  Workaround: Unconfigure storm control on interface.

- CSCsk48089

  Symptoms: This is to allow users to unconfigure policy on an interface when both route-map tag and "CR" option are given.

  Conditions: Enhancement in the **ip policy route-map** command for backward compatibility.

Workaround: There is no workaround.

- CSCsk65515

  Symptoms: Spurious or misaligned memory access can be seen at atm_nvgen_static_map.

  Conditions: The symptoms can be observed when an SVC is configured on an ATM interface and when executing the command **show running- config**.

  Workaround: There is no workaround.

- CSCsl15443

  Symptoms: Console port can lock up after 10-15 minutes. Telnet sessions fail.

  Conditions: Occurs when terminal server is connected to router's console port.

  Workaround: There is no workaround.

- CSCsm53260

  Symptoms: TCP may exhibit some unexpired managed timers. The TCP retransmission timer for a given TCB in **show tcp** may be past due.

  Conditions: This is a rare situation.

  Workaround: There is no workaround.

- CSCsm53996

  Symptoms: Router crashes while unconfiguring IP SLA RTP.

  Conditions: The issue is seen only when very large number of RTP operations (1000) are configured.

  Workaround: There is no workaround.

- CSCso05336

  Symptoms: A Cisco 1811 router reloads when trying to connect to irc.freenode.net during the first 36 hours following a reload.

  Conditions: The symptom is observed only in the first 36 hours following a reload.

  Workaround: Do not connect to irc.freenode.net the first 36 hours following a reload.

- CSCso67601

  Symptoms: When a call using a CMM ACT transcoder is disconnected from the H323 endpoint, the transcoder shows as being unregistered. The transcoder remains unregistered on resetting it from the CCMAdmin page. The **show dspfarm all** command shows two active connections even though the CCM side has already cleared the call.

  Conditions: The symptoms are observed when a CMM ACT transcoder is used and the call is cleared by an H323 endpoint.

  Workaround: On reloading the jagger, the transcoder registers to the CCM.

- CSCso97304

  Symptoms: Configuring and unconfiguring hierarchical QoS may cause memory leak on a Cisco router.

  Conditions: This symptom occurs on a Cisco router that is running Cisco IOS Release 12.4(15)T4.

  Workaround: There is no workaround.

- CSCsq24002

  Cisco IOS Software contains a vulnerability that could allow an attacker to cause a Cisco IOS device to reload by remotely sending a crafted encryption packet. Cisco has released free software updates that address this vulnerability. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-tls.shtml.

- CSCsq51158

  Symptoms: The signal of a Cisco 851w router may fluctuate.

  Conditions: The symptom applies to different environments where multi-path is more of an issue.

  Workaround: There is no workaround.

  Further Problem Description: A spectrum analyzer shows that the router has a signal of -60(+/-10)Db and that it stays at that level for about 7-10 seconds. It then drops by 40Db for 7-10 seconds before it restores itself to its original level.

- CSCsq58289

  Symptoms: The connected interface prefix that is redistributed to OSPF is not seen as a Type 5 LSA in the OSPF database.

  Conditions: The symptom is observed with the prefix that is initially covered by a “network ...” statement under **router ospf ...** and later removed by doing **no router ospf ...** instead of **no network ...**.

  Workaround: Perform a **shut** then **no shut** on the interface with the prefix that is not being redistributed.

- CSCsr16147

  Symptoms: Session is not getting disconnected when the locally configured timers expire.

  Conditions: Occurs while testing an internal build of Cisco IOS Release 12.4(22)T on the Cisco 7200.

  Workaround: There is no workaround.

- CSCsr20889

  Symptoms: The system reloads.

  Conditions: The symptom is observed when a dynamic crypto map is added to the existing GETVPN crypto map with a different sequence.

  Workaround: There is no workaround.

- CSCsr60092

  Symptoms: One-way audio is observed after use of TCL [connection create] command.

  Conditions: Occurs with TCL application playing media in incoming_leg and leg setup without bridging incoming leg [leg setup $dnis callInfo].

  Workaround: There is no workaround.

- CSCsr62645

  Symptoms: Software-forced reload occurs on Cisco 870 router.

  Conditions: Encountered during extended VLAN testing.

  Workaround: There is no workaround.

- CSCsr90248

  Symptoms: Changing any of the parameters of a route-map does not take effect.

Conditions: Occurs when using a BGP aggregate-address with an advertise map.

Workaround: Delete the aggregate-address statement and then put it back for the change to take effect.

- CSCsr96042

  Symptoms: ASR1000 Router crashes.

  Conditions: Occurs if “ip vrf” is deleted from the configuration.

  Workaround: There is no workaround.

- CSCsr96084

  Symptoms: A router crashes with the following error:

  ```
  %SYS-6-STACKLOW: Stack for process NHRP running low, 0/6000
  ```

  Conditions: The symptom is seen on routers that are running Dynamic Multipoint VPN (DMVPN) when a routing loop occurs while an NHRP resolution request is received by the router. If the routing loop leads to a tunnel recursion (where the route to the tunnel endpoint address points out of the tunnel itself) the crash may be seen.

  Workaround: Use PBR for locally-generated traffic to force the GRE packet out of the physical interface which prevents the lookup that can lead to the recursion. For example (note: the interfaces and IPs will need to be changed to the appropriate values):

  ```
  interface Tunnel97
   ...
   tunnel source POS6/0
   ...

   interface POS6/0
   ip address 10.2.0.1 255.255.255.252

   ip local policy route-map Force-GRE

   ip access-list extended Force-GRE
   permit gre host 10.2.0.1 any

   route-map Force-GRE permit 10
   match ip address Force-GRE
   set interface POS6/0
  ```

- CSCsu02975

  Symptoms: Router crashes due to memory corruption.

  Conditions: WAN router crashes when feature combination includes Frame Relay, EIGRP, GRE, QoS, and multicast are configured on WAN aggregation and branches.

  The issue is seen only on PA-MC-2T3/E3-EC. The issue is seen only when frame-relay fragment and service-policy is part of map-class frame-relay configurations.

  Workaround: Have either frame-relay fragment or service-policy as part of map-class frame-relay configurations.

- CSCsu32452

  Symptoms: Spurious memory access occurs.

  Conditions: Occurs while attempting to unconfigure the EzVPN client configuration on an EzVPN client inbound interface.

  Workaround: There is no workaround.

- CSCsu58763

  Symptoms: Card crashed upon attaching the policy-map to the output interface.

  Conditions: Happening in all types of VCs (PVC/SVC) when the service policy is defined with **shape** command.

  Workaround: There is no workaround.

- CSCsu73571

  Symptoms: VIP may crash on a Cisco 7500 series router.

  Conditions: The symptom is observed when Distributed Link Fragmentation and Interleaving over Leased Lines (dLFIoLL) or Distributed Link Fragmentation and Interleaving over ATM (dLFIoATM) is configured and "ip flow egre" is configured on multilink or VT.

  Workaround: There is no workaround.

- CSCsu79754

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

  Conditions: Unknown at this time.

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

- CSCsu92724

  Symptoms: The following errors are logged:

```
Sep 21 05:07:25: %ISDN-4-ISDN_UNEXPECTED_EVENT: INVALID INPUT: Occurred at
../isdn/isdnif_modem.c:99 Sep 21 05:07:25: %SYS-2-QCOUNT: Bad dequeue 62D74734 count
-1 -Process= "ISDN", ipl= 4, pid= 162 -Traceback= 0x6046769C 0x605B2E64 0x60158F0C
0x600B2204 0x600B2238 0x600B220C
Sep 21 05:07:25: %ISDN-4-ISDN_UNEXPECTED_EVENT: INVALID INPUT: Occurred at
../isdn/isdnif_modem.c:99 Sep 21 05:07:25: %SYS-2-QCOUNT: Bad dequeue 62D74734 count
-1 -Process= "ISDN", ipl= 4, pid= 162 -Traceback= 0x6046769C 0x605B2E64 0x60158F0C
0x600B2204 0x600B2238 0x600B220C
Sep 21 05:07:25: %ISDN-4-ISDN_UNEXPECTED_EVENT: INVALID INPUT: Occurred at
../isdn/isdnif_modem.c:99 Sep 21 05:07:25: %SYS-2-QCOUNT: Bad dequeue 62D74734 count
-1 -Process= "ISDN", ipl= 4, pid= 162 -Traceback= 0x6046769C 0x605B2E64 0x60158F0C
0x600B2204 0x600B2238 0x600B220C
Sep 21 05:07:25: %ISDN-4-ISDN_UNEXPECTED_EVENT: INVALID INPUT: Occurred at
../isdn/isdnif_modem.c:99 Sep 21 05:07:28: %SYS-2-QCOUNT: Bad dequeue 62D74734 count
-1 -Process= "ISDN", ipl= 4, pid= 162 -Traceback= 0x6046769C 0x605B2E64 0x60158F0C
0x600B2204 0x600B2238 0x600B220C
Sep 21 05:07:28: %ISDN-4-ISDN_UNEXPECTED_EVENT: INVALID INPUT: Occurred at
../isdn/isdnif_modem.c:99 Sep 21 05:07:28: %SYS-2-QCOUNT: Bad dequeue 62D74734 count
-1 -Process= "ISDN", ipl= 4, pid= 162 -Traceback= 0x6046769C 0x605B2E64 0x60158F0C
0x600B2204 0x600B2238 0x600B220C
Sep 21 05:07:28: %ISDN-4-ISDN_UNEXPECTED_EVENT: INVALID INPUT: Occurred at
../isdn/isdnif_modem.c:99 Sep 21 05:07:28: %SYS-2-QCOUNT: Bad dequeue 62D74734 count
-1 -Process= "ISDN", ipl= 4, pid= 162 -Traceback= 0x6046769C 0x605B2E64 0x60158F0C
0x600B2204 0x600B2238 0x600B220C
```

  Conditions: Occurs when ISDN is enabled.

  Workaround: There is no workaround.

- CSCsv27607

  Symptoms: BGP router filters outbound routes to the peers when doing soft reset with specifying peer address using the **clear ip bgp** *ip-addr* **soft out** command. However, the routes to be filtered are not deleted from the routing table on the BGP peer router.

Conditions: The symptom happens when removing and then reapplying an outbound route-map. When issuing the **clear ip bgp** *neighbor-address* **soft out** command for each peer in an update-group after applying the outbound route-map filtering policy. The withdraw for filtered prefixes is sent to the first peer specified in soft reset, but the next peers in the same update-group do not withdraw the routes.

Workaround: Perform a hard BGP reset using the **clear ip bgp** *ip-addr* command.

- CSCsv30540

  Symptoms: The error message %SYS-2-CHUNKBOUNDSIB and traceback are seen.

  Conditions: The symptoms are observed when the **show running- config/write memory** command is issued.

  Workaround: There is no workaround.

- CSCsv91628

  Symptoms: BGP prefixes are not exchanged between route reflectors.

  Conditions: Occurs when route reflectors are present in different AS and they have MP-EBGP relationship between them.

  Workaround: There is no workaround.

- CSCsw43211

  Symptoms: Following errors are seen:

  ```
  %IDMGR-3-INVALID_ID: bad id in id_to_ptr (bad id) (id: 0xFFFFFFFF)
  -Traceback= 60476EBC 60477400 60491664 616C5834 616C7EEC 61AB72CC 61AC2E64 61AC2EBC
  60FE4274 60FDEFA4 60FD4180 60FD4874 60FD4BBC 60FD275C 60FD27A0 60FC8F74
  ```

  Conditions: This has been seen on a Cisco 7200 after upgrading to Cisco IOS Release 12.2(33)SRC2.

  Workaround: There is no workaround.

- CSCsw64933

  Symptoms: A VXML gateway may stop providing audio prompts to caller.

  Conditions: This symptom occurs when TTS text contains “&”, which is escaped as “&”. The XML parser converts it to “&”. VXML interpreter did not escape it when sending the TTS to server. This causes TTS to generate a parse error.

  Workaround: Remove the “&” in the VXML script.

- CSCsw78413

  Symptoms: The BFD configuration may be lost from the interface/sub-interface upon a router reload or physical module of OIR.

  Conditions: The symptom is seen when BFD is configured on an interface in certain multi-slot chassis.

  Workaround: Ethernet interfaces seem immune to this problem. Certain platforms, such as the Cisco 10000 series router, are also immune.

- CSCsw78879

  Symptoms: The secondary key server crashes when it sends a KEK rekey to the GMs soon after it takes over as the primary key server.

  Conditions: The symptom is seen when the secondary key server switches to primary just before it is time to send the KEK rekeys to the group members. This problem can be seen in any co-operative key server environment.

Workaround: There is no workaround.

- CSCsw85293

  Symptoms: The following CPUHOG messages are seen for Crypto ACL process:

  ```
  %SYS-3-CPUHOG: Task is running for (xxxx)msecs, more than (2000)msecs (9/7),process =
  Crypto ACL.
  ```

  Conditions: This has been seen on Cisco routers that are running Cisco IOS Release 12.4(15)T8 (other versions may be affected as well) with GETVPN configured.

  Workaround: Reducing the size and complexity of the crypto ACLs will often stop these errors.

- CSCsw93682

  Symptoms: The KS database becomes unreliable.

  Conditions: The symptom is observed when clearing the GM database from KS and re-registering GMs with different criteria.

  Workaround: There is no workaround.

- CSCsx07423

  Symptoms: The router stays at 100% CPU usage after trying to establish an SSL session with an SSL server when this SSL server is not reachable.

  Conditions: The symptom is observed with any applications on the router that use an SSL client to establish a secure session with the SSL server. At the same time, the secure server is not available for whatever reason.

  Workaround: Make sure the SSL server is reachable by pinging it. Save the configuration as startup-config and reload the router.

- CSCsx20984

  Symptoms: Router reloads with a bus error and no tracebacks.

  Conditions: Unknown at this time.

  Workaround: There is no workaround.

- CSCsx25880

  A vulnerability exists in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software that could allow an unauthenticated attacker to cause a denial of service (DoS) condition on an affected device when the Cisco Unified Border Element feature is enabled. Cisco has released free software updates that address this vulnerability. For devices that must run SIP there are no workarounds; however, mitigations are available to limit exposure of the vulnerability. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-sip.shtml.

- CSCsx34297

  Symptoms: Watchdog reset seen with combination of NPEG1+PA-POS-1OC3/PA-POS-2OC3.

  Conditions: The symptom is observed on a Cisco 7200 series router and Cisco 7301 router with an NPEG1 processor.

  Workaround: Change the MDL of operation to PULL using the command **dma enable pull model**.

- CSCsx46421

  Symptoms: The file transfer aborts with the Active FTP.

  Conditions: The symptom is observed with the image c7200-adventerprisek9-mz.124-23.15.T3.

  Workaround: Use Passive FTP (**ip ftp passive**) for the FTP file to be properly transferred.

- CSCsx47915

  Symptoms: Spurious memory access and alignment error observed when removing policy-map from interface under certain configuration sequence.

  Conditions: The problem is seen on Cisco routers running Cisco IOS Release 12.4(18e).

  Workaround: There is no workaround.

- CSCsx55861

  Symptoms: On a Cisco 880 router, the UUT crashes when the PVC comes up and when “auto qos voip” is configured.

  Conditions: The symptom is observed when “auto qos voip” is configured under ATM and when the PVC is toggled (due to, for example, a shut/no shut of the ATM interface or a cable being pulled and then restored).

  Workaround: There is no workaround.

- CSCsx59436

  Symptoms: Cisco 837 experiences failure of LAN ports after power cycle. If the LAN port is set to 100/Full, the connection to the other device cannot be reestablished.

  Conditions: Occurs on a router running either Cisco IOS Release 12.3 or 12.4.

  Workaround: Set the LAN port to duplex and speed Auto/Auto.

- CSCsx67255

  Symptoms: An outgoing call from an IP phone to PSTN through ISDN PRI fails on a channel due to a DSP allocation failure (not enough DSPs to support the call). Subsequent calls through that same channel continue to fail with “resource unavailable” cause value equal to 47 even after DSP resources have been made available to handle the call.

  Conditions: The symptom occurs on a router running Cisco IOS Release 12.4(15)T8 or higher. The call must first fail with a legitimate DSP allocation error. Any call made through the same channel as the failed call will also fail.

  DSP allocation failures on gateway can be checked through the use of the exec command **show voice dsp group all**. The last line of the show command output includes a counter for “DSP resource allocation failure”.

  This issue can be seen also in some cases upon bootup. When a gateway is reloaded, system resources will come up with slightly different timing. If, for example, a PRI interface comes up before the DSP resources have fully initialized, there may be a similar failure.

  Workaround:

  1. Reload the router to clear the channel. If a reload cannot be done, busy out the channel with the failed calls using the **isdn busy b_channel** command under the serial interface.
  2. If this issue is due to oversubscription of the DSP resources, change the configuration to meet the DSP resources available on the gateway. Further information can be found with the CCO “DSP Calculator” at http://www.cisco.com/cgi-bin/Support/DSP/cisco_prodsel.pl.
  3. If the issue is related to timing issues upon reload, shutdown the voice-port in question before reloading the gateway. When the gateway comes back up, take the voice-port out of shutdown.

- CSCsx68596

  Symptoms: The system may display a %SYS-3-NOELEMENT message, similar to:

  ```
  %SYS-3-NOELEMENT: data_enqueue:Ran out of buffer elements for enqueue
  -Process= "<interrupt level>", ipl= 6
  ```

after which system behavior can be unpredictable. If the interrupts are rapid enough, the system may become unresponsive (hang), use all available memory to create more buffer elements, or crash due to CSCsj60426.

Conditions: The message is caused by extremely rapid changes in flow control or modem control lead status on a console port.

Workaround: Eliminate the source of the rapid lead changes. As modem control and flow control are generally not supported on the console, these changes are usually due to misconfigured devices attached to the console.

- CSCsx70889

  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/warp/public/707/cisco-sa-20090923-tunnels.shtml.

- CSCsx75353

  Symptoms: High CPU usage is observed on a Cisco 2821 router. An increase of almost 10 percent in CPU utilization is observed with every voice call.

  Conditions: This symptom is observed when an AIM compression card is present on the motherboard (specifically AIM-COMPR2-V2).

  Workaround: Remove the AIM compression card from the motherboard.

- CSCsx94324

  Symptoms: Packets with certain packet sizes get dropped when being CEF-switched on a router.

  Conditions: The symptom is observed when CEF is enabled and when the outbound interface is an HWIC-4SHDSL DSL interface. It is observed when the packet undergoes fragmentation.

  Workaround: Disabling CEF is a workaround.

- CSCsx98284

  Symptoms: A router may crash with a bus error and with a corrupted program counter:

  ```
  %ALIGN-1-FATAL: Corrupted program counter pc=0x66988B14 , ra=0x66988AFC ,
  sp=0x66A594D0
  ```

  Conditions: The symptom is observed on a Cisco IOS Voice over IP (VOIP) gateway configured for IPIPGW (CUBE) as well as Cisco Unified Communications Manager (CUCM) controlled MTP on the same gateway. Under situations where a call loop is present (same call routing back-forth through the same gateway), the system may reload if an MTP is also present in the loop.

  Workaround: Find and break the source of the call loop. Be careful of default destination-pattern/route-patterns that may kick in under some conditions.

  Alternate workaround: Separate the MTP functionality from the gateway.

- CSCsy05111

  Symptoms: A router crashes after enabling and disabling NBAR on an interface if a class-map with match protocol is configured first (“match protocol rtp audio”).

  Conditions: The symptom is observed if the “match protocol rtp audio” statement is found in the class-map configuration. RTP uses a label heuristic which quickly reproduces the bug.

  Workaround: Do a config/no-config on one interface while keeping NBAR configured on any other interface.

- CSCsy05298

  Symptoms: The IOSD-crash is seen and is affecting the main functionality.

  Conditions: This symptom is observed when a large number of groups (i.e. 50) is configured. The IOSD-crash is seen when we give the **show crypto gdoi** command after applying the general configuration and after checking the ping between all the PIM neighbors.

  Workaround: Use the **show crypto gdoi group** *group- name* to display a specific group's information.

- CSCsy09250

  Skinny Client Control Protocol (SCCP) crafted messages may cause a Cisco IOS device that is configured with the Network Address Translation (NAT) SCCP Fragmentation Support feature to reload.

  Cisco has released free software updates that address this vulnerability. A workaround that mitigates this vulnerability is available.

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

- CSCsy10893

  Symptoms: A router reloads occasionally after the command **show buffers leak** is repeatedly issued.

  Conditions: The symptom is observed when issuing the **show buffers leak** command. It occurs only with certain patterns and scale of traffic and does not occur all the time.

  Workaround: There is no workaround.

- CSCsy16078

  Symptoms: A GETVPN group member might reload when removing "crypto map" from the interface, if that crypto map also contains a dynamic-map set together with the GDOI set.

  Conditions: The symptom only occurs when a dynamic-map set is added to a crypto map that is already applied to an interface and then the whole crypto map is removed, added and removed again. It is on the second removal that the reload occurs.

  Workaround: Execute the command **clear crypto gdoi** before removing the crypto map from the interface.

- CSCsy16092

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

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

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

  Workaround: Remove this debug command.

- CSCsy16177

  Symptoms: Cisco 2811 experiences invalid checksum over SCP on SSH version 2.

  Conditions: Occurs on a Cisco 2811 with flash type file system.

  Workaround: There is no workaround.

- CSCsy19659

  Symptoms: When using Point-to-Point Tunnelling Protocol (PPTP) with RADIUS Accounting, there may be several "nas-error" and "lost-carrier" listed in accounting as the Acct-Terminate-Cause.

Conditions: The symptom is observed when using Cisco IOS Release 12.4T (Releases 12.4(15)T-12.4(22)T confirmed) and using PPTP with RADIUS Accounting in place.

Workaround: There is no workaround.

- CSCsy20008

  Symptoms: LDP/TDP configured on an ATM bundle interface does not work properly. There should be "Implicit-null" or "POP" labels assigned to a particular FEC (and that is also true for MPLS LDP bindings) but in the MPLS forwarding table the "Untagged" outgoing label is installed for that FEC.

  Conditions: The symptom is observed on an NPE-G2 that is running Cisco IOS Release 12.4(15)T8.

  Workaround: Use Cisco IOS Release 12.4(15)T5.

- CSCsy22311

  Symptoms: Using secure copy (SCP) between Cisco routers may cause compatibility issues.

  Conditions: Occurs when using SCP SSH version 2 between a Cisco 1800 and Cisco 2800.

  Workaround: There is no workaround.

- CSCsy31552

  Symptoms: A Cisco 1841 router equipped with xDSL WIC will suddenly stop forwarding packets. The packets will appear as output drops on the ATM interface statistics. Under the PVC level, there are no drops. The DSL line is not flapping but the ATM interface(s) report output drops.

  Conditions: The symptom is observed when using a Cisco 1800 and 2800 series router equipped with the same ADSL-WIC module. The ATM interface(s) need to be bridge-group configured. The bridge-group is in forwarding mode.

  Workaround: Reload the router.

- CSCsy32904

  Symptoms: T.38 fax calls may not work with some third-party devices.

  Conditions: The symptom can be observed in Cisco IOS Release 12.4(15)T and onwards.

  Workaround: From Cisco IOS Release 12.4(20)T and onwards, SIP Profiles can be used to remove the a-line in the SDP body.

  Further Problem Description: SIP T.38 fax gateway, when receiving fax call, may fail to negotiate T38FaxFillBitRemoval, T38FaxTranscodingMMR and T38FaxTranscodingJBIG attributes in the SDP response from the sending gateway.

  The gateway indicates to the remote side that it does not support turning on T38FaxFillBitRemoval capability using the "a=T38FaxFillBitRemoval:0" attribute in the outgoing OFFER and if the T38FaxFillBitRemoval capability is not present in the OFFER, the ANSWER should not turn on that capability. But in the case of some third-party endpoints, the remote endpoint may turn on T38FaxFillBitRemoval capability in ANSWER since the remote endpoint misunderstands the "a=T38FaxFillBitRemoval:0" as T38FaxFillBitRemoval capability supported by the gateway. (It goes by the new representation of inclusion = true, exclusion = false.) It is a similar case for the other two attributes.

- CSCsy39667

  Symptoms: On a PPP aggregator using dhcp-proxy-client functionality, in a situation where a PPP client session is torn down and then renegotiated within 5 seconds, the DHCP proxy client may send a DHCP RELEASE for the previous DHCP handle after the new DHCP handle (created as a result of new IPCP CONFREQ Address 0.0.0.0) has accepted the same IP address allocation from the offnet DHCP Server. This results in the offnet DHCP server having no record of the lease as it exists on the PPP aggregator which causes future addressing conflicts.

Conditions: The symptom is observed on a Cisco 7200 (NPE-400) and 7200 (NPE-G2) that is running Cisco IOS Release 12.4 T, or 12.2 SB.

Workaround:

1. Automated: Write a script to compare active leases on the PPP aggregator to active leases on DHCP server. If a lease is found to only exist on the PPP aggregator, use **clear interface virtual-access** to recover.
2. Manual: use the command **clear interface virtual-access**.

Further Problem Description: This issue occurs because the DHCP client holdtime is static at 5 seconds and there are no IOS hooks to tie PPP LCP session removal and IPAM to suppress stale DHCPRELEASES waiting in queue for HOLDTIME to expire.

- CSCsy40745

  Symptoms: After disabling SSH, an alternate SSH port is still enabled on the router.

  Conditions: Occurs on routers that have been configured to use a port other than Port 22 for SSH.

  Workaround: Do not configure alternate SSH ports.

- CSCsy43875

  Symptoms: A system may crash due to “Watchdog Time Expired” errors during normal operation without generating a crashinfo file or error messages prior to the crash.

  Conditions: The symptom is observed when any code tries to generate traceback via trace_caller. It is more likely to occur if BFD is configured.

  Workaround: There is no workaround.

- CSCsy45371

  Symptoms: The **clear ip nat tr *** command removes corresponding static NAT entries from the running configuration, but removing static NAT running configuration does not remove the corresponding NAT cache.

  Conditions: Occurs when NAT commands are entered while router is processing around 1 Mb/s NAT traffic.

  Workaround: Stop the network traffic while configuring NAT.

- CSCsy45838

  Symptoms: The **show ip ospf border-router** may cause a router to crash.

  Conditions: Occurs if the border table is recalculated in a significant way while the output is being printed on the console. The risk of a crash is reduced if you avoid using the auto-more feature and allow the entire output to display at once.

  Workaround: There is no workaround.

- CSCsy46007

  Symptoms: EzVPN tunnel will not come up after a reload. EzVPN is trying to connect to the peer with outside interface IP address to be “NULL”. The below debug message will be seen if “debug crypto isakmp” is enabled:

  ```
  EX: "ISAKMP:(0):receive null address from sa_req (local 0.0.0.0, remote 192.168.76.40)
  ```

  Conditions:

  1. EzVPN is in connect acl or auto mode
  2. Outside interface is configured on dialer interface.

3. This issue is seen only when EzVPN is trying to ask the dialer to kick start and dialer is not yet ready or dialer has not yet assigned the IP address to the interface.

Workaround: There is no workaround.

- CSCsy48838

  Symptoms: A router may crash with the following (or similar) message:

  ```
  %ALIGN-1-FATAL: Corrupted program counter
  ```

  Conditions: The symptom is observed when IOS firewall/ip inspect on H323 traffic is configured ("ip inspect name MY_INSPECT h323").

  Workaround: Do not inspect H323.

- CSCsy55821

  Symptoms: With a VTI tunnel between a Cisco ASR 1000 and another device (non-ASR), the VPN peer of a Cisco ASR 1000 is reporting packets with an invalid SPI.

  Conditions: The symptom is observed in the following scenario:

  – LAN-to-LAN VPN with VTIs.

  – One VPN end point is a Cisco ASR 1002 (RP1) that is running Cisco IOS Release 12.2(33)XNC.

  – The other VPN end point is a Cisco 7206VXR (NPE-G1) that is running Cisco IOS Release 12.4(15)T1 initially, then is upgraded to Cisco IOS Release 12.4(22)T and NPE-G2 plus VSA.

  Workaround: There is no workaround.

  Further Problem Description: At rekey, the Cisco ASR 1000 is sending delete-notify to the Cisco 7200 series router but still keeps using the old SA to encrypt, causing the drops.

- CSCsy56016

  Symptoms: BERT errors and jitter buffer errors reported on AS5xxx when using the **show tech** command.

  Conditions: The symptom is observed on the gateway when the commands **show tech** or **show as5400** are executed.

  Workaround: There is no workaround.

- CSCsy57750

  Symptoms: IPIPGW reloads while making an RSVP-enabled voice call with media statistics configuration.

  Conditions: The symptom is observed with Cisco IOS 12.4(24.6)T2 image.

  Workaround: There is no workaround.

- CSCsy69681

  Symptoms: Policy-based routing (PBR) fails to resolve next-hop.

  Conditions: Occurs when PBR is configured on a Cisco 871 to forward traffic to a DHCP-enabled interface.

  Workaround: There is no workaround.

- CSCsy74329

  Symptoms: The following message appears on the console:

```
[crypto_bitvect_alloc]: bitvect full (size = 8192)
-Traceback= 0x4244AB0 0x426875C 0x426AE60 0x426B330 0x426FAF4 0x4292B7C 0x4293278
0x75429C
```

Conditions: The symptom is observed when the GetVPN rekey is used with a number of Deny ACL entries and with VSA.

Workaround: There is no workaround.

- CSCsy77191

  Symptoms: Native GigE interfaces of a Cisco 7200 NPE-G2 router will not acknowledge reception of pause frames and will not stop its transmission in case of media-type RJ45.

  Conditions: The symptom is observed with media-type RJ45 and with SFP with “no neg auto” configured.

  Workaround: There is no workaround.

  Further Problem Description: There are no issues with SFP with a “neg auto” configuration.

- CSCsy79301

  Symptoms: A router crashes when a multicast group address joins and leaves the MLD group from the client within the configured delay time.

  Conditions: The symptom is observed when applying MLD leave for the group for which accounting has not yet started.

  Workaround: There is no workaround.

- CSCsy79955

  Symptoms: Reverse SSH using PVDM2 modems fails. If the **ssh -l** *username:line #* **ip** command is entered, modem activation is triggered. The input of “atdt *number*” is making it to the modem, meaning whatever the *number* field is typed, it is reported in the debugs. However, the modem does not send anything back to router about it and no connection is made. At modem prompt, “at”, “at&f”, “ate1” (and perhaps others) do not appear to be taken.

  Conditions: Seen on routers running Cisco IOS Release 12.4(22)T and 12.4(23). Appears to be issue with all releases. Issue is seen when using both **ssh -l** *username:line* **# ip** and by using SSH from a client to a particular line.

  Workaround: There is no workaround.

- CSCsy81339

  Symptoms: A Cisco router may unexpected reload due to a Bus error exception.

  Conditions: The reload happens when a QoS configuration change is made while a packet is in the middle of being processed on the interface the QoS is applied.

  Workaround:

  1. Shutdown the interface before making any QoS config changes
  2. Remove the service policy from the interface while making the configuration change.

- CSCsy84229

  Symptoms: When an HTTP request with payload of greater than 10MB is sent to the HTTP server of the router, the server is not able to process the request and responds back with the message “request entity too large”.

  Conditions: The symptom is observed with Cisco IOS Releases 12.4(22)T and 12.4(24)T and when the payload is above 10MB

  Workaround: Updating the signatures from S385 is a potential workaround.

Further Problem Description: This behavior is only evident while applying S386 and above on devices that do not have any previous signature package. This error does not appear while updating signature from S385 to S386.

- CSCsy87674

  Symptoms: Calls via an MGCP gateway that is registered to a Cisco Unified Communications Manager (CUCM) fail immediately with a codec negotiation error.

  Conditions: This symptom is observed when a CUCM is configured to use the G729 codec for the MGCP gateway.

  Workaround: Use the G729 AnnexB codec between the MGCP gateway and the CUCM.

- CSCsy90542

  Symptoms: Multicast traffic is dropped at decrypting side.

  Conditions: This symptom occurs when traffic ACL on the KS is of the type:

  ```
  permit ip host address any
  permit ip any host address
  ```

  Workaround: There is no workaround.

- CSCsy91748

  Symptoms: An NM-CEM-4SER module crashes.

  Conditions: The symptom is observed with an NM-CEM-4SER module when its payload size is changed on a CEM port which is part of a multiplexed group that is created using the **attach <port>** command.

  Workaround: Reload the router after using the **write config** command.

- CSCsy97506

  Symptoms:

  Case 1: All NAT multicast data packets are processed by software.

  Case 2. Spurious memory access occurs.

  Conditions:

  Case 1. NAT with static port entry, or dynamic overload configuration.

  Case 2. Configure **ip nat dynamic nat** rule with an undefined NAT pool.

  Workaround:

  Case 1: Configure NAT as static entry without port, or dynamic non-overload.

  Case 2: Configure with defined pool.

- CSCsz02000

  Symptoms: Router reloads at “atm_update_bundle_counters”.

  Conditions: Occurs during normal operation.

  Workaround: There is no workaround.

- CSCsz13123

  Symptoms: Frame-relay DLCI is not released from interface in a certain configuration sequence.

  Conditions: The symptom is observed on a Cisco router that is running Cisco IOS 12.4T images.

  Workaround: There is no workaround.

- CSCsz14236

  Symptoms: LLC stops forwarding I frames, but continues to respond to poll frames.

  Conditions: The symptom is detected when the output from **show llc** shows that frames are queued up for transmission in the Tx Queue. If DLSw is transporting the LLC frames, the associated DLSw circuit will show that the link is in a max congestion state.

  Workaround: There is no workaround.

- CSCsz20496

  Symptoms: A Cisco VG224 voice gateway displays the wrong secondary dialtone to the customer if “cptone CN” is configured under the voice-port.

  Conditions: The symptom is observed with Cisco IOS Releases 12.4(24)T, 12.4(20)T1, and 12.4(9)T7.

  Workaround: Upgrade to the latest IOS version (see bug CSCsk28301) and change the dial_tone2 to make it same as the dialtone by using the command **test voice tone cn 2nd_dialtone**:

```
event manager applet setCNsecondDialtone
    event syslog occurs 1 pattern ".*%SYS-5-RESTART: System restarted --.*"
    action 1.0 syslog msg "Setting DIAL_TONE2 for cptone CN"
    action 2.0 cli command "enable"
    action 3.0 cli command "test voice tone CN 2nd_dialtone 1 450 0 -100 -100
 -100 0 0 0 0xFFFF 0 0 0 0 0 0 0"
    action 4.0 syslog msg "DIAL_TONE2 for cptone CN has been set"
```

  Copy the script to the running-configuration and then save it to NVRAM. If the router reloads, the setting “test voice tone CN 2nd_dialtone 1 450 0 -100 -100 -100 0 0 0 0xFFFF 0 0 0 0 0 0 0” will automatically be re-asserted. If you want the command set immediately without a reload then cut and paste the command directly at the EXEC prompt.

- CSCsz23976

  Symptoms: A Cisco 7200 series router that is running Cisco IOS Release 12.4(15)T7 may experience an unexpected reset while forwarding traffic with a Cisco 7200 VSA.

  Conditions: The symptom is observed on a Cisco 7200 series router running with a Cisco 7200 VSA installed on Cisco IOS 12.4(15)T code.

  Workaround: There is no workaround.

- CSCsz29815

  Symptoms: TTY sessions not accessible after reverse SSH session to the same TTY port results in failed authentication.

  Conditions: Occurred on a router running Cisco IOS Release 12.4(24)T and configured with TTY lines accessed using reverse SSH Version 2. Issue also affects SSH version 1 and affects VTY lines.

  Workaround: Reload the router.

- CSCsz31940

  Symptoms: Active secure NAT (SNAT) continuously prints the following tracebacks and the router is not operational while tracebacks are printed:

```
%SYS-2-INSCHED: suspend within scheduler
-Process= "<interrupt level>", ipl= 1,
-Traceback= 0x41732A78 0x4009B8AC 0x42DF1EC8 0x41F780E4 0x41F9E790 0x41F53274
0x41F7D830 0x400ECDD8 0x40069574 0x439BE7A8 0x439BC010 0x40047734 0x4000FCC0
```

  Conditions: The symptom is observed when flow switching and SNAT are configured on the router interface and SNAT traffic passes through the router.

  Workaround: Stop the SNAT traffic and wait for the tracebacks to clear.

- CSCsz34920

  Symptoms: Router continuously reboots.

  Conditions: The symptom is observed when an NME-502 is installed in the router.

  Workaround: Replace or take out the NME-502.

- CSCsz38104

  The H.323 implementation in Cisco IOS Software contains a vulnerability that can be exploited remotely to cause a device that is running Cisco IOS Software to reload. Cisco has released free software updates that address this vulnerability. There are no workarounds to mitigate the vulnerability apart from disabling H.323 if the device that is running Cisco IOS Software does not need to run H.323 for VoIP services. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-h323.shtml.

- CSCsz45419

  Symptoms: WORD option is not seen in some of the NTPv4 commands. Some NTP commands are not working properly.

  Conditions: This happens on a Cisco router running an internal build of Cisco IOS Release 12.4T.

  Workaround: There is no workaround.

- CSCsz45539

  Symptoms: Unable to attach the frame relay DLCI to the serial subinterface. The following error is received:

  ```
  %PVC already assigned to interface Serial3/0
  ```
  Conditions: The symptom occurs with a Cisco 7200 series router that is running Cisco IOS Release 12.4(24)T.

  Workaround: There is no workaround.

- CSCsz45567

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

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

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

  Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are available.

  This advisory is posted at:

  http://www.cisco.com/warp/public/707/cisco-sa-20100324-ldp.shtml

- CSCsz49741

  Devices running Cisco IOS Software and configured for Cisco Unified Communications Manager Express (CME) or Cisco Unified Survivable Remote Site Telephony (SRST) operation are affected by two denial of service vulnerabilities that may result in a device reload if successfully exploited. The vulnerabilities are triggered when the Cisco IOS device processes specific, malformed Skinny Call Control Protocol (SCCP) messages.

  Cisco has released free software updates that address these vulnerabilities.

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

- CSCsz50423

  Symptoms: The **clear interface atm5/ima** command makes the ATM PVC inactive.

  Conditions: Occurs on a Cisco 7200 router running Cisco IOS Release 12.4(24.6)T8.

  Workaround: There is no workaround.

- CSCsz52815

  Symptoms: If number of hours for statistics is increased to 10 or more after the probe is initially run and then restarted, system crashes with memory corruption

  Conditions: Occurs when the probe is started with the hours of statistics less than 10 and then re-started with the hours of statistics greater than 9.

  Workaround: There is no workaround.

- CSCsz53177

  Symptoms: When running Network Load-balancing (IGMP-mode) in VLANs with PIM enabled and static ARP entries for unicast IP to layer-2 multicast address, packet duplication will occur.

  Conditions: This symptom occurs when sending unicast (non-multicast) IP packets with multicast layer-2 destinations.

  Workaround: Use non-IGMP NLB modes (unicast or multicast with static macs) or use IGMP snooping querier instead of PIM on NLB SVIs.

- CSCsz55055

  Symptoms: Attaching or removing a service policy flaps the Gigabit Ethernet interface.

  Conditions: This symptom is observed only with a Cisco 3845 NM-1GE.

  Workaround: There is no workaround.

- CSCsz56169

  Symptoms: A software-forced crash occurs after a **show user** command is performed.

  Conditions: The crash occurs after the user performs a **show user** command and then presses the key for next page. It is observed on a Cisco 3845 that is running Cisco IOS Release 12.4(21a).

  Workaround: Do not perform a **show user** command.

- CSCsz56382

  Symptoms: The Tunnel0 interface used on a DMVPN hub is reporting “Tunnel0 is reset, line protocol is down” or no traffic is passing through this interface anymore.

  The IKE and IPSec SAs may still be up, but only the decaps counters will be seen increasing, not the encaps counters.

  Conditions: This symptom is observed on Cisco 2821 routers that are running Cisco IOS Releases 12.4(9)T7 or 12.4(15)T9. Other platforms and releases may be affected.

  Workaround: Shutdown Tunnel0 and create interface Tunnel1 with the same configuration instead, if you cannot reload the router.

  Otherwise reloading the router will resolve the issue. Do not configure another identical Tunnel interface in this case or you will run into CSCsl87438. If you reload the router at a later time, be sure to remove the duplicate Tunnel interface prior to the reboot.

- CSCsz60659

  Symptoms: The cooperative GDOI keyserver starts printing %GDOI-5-COOP_KS_REACH and/or %GDOI-5-COOP_KS_UNREACH syslog messages.

Conditions: The symptom is observed if two or more ISAKMP connection attempts fail, which might be normal in production networks.

Workaround: There is no workaround.

Further Problem Description: In fixed versions, the logic of the reachability test was changed to avoid this problem.

- CSCsz63721

  Symptoms: CPU utilization goes to 90% or above when PfR is configured with a large number of policy using fastmode and forced target.

  Conditions: The problem is limited to a large number of forced target (greater than 500) and fastmode with probe frequency of 2-5 seconds. CPU usage progressively gets worse with the increase in number.

  Workaround: Use longest-match targets instead of forced targets. Forced targets are configured under oer-map, and longest-match targets are configured under OER master. Forced targets are required only if the target does not belong to the destination subnet of the traffic-class being optimized.

- CSCsz71392

  Symptoms: WCCP stops functioning when GDOI SA is accelerated by VSA.

  Conditions: The symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 12.4(24)T with VSA (FPD 0.23). It is seen when **ip wccp** *61* **redirect out** and **ip wccp** *62* **redirect in** are applied to the inside interface, and traffic gets WCCP GRE redirected to WAE. When GDOI crypto-map (currently in inbound-only state) is applied to the outside interface, traffic is returned from WAE via WCCP and GRE gets dropped within UUT.

  Workaround: Disabling VSA with **no crypto engine slot 0** restores connectivity to normal.

- CSCsz75186

  Cisco IOS Software is affected by a denial of service vulnerability that may allow a remote unauthenticated attacker to cause an affected device to reload or hang. The vulnerability may be triggered by a TCP segment containing crafted TCP options that is received during the TCP session establishment phase. In addition to specific, crafted TCP options, the device must have a special configuration to be affected by this vulnerability.

  Cisco has released free software updates that address this vulnerability.

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

- CSCsz79001

  Symptoms: A Cisco 87x router may hang or crash after displaying “Now reloading” during ROMmon upgrade when using the **upgrade rom-monitor file flash:** command.

  Conditions: This occurs when a router running ROMmon release 12.3(8r)YI4 or an older ROMmon from alternate space is upgraded to YI5 or a newer ROMmon version

  Workaround: Powercycle the router to recover from this hang state. The router will then boot with the upgraded ROMmon.

- CSCsz92368

  Symptoms: Occasionally, the following log warning is observed when **no mpls ip** is configured on the last MPLS interface on the router:

  ```
  %MDEBUG-2-ACCESSFREED:
  ```

  Conditions: The symptom is observed when the MDEBUG in ROMmon mode has been activated with ROMmon commands:

```
MDEBUG_OPTIONS=0x3 MDEBUG_ENTRIES=49152
```
Workaround: There is no workaround.

- CSCsz92463

  Symptoms: GetVPN Key Servers no longer function in cooperative mode. The Key Servers (KSs) will fail to communicate with each other, and each will assume it is the primary. GMs registering to different KSs will not be able to communicate with GMs registered to a different KS.

  Conditions: This symptom occurs when using GetVPN Key Servers in cooperative mode.

  Workaround: There is no workaround.

- CSCsz92924

  Symptoms: CPU HOG in Crypto ACL is seen on the GM. The GM may crash some milliseconds later after printing the hog.

  Conditions: This symptom is observed on a large ACL on the KS (greater than 70 lines) with or without large ACL locally on the GM.

  Workaround: Limit the ACL length drastically.

- CSCsz93207

  Symptoms: In an EZVPN scenario, the traffic to the internet is not getting NATed.

  Conditions: The symptom is observed in an EZVPN scenario with “identical addressing” and “split tunnel” configured.

  Workaround: Use Cisco IOS Release 12.4(15)T3.

- CSCsz96323

  Symptoms: A Cisco 7301 router crashes with “protocol pptp” configured.

  Conditions: The symptom is observed with a Cisco 7301 router when “protocol pptp” is configured.

  Workaround: There is no workaround.

- CSCta00794

  Symptoms: %SYS-3-CPUHOG is seen when multicast fanout performance test is executed with a large number of IGMP or PIM joins and forwarding out through a large number of OIF (1000 sub-interfaces).

  Conditions: Observed on a Cisco 7200 router running Cisco IOS Release 12.4(24.06)T9.

  Workaround: There is no workaround.

- CSCta02089

  Symptoms: There is a crash on a Cisco AS5400 due to CPU signal 10.

  Conditions: The symptom is observed on a Cisco router due to expiration of freed receive_digit timer in SIP

  Workaround: There is no workaround.

- CSCta02460

  Symptoms: On a router that has a PRI trunk towards the PSTN, you may hear dead air when calling any ISDN device that returns cause code 0x8484 in a PROGRESS message that also contains a progress_ind with value 8.

  Conditions: The symptom is seen when using the primary-4ess (PRI 4ESS) and primary-5ess (PRI 5ESS) switch type.

  Workaround: There is no workaround.

Further Problem Description: The problem was discovered when a user attempted to call a cell phone on a wireless network that was switched off. The user did not have voicemail, and the wireless network played a message in the band to alert that the phone was off. It is this message that should be heard - but it is not, due to this bug.

The issue is due to an invalid cause value sent from the provider for an outgoing to call to a mobile phone which is switched off. The cause value of 4 is not supported by PRI 4ESS switches. Hence ISDN will send a STATUS message reporting invalid information element contents and the provider disconnects the call.

- CSCta04123

  Symptoms: A router may crash with a "STACKLOW" message or memory corruption.

  Conditions: The symptom is observed when the router is configured for IP inspect (only a basic IP inspect configuration is necessary).

  Workaround: Disable IP inspect.

- CSCta05809

  Symptoms: A group member on a GETVPN network may stop passing encrypted traffic.

  Conditions: A GETVPN group member (GM) may accept and process an old or duplicate rekey message from the designated key server (KS). If the rekey message includes a TEK which was previously used to encrypt data, but which has already expired, the GM may become unable to send and receive encrypted traffic.

  Workaround: There is no workaround.

- CSCta12296

  Symptoms: Group member router crashes.

  Conditions: Occurs when unicast re-keys are received frequently (TEK 300).

  Workaround: There is no workaround.

- CSCta45116

  Symptoms: EAP-FAST authentication fails between router and client (PC or laptop running ADU).

  Conditions: The symptom is observed when the wireless client is running "ADUv2.x" and the router is running with Cisco IOS Release 12.4(15)T8.

  Workaround: Upgrade the wireless client ADU to version 3.x or 4.x.

- CSCta45845

  Symptoms: All show commands under crypto are showing blank outputs. For example **show crypto pki certificates** shows a blank output, even though there may be some crypto certificates on the device.

  Conditions: This happens only when using web interface to an IOS device. The commands are:

```
7200-12-3#sh crypto pki  ?
   certificates  Show certificates
   counters      Show PKI Counters
   crls          Show Certificate Revocation Lists
   server        Show Certificate Server
   session       Show PKI Session Data
   timers        Show PKI Timers
   token         Show PKI Token(s)
   trustpoints   Show trustpoints
```

  Workaround: There is no workaround.

Further Problem Description: CCA uses HTTP(s) service to get the output. Even when the certificate is shown using telnet/SSH, CCA GUI shows as unconfigured.

- CSCta46486

  Symptoms: CPU hogging in IKE and traceback seen on headend router terminating large amount of DVTIs.

  Conditions: The symptom is observed with any kind of outage on the remote site or clearing large amount of tunnels with the headend router actively participating in the routing and re-distributing the routes learned via the tunnel to the central site.

  Workaround: There is no workaround.

- CSCta65793

  Symptoms: Router crashes while configuring “no auto-summary” in EIGRP at startup.

  Conditions: The symptom is observed on a Cisco 7200 series router that is running Cisco IOS 12.4M and 12.4T images.

  Workaround: As the router processes the auto-summary command prior to any interfaces participating in EIGRP becoming fully established, the workaround is to defer configuring the auto-summary command until after interfaces have been fully enabled and are participating in EIGRP.

- CSCta69118

  Symptoms: The ping from CE1 to CE2 fails when VLAN xconnect is provisioned, even though the session is up.

  Conditions: The symptom is observed with Cisco IOS Release 12.4(20)T4.

  Workaround: There is no workaround.

- CSCta75271

  Symptoms: When we change a policy-map from a pure precedence policy (only match precedence classes) to a pure DSCP policy (only match DSCP classes), it causes a crash.

  Conditions: When we remove the last precedence/DSCP class from a pure policy and replace it with DSCP/QoS_group, it causes a crash. Occurs in Cisco IOS Release 12.4(20)T and 12.4(24)T throttles.

  Workaround: Remove the service-policy from the interface, then make the change to the policy-map and reapply the service-policy on the interface again.

- CSCta75923

  Symptoms: One-way voice may occur after a transfer through a CMM transcoder if the stream goes through an RTP-aware firewall such as an ASA. The transcoder in some transfer situations will reuse a previous SSRC, which causes a security violation.

  Conditions: In a situation where there are 3 SSRCs in a single transfer, the outgoing stream from the transcoder will reuse the first SSRC in place of the third SSRC. This is against the RTP RFC, and some firewalls may drop the packet. Some gateways and endpoints may also not correctly process the packets, depending on the strictness of the RFC implemented.

  Workaround: It was found that some endpoints, like the Cisco Unified IP Phone 7960, activated a transfer with only 2 SSRC changes. It was also found that a Cisco Unified IP Phone 7941 with firmware 8-3-2 had the problem, but the latest 8-4-X image did not. Some endpoints, such as an autoattendant, do not have the ability to change this behavior. The only other workaround is to use a different type of transcoder than the ACT CMM.

- CSCta77552

  Symptoms: A Cisco 5850 crashed 2 minutes after the card in slot 5 crashed.

  Conditions: This symptom was observed on a Cisco 5850 with Cisco IOS Release 12.4(25).

  Workaround: There is no workaround.

- CSCta77678

  Symptoms: RTP timestamp on the RFC 2833 event is modified. IP Phones are using RFC2833 to transport the DTMF signals, which causes problems with the Voicemail systems.

  Conditions: This symptom occurs when RTP header compression is enabled.

  Workaround: There is no workaround.

  Further Problem Description: The problem disappears if cRTP is disabled. The issue is seen with Class-Based cRTP configured and also with other cRTP configuration types.

- CSCta79634

  Symptoms: System crash in L2TP. Following this, most of the L2TP setups fail.

  Conditions: The symptom occurs at an L2TP control-plane event.

  Workaround: Clear VPDN again or reload the router.

- CSCta87146

  Symptoms: There are no flows in the netflow cache when PFR is enabled.

  Conditions: The symptom is observed when PFR is enabled.

  Workaround: Disable PFR.

- CSCta91556

  Symptoms: Packets are getting SSS switched on the LAC towards LNS.

  Conditions: The symptom is observed when bringing up any PPPoE or PPPoA session.

  Workaround: There is no workaround.

- CSCtb13396

  Symptoms: Active probes are not running, and traffic class/prefixes are uncontrolled.

  Conditions: This symptom is observed when changing policy-rules to a different prefix-list name or changing a prefix-list (adding a new sequence to the prefix-list).

  Workaround: Delete and paste back OER master configuration before active probes run.

  Or, shut oer-master, delete “match traffic-class prefix-list”, no shut the oer master, and then add back “match traffic-class prefix-list” will make the PfR work again.

- CSCtb13546

  Symptoms: A Cisco IOS router crashes with a bus error.

  Conditions: This symptom occurs when a Cisco IOS router is performing multihop VPDN (a.k.a. tunnel switching). The router may infrequently crash due to a bus error.

  This crash is limited to cases where at least one of the following VPDN group commands are configured:

  ```
  ip pmtu
  ip tos reflect
  ```

  Workaround: Disable the above mentioned commands. However the consequences of this on user traffic must be evaluated first.

- CSCtb14400

  Symptoms: Packets received from the virtual-access CE-facing interface are not CEF-switched into the MPLS cloud.

  Conditions: The symptom is observed on a MPLS/VPN PE router.

  Workaround: There is no workaround.

- CSCtb26955

  Symptoms: The following error message is seen:

  ```
  %CRYPTO-4-GM_REGSTER_IF_DOWN: Can't start GDOI registration as interface
  FastEthernet1.2 is down
  ```
  Problem: The interface is not actually down. The registration should go through.

  Conditions:

  1. Manually clear the rekey SA (**clear cry isakmp** *connid*).
  2. Wait for the re-registration to start.

  Workaround: Use the **clear cry gdoi** *group* command or remove and add the crytpo map. The manual deleting of rekey SAs is not a valid option.

  Further Problem Description: An incomplete check in the code interprets this as "the associated interface is down". The registration fails with the GM_REGSTER_IF_DOWN error message.

- CSCtb29256

  Symptoms: A router crashes after entering the **sh isdn history** command.

  Conditions: This issue has been seen in a Cisco 7206VXR (NPE-G2) that is running Cisco IOS Release 12.4(15)T9.

  Workaround: Avoid using the **sh isdn history** command and use the **sh isdn active** command.

- CSCtb34920

  Symptoms: Calls may intermittently be dropped or disconnected.

  The debug output for "debug isdn q931" will reveal that the gateway is sending a Q.931 INFORMATION message similar to the following:

  ```
  Aug 11 13:51:20.137 EST: ISDN Se0/2/1:23 Q931: TX -> INFORMATION pd = 8 callref =
  0x80AE
  ```
  The connected service provider switch may respond with a Q.931 STATUS message similar to the following:

  ```
  Aug 11 13:51:20.197 EST: ISDN Se0/2/1:23 Q931: RX <- STATUS pd = 8 callref = 0x00AE
  Cause i = 0x81E17B - Message type not implemented Call State i = 0x0A
  ```
  The connected service provider switch may also respond with a Q.931 DISCONNECT message similar to the following:

  ```
  Aug 11 13:51:20.297 EST: ISDN Se0/2/1:23 Q931: RX <- DISCONNECT pd = 8 callref =
  0x00AE Cause i = 0x81E4 - Invalid information element contents
  ```
  Conditions: This problem may occur when an ISDN PRI is configured to use "switch-type primary-4ess" or "switch-type primary-5ess."

  This problem may occur when an IP phone user blind transfers a call to another destination (another IP phone, IVR, IPCC queue, etc.). The transfer request triggers the Cisco Unified Communications Manager (CUCM) server to send an H.225 INFORMATION message with a Signal IE to the Cisco IOS H.323 gateway indicating to start/stop playing ringback tone toward the PSTN. The Cisco IOS H.323 gateway should generate the ringback tone, but it should NOT send the Q.931 INFORMATION message toward the connected service provider switch.

The 4ess spec indicates that the INFORMATION message is NOT supported per AT&T TR 41459 section 3.1.8. Also the Lucent AT&T 235-900-342 5ess spec does not even mention the INFORMATION message in section 4.2 which covers all other supported Q.931 message types.

Workaround: Another similar defect CSCsr38561 was previously opened for this same type of problem with "switch-type primary-ni" and has now been resolved.

If you are running a version of Cisco IOS, which has the fix for CSCsr3856, it "may" be possible to reconfigure the Cisco IOS gateway user side of the PRI to use "switch-type primary-ni" even though the connected service provider switch may be provisioned for 4ess or 5ess. This should only be used as a temporary workaround because it could expose other interworking errors due to switch-type mismatch configuration.

- CSCtb68229

  Symptoms: The box crashes within "cns config notify code".

  Conditions: This symptom is observed in the corner case when someone removes "cns config notify diff" from the config while adding other CLIs to the running config by using the method "config replace". The box can crash.

  Workaround: Do not remove "cns config notify diff" using "config replace".

Resolved Caveats—Cisco IOS Release 12.4(15)T9

Cisco IOS Release 12.4(15)T9 is a rebuild release for Cisco IOS Release 12.4(15)T. The caveats in this section are resolved in Cisco IOS Release 12.4(15)T9 but may be open in previous Cisco IOS releases.

- CSCeg87070

  Symptoms: A Cisco 10000 crashes at igmp-process:

  ```
  Cisco IOS Software, 10000 Software (C10K2-P11-M), Version 12.3(7)XI2b, RELEASE
  SOFTWARE (fc1) Technical Support: http://www.cisco.com/techsupport Copyright (c)
  1986-2005 by Cisco Systems, Inc. Compiled Sat 08-Jan-05 16:25 by <software engineer>
  ROM: System Bootstrap, Version 12.0(20020314:211744) [REL-pulsar_sx.ios- rommon 112],
  DEVELOPMENT SOFTWARE
  r-pa068 uptime is 19 hours, 58 minutes System returned to ROM by RPR switchover at
  19:03:47 MET Mon Jan 24 2005 System restarted at 19:07:22 MET Mon Jan 24 2005 System
  image file is "disk0:c10k2-p11-mz.123-7.XI2b"
  ```

  Conditions: This symptom is observed during 7xi2b monitoring.

  Workaround: There is no workaround.

- CSCek32744

  Symptoms: The vlan-id is not propagated in the NAS Port ID field when the PPPoE over VLAN call is up.

  Conditions: The symptom is observed when using both configurations (main interface and sub-interface) for PPPoE over VLAN. The NAS Port ID value shows correctly while using the sub-interface configuration but incorrectly when using the main interface. The main interface used for PPPoE over VLAN is shown below:

  ```
  interface Ethernet1/0
   no ip address
   vlan-id dot1q 4
    pppoe enable group global
    exit-vlan-config
  ```

  The expected NAS Port ID is 1/0/0/4 but 1/0/0/0 is received.

Workaround: There is no workaround.

Further Problem Description: This will impact AAA as this information should be updated by PPP to AAA.

- CSCsc78999

  Symptoms: An Address Error exception occurs after Uninitialized timer in TPLUS process.

  Conditions: This is a platform independent (AAA) issue. It may be seen with a large number of sessions while accounting is configured with a T+ server.

  Workaround: Disable accounting, or use RADIUS accounting instead of a T+ server.

- CSCsg84765

  Symptoms: A MWAM-SSG processor may reload automatically with the following error message:

  ```
  %ALIGN-1-FATAL: Corrupted program counter pc=0x0 , ra=0x21A8C118 , sp=0x45E7D7D0
  ```

  Conditions: The symptom is observed with MWAM in a Cisco 7600 series router that is running Cisco IOS Release 12.4(3b).

  Workaround: There is no workaround.

- CSCsh52567

  Symptoms: A Cisco RSP720 crash is experienced when BGP is established over SPA-1XOC12-POS interface where the problem is seen in Cisco IOS Release 12.2(33) SRB2.

  Conditions: This symptom is observed when BGP speaker is originating a prefix with an outbound routemap having *routemap continue* keyword and **set as-path prepend** in the routemap policy, under certain corner conditions, the router may reload.

  Workaround: In the BGP route map policy, remove the routemap *continue* keyword and change the policy logic when it is used along with routemap CmdBold>set aspath prepend command. Note that once routemap *continue* is removed, please make sure that the polices are changed such that they are similar to the originally intended policy behavior.

- CSCsh69043

  Symptoms: The default MTU size on onboard Fast Ethernet interfaces is not sufficient to support Ethernet over MPLS. A larger MTU size is needed to support EoMPLS (untagged and tagged) without fragmentation at the higher layers.

  Conditions: End-to-end EoMPLS packets will not be exchanged with the default interface MTU. Pings fail.

  Workaround: There is no workaround.

  Further Problem Description: This defect is applicable only for Fast Ethernet interfaces. Gigabit Ethernet interfaces, by default, already support higher MTU sizes.

- CSCsi14180

  Symptoms: In rare instances, a router may reload when removing a VLAN configuration while also executing a **show vlans** command. Specifically, if a user connects to a router and executes a **show vlans** command, pausing the show command display using automore, and then removes the VLAN configuration using another EXEC command session, the router may reload when the **show vlans** command resumes.

  Conditions: This symptom is observed in Cisco IOS Release 12.4T.

  Workaround: Complete the **show vlans** output before deleting the VLAN configuration, or avoid multiple EXEC sessions to the same router when deleting the VLAN configuration.

- CSCsi43340

  Symptoms: DSMP is not programming the DSP for supervisory tone while alerting tone is there, which leads to FXO disconnect supervision issue.

  Conditions: Occurs on routers running Cisco IOS Release 12.3(14)T and later releases.

  Workaround: Downgrade to Cisco IOS Release 12.3(11)T.

- CSCsi99449

  Symptoms: A traceback is seen.

  Conditions: This symptom is observed when the WLAN feature of NAT is configured and when the host with the static IP address tries to contact any host connected to the outside interface of the NAT.

  Workaround: There is no workaround.

- CSCsj36031

  Symptoms: The configuration for “xconnect” may not be accepted.

  Conditions: Problem seen only when the existing “xconnect” configuration is removed from ATM PVC with “encap aal0” and then attached to the same ATM pvc.

  Workaround: Remove the ATM PVC and reconfigure again with aal0 encapsulation and “xconnect”.

- CSCsj54837

  Symptoms: A Cisco 7200 that is running Cisco IOS Release 12.4 or 12.4(11)T2 crashes with a TLB (store) exception.

  Conditions: This symptom is observed when Rate Based Satellite Control Protocol (RBSCP) tunneling is configured on the device.

  Workaround: There is no workaround.

- CSCsj62846

  Symptoms: A MIB walk of the udpTable will have extra bad entries when a UDP IPv6 connection to the device is made.

  Conditions: IPv6 must be configured, and an IPv6 UDP socket must be present.

  Workaround: There is no workaround. This defect should not interfere with normal device operation.

- CSCsj78403

  Symptoms: A router may crash when the **clear ip bgp** command is entered.

  Conditions: Occurs on devices running BGP and configured as a route reflector client with conditional route injection configured.

  Workaround: Unconfigure conditional route injection.

- CSCsj93465

  Symptoms: A PRE-3 may crash at the “pppatm_pas_fs” function.

  Conditions: This symptom is observed on a Cisco 10000 series that runs the c10k3-p11-mz image of Cisco IOS Release 12.2(31)SB1 and that is configured for PPP. The symptom occurs after a write operation. The symptom may not be platform-specific.

  Workaround: There is no workaround.

- CSCsk34641

  Symptoms: A router may exception while registering a corrupt eToken.

Conditions: This symptom is observed only when a particular corrupt eToken is inserted. This symptom has been observed only on a single eToken.

Workaround: Format the eToken.

- CSCsk34832

  Symptoms: Memory leaks out at about 10 to 15 percent overnight.

  Conditions: This symptom occurs when a mix of application traffic is sent to the HTTP Secure server and when CPU utilization is at about 30 percent.

  Workaround: There is no workaround.

- CSCsk45399

  Symptoms: A device might crash when the QoS configuration is changed.

  Conditions: This symptom is observed on a device that has a QoS configuration.

  Workaround: There is no workaround.

- CSCsl46159

  Symptoms: When the cost-minimization feature is used in OER, prefixes are moved to minimize the cost, but it never reaches a stable point. In other words, prefixes are moved back and forth periodically.

  Conditions: This symptom is observed only if OER cost-minimization is configured.

  Workaround: There is no workaround.

- CSCsm03452

  Symptoms: A Cisco AS5850 that is configured as a SIP gateway may crash unexpectedly when running a high volume of SIP calls.

  Conditions: This symptom is observed on the Cisco AS5850.

  Workaround: There is no workaround.

- CSCsm44620

  Symptoms: Multicast tunnel not coming up after RPM change. A misconfiguration with overlapping networks causes the join to be rejected. This can be seen on the PIM neighbor list.

  Conditions: There is a problem related to one of the hub card in rpm-xf.10 in forwarding PIM traffic from 2 PEs (rpm-xf.13 & rpm-xf.11). After RP migration from AVICI to CRS we found that tunnels from PE in slot 13 were not coming up. PE in slot 13 was in consistently in registering mode. PE was not coming out of registering mode which was preventing the tunnels from coming up. For PE to come out of registering mode S,G state should be built from new RP down to PE. At this stage the CRS (RP) showed that S,G tree was establish at the RP. S,G tree was OK all the way down from CRS to the last hop (P in slot 10) connecting to the slot 13 PE. The P router in slot 10, which is directly connected to PE, showed that S,G state was established and PE facing interface was in OIL. But there were couple of discrepancies on the P in slot 10. There were no flags set on this P for the mroute of PE. In addition, we found that PE was not receiving any PIM traffic from the P in slot 10. This led to suspicion that although the P showed the correct S,G and OIL but is still not able to forward traffic to the PE. And this could be the reason for PE to remain in registering mode hence preventing the tunnels from coming up.

  Workaround: Remove the following configurations:

  a. rpm-xfh10-z135 - Shut and remove interface Switch1.4073

  b. rpm-xfh09-z134 - Shut and remove interface Switch1.4073

  c. rpm-xfp11-l172 - Remove interface Switch1.3172

d. rpm-xfp13-z074 - Remove interface Switch1.4074

e. rpm-xfp04-l171 - Remove interface Switch1.3171

- CSCsm56940

  Symptoms: Traceback seen while doing Telnet with SSH enabled.

  Conditions: Occurs when SSH is enabled on a Cisco 7200 router.

  Workaround: There is no workaround.

- CSCsm87071

  Symptoms: A NAT pool cannot be deleted after traffic is stopped and NAT translations are cleared.

  Conditions: This symptom is observed when traffic is started and then stopped.

  Workaround: Reload the router.

- CSCsm87925

  Symptoms: Memory leak occurs in SSGCmdQue

  Conditions: Occurs on routers configured for Service Selection Gateway (SSG) and running Cisco IOS Release 12.4(15)T2.

  Workaround: There is no workaround.

- CSCsm99079

  Symptoms: The kron process may generate the following syslog and cause the device to reload:

  ```
  Dec 30 23:47:31.920: %SYS-3-CPUHOG: Task is running for (2004)msecs, more than
  (2000)msecs (1/0),process = Kron Process. -Traceback= 0x42725288 0x42725778 0x42724AC0
  0x41E0D72C 0x41E0E0BC 0x41E0E3FC
  ```

  Conditions: The symptom is observed when the command **kron** is configured with the *at* parameter.

  Workaround: Try redesigning the **kron** command to use the *in* parameter.

- CSCso21463

  Symptoms: A one-way voice issue is seen when making a transcoded transfer call with an H.323 endpoint.

  Conditions: A one-way voice issue is observed when DSP farm resources are controlled by CCM and the transcode profile has g711alaw and g729 codecs, but no g711ulaw, configured on the DSP farm router. The checkbox for MTP required is checked under the H.323 gateway configuration page.

  Workaround: Add g711ulaw in the transcode profile.

- CSCso32765

  Symptoms: Multicast Layer 2 set features are not working.

  Conditions: All Layer 2 set features are broken in the multicast switching path.

  Workaround: There is no workaround.

  Further Problem Description: The issue here is that all Layer 2 set features are broken in the multicast switching path. On analysis, it was found that the set functions to set the qos_flags to indicate that a specific L2 set feature needs to be executed are invoked, but the follow-on invocation to actually set the fields is missing.

- CSCso69413

  Symptoms: A Cisco router may reload when Flexible Packet Matching is configured.

Conditions: This symptom occurs when a class is configured to match on a protocol field when the protocol stack has not been defined. The stack class-map is required for all field references.

Workaround: Specify the exact bits to be matched with the **match start** command.

- CSCso90058

  Symptoms: 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.

- CSCsq29139

  Symptoms: When IPv6 prefix delegation receives periodic RENEW message from a client, it may incorrectly bind the corresponding prefix for another client.

  Conditions: The symptom is observed when IPv6 prefix delegation assigns a prefix to a client that is connected via a virtual access interface.

  Workaround: There is no workaround.

- CSCsq92019

  Symptoms: An SCCP phone cannot act as a conferencing controller.

  Conditions: This symptom is specific to a customer test setup where there is NAT back-to-back. NAT segmented code synchronization fails when NAT is back-to-back.

  Workaround: Configure the **no ip nat service skinny tcp port 2000** command.

- CSCsq93508

  Symptoms: When onboard hardware crypto is enabled and if an SSLVPN AnyConnect tunnel is brought up, tracebacks are continuously seen and no traffic will go through the tunnel.

  Conditions: The symptom is observed with hardware crypto enabled on a Cisco 1800 series router.

  Workaround: Enable software crypto.

  Further Problem Description: The issue is seen on an 1800 platform because other ISR routers do not handle SSL with a hardware engine; they use only software code for SSLVPN (even onboard crypto engine enabled).

- CSCsq98742

  Symptoms: Cisco AS5400 router crashes frequently with Cisco IOS Release 12.4 (19b) attempting to free memory for X28 component.

  Conditions: This symptom is observed on a Cisco AS5400.

  Workaround: There is no workaround.

- CSCsr16693

  A series of TCP packets may cause a denial of service (DoS) condition on Cisco IOS devices that are configured as Easy VPN servers with the Cisco Tunneling Control Protocol (cTCP) encapsulation feature. Cisco has released free software updates that address this vulnerability. No workarounds are available; however, the IPSec NAT traversal (NAT-T) feature can be used as an alternative.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090325-ctcp.shtml.

Note: The March 25, 2009, Cisco IOS Security Advisory bundled publication includes eight Security Advisories. All of the advisories address vulnerabilities in Cisco IOS Software. Each advisory lists the releases that correct the vulnerability or vulnerabilities in the advisory. The following table lists releases that correct all Cisco IOS Software vulnerabilities that have been published in Cisco Security Advisories on March 25, 2009, or earlier.

http://www.cisco.com/en/US/products/products_security_advisories_listing.html

- CSCsr17680

  Symptoms: AA-request, sent to a particular server, getting failed-over to all other servers in the server group, when the first server is not responding or first server is unreachable.

  Conditions: This issue is observed when sending request to particular server on a server-group.

  Workaround: There is no workaround.

- CSCsr23454

  Symptoms: A device reloads with a bus error and may display the following message:

  ```
  CMD: ' aggregate-address 224.0.0.0 224.0.0.0 attribute-map GCI-aggregations
  suppress-map Suppress-ESNAK' Address Error (load or instruction fetch) exception, CPU
  signal 10, PC = 0x60CDD444
  ```

  Conditions: The symptoms are observed on a device configured with Border Gateway Protocol (BGP).

  Workaround: There is no workaround.

- CSCsr25086

  Symptoms: A Cisco 7200 router might unexpectedly reload during normal working conditions.

  Conditions: This problem occurs on Cisco 7200 routers equipped with NPE-G2 and enabled for VSA card, along with T1 PRI card. It does not happen when running on NPE-G1 with VAM2 card.

  Workaround: There is no workaround.

- CSCsr25788

  Symptoms: Output drops can be observed on GE/FE interface on a Cisco 2800 router.

  Conditions: Problem is observed when NAT is enabled while router is configured to pass multicast traffic.

  Workaround: There is no workaround.

- CSCsr50834

  Symptoms: A CPU hog may be seen after changing the “logging buffered” setting to up to 50 MB or more. This issue can cause an OSPF flap.

  Conditions: The symptoms are observed with Cisco IOS Release 12.2(33)SXH2 on a Cisco WS-C6506.

  Workaround: Instead of manipulating such a large logging buffer at runtime when the device/network is busy, consider configuring the “logging buffered” setting once and save it as part of the startup configuration. This way, the huge logging buffer will be allocated during the device initialization without runtime impact.

- CSCsr51801

  Symptoms: Some of the route-maps configured for BGP sessions (eBGP) are not permitting the prefixes upon a router reload.

  Conditions: The symptom is observed when a large number of route-maps for a BGP session are configured and the router is reloaded.

Workaround: Issue the **clear ip bgp * soft** command.

- CSCsr72352

  Symptoms: EBGP-6PE learned IPv6 labeled routes are advertised to IBGP-6PE neighbor by setting NH as local IP address.

  Conditions: This symptom is observed on 6PE Inter-AS Option C with RR case.

  Workaround: There is no workaround.

- CSCsr83547

  Symptoms: Dialer watch on the Cisco 3845 router makes the backup link of PPP multilink on the PRI port which is connected to BRI 4 port of peer router through ISDN net. If one out of four BRI ports is shut down on the peer router, the dialer watch does not keep the backup link up without resetting the idle timer at the expiration of idle timeout though the primary link remains down, causing the other three ports to be disconnected.

  Conditions: This symptom occurs only when the BRI port which contains B-ch that became link up first is shut down. This symptom does not occur even if the other BRI ports are shut down.

  Workaround: There is no workaround.

- CSCsr93764

  Symptoms: Bus error exceptions due to Application Firewall HTTP inspection.

  Conditions: This issue has been seen in several Cisco 3845 routers running Cisco IOS Release 12.4(15)T5 with IP Inspect configured.

  Workaround: There is no workaround.

- CSCsr96753

  Symptoms: A router may crash when entering the **isdn test call** command.

  Conditions: The symptom is observed when the BRI interface is up.

  Workaround: There is no workaround.

- CSCsr97753

  Symptoms: Pinging an interface fails.

  Conditions: Occurs when unconfiguring xconnect on the interface.

  Workaround: Perform a **shut/no shut** on the the interface.

- CSCsr98707

  Symptoms: When the main ATM interface MTU has an explicit non-default value (something other than 4470), then the subinterfaces may not save (shown with the **show run** command) the explicit MTU configuration of the default (4470) even though the command is expected.

  Conditions: The symptoms are observed only for the ATM MTU value 4470. This unexpected behavior is not seen for any other value (less than or more than 4470 within allowed ATM MTU values).

  Workaround: Upon reload, manually (explicitly) configure MTU 4470. You can configure an IP MTU under the ATM interface instead of an ATM MTU.

- CSCsu03038

  Symptoms: A memory leak occurs.

  Conditions: This symptom is observed in some cases when SSG TCP redirection is used.

  Workaround: There is no workaround.

- CSCsu21828

  A series of TCP packets may cause a denial of service (DoS) condition on Cisco IOS devices that are configured as Easy VPN servers with the Cisco Tunneling Control Protocol (cTCP) encapsulation feature. Cisco has released free software updates that address this vulnerability. No workarounds are available; however, the IPSec NAT traversal (NAT-T) feature can be used as an alternative.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090325-ctcp.shtml.

  Note: The March 25, 2009, Cisco IOS Security Advisory bundled publication includes eight Security Advisories. All of the advisories address vulnerabilities in Cisco IOS Software. Each advisory lists the releases that correct the vulnerability or vulnerabilities in the advisory. The following table lists releases that correct all Cisco IOS Software vulnerabilities that have been published in Cisco Security Advisories on March 25, 2009, or earlier.

  http://www.cisco.com/en/US/products/products_security_advisories_listing.html

- CSCsu24087

  Symptoms: A router hangs for a couple of minutes and then crashes anytime the **clear ip bgp neighbor x.x.x in** command is issued.

  Conditions: This symptom occurs when a router crashes when the **clear ip bgp neighbor x.x.x.x soft in** command is issued when the following commands are configured for that neighbor (without route-map):

  1) **neighbor x.x.x.x soft-reconfiguration inbound**

  2) **neighbor x.x.x.x weight**

  3) **neighbor x.x.x.x filter-list in**

  If any one of the commands is not configured, then the router will not crash.

  Workaround: Configure route-map instead of filter-list for inbound direction. For example: **neighbor x.x.x.x filter-list 1** in replace with **neighbor x.x.x.x route-map *name* in**.

  Where, route-map *name* permit 10 match as-path 1.

- CSCsu29526

  Symptoms: Customer is seeing memory corruption crash on his device while doing NAT protocol translation from IPv4 to IPv6.

  Conditions: System was restarted by error—an unknown failure.

  Workaround: Apply the following to the configuration:

  no ipv6 nat service dns

  Note that there will not be IP address translation in DNS packets going between IPv6 and IPv4 network.

- CSCsu44789

  Symptoms: Spurious memory access traceback is seen.

  Conditions: The symptom is observed when an MGCP Gateway tries to defer a Request Notification (RQNT) without the requested/signal event.

  Workaround: There is no workaround.

- CSCsu71818

  Symptoms: A Cisco 7206VXR (NPE-G1) experiences a memory corruption and then crashes.

Conditions: Occurred on a Cisco 7206VXR (NPE-G1) that is very busy running NAT. The router crashed with the following Cisco IOS Release 12.4(16a) and 12.4(15)T1.

Workaround: There is no workaround.

- CSCsu77667

  Symptoms: The **time-range** commands used by ACLs no longer work, and the ACL time-range entries show as always active.

  Conditions: Configure ACL time-ranges and have Cisco IOS code that supports SSLVPN. Once the router is reloaded, SSLVPN takes over the ACL time ranges and these time ranges no longer work for ACLs.

  Workaround: Reconfigure the configuration mode ACL time ranges after the reboot.

  Further Problem Description: The **show startup-configuration** command will show the correct configuration:

  ```
  webvpn context Default_context ssl authenticate verify all ! no inservice ! time-range
  afternoon periodic weekdays 12:00 to 16:59
  ```

  With the **time-range** command in global context.

  The **show running-config** command will show the incorrect configuration:

  ```
  webvpn context Default_context ssl authenticate verify all ! time-range “afternoon”
  periodic weekdays 12:00 to 16:59 ! no inservice ! with the time-range command in
  webvpn context.
  ```

- CSCsu78553

  Symptoms: Spurious memory found in sslvpn_create_session procedure.

  Conditions: The symptom is observed when SSLVPN is configured.

  Workaround: There is no workaround.

- CSCsu92432

  Symptoms: The router’s async line used for reverse SSHv2 might hang after a failed authentication and not recover unless the router is rebooted. The router log displays:

  ```
  %SYS-3-HARIKARI: Process SSH Process top-level routine exited
  ```

  Conditions: The symptom is observed on a router that is running Cisco IOS Release 12.4 with async lines.

  Workaround: Use the traditional way of using reverse SSH with the use of rotaries.

- CSCsv01474

  Symptoms: The **ip rip advertise** command might be lost from the interface.

  Conditions: This symptom occurs in any of the following three cases:

  1. The interface flaps.

  2. The **clear ip route** command is issued.

  3. The **no network <prefix>** command and then the **network <prefix>** command are issued for the network corresponding to the interface.

  Workaround: Configure the **timers basic** command under the address-family under rip.

- CSCsv04275

  Symptoms: The **show logging** command displays messages such as the following:

  ```
  <date>: %ATM_AIM-5-CELL_ALARM_UP: Interface ATM<if ID> lost cell delineation. <date>:
  %ATM_AIM-5-CELL_ALARM_DOWN: Interface ATM<if ID> regained cell delineation.
  ```

  The link may go down and then recover automatically.

Conditions: This symptom is observed under ordinary operation. There is no apparent trigger. The physical line is known to be good.

Workaround: There is no workaround.

- CSCsv04674

  Symptoms: The M(andatory)-Bit is not set in Random Vector AVP, which is a must according to RFC 2661.

  Conditions: This symptom is observed with Egress ICCN packet with Random Vector AVP during session establishment.

  Workaround: There is no workaround.

- CSCsv12795

  Symptoms: Control Plane Policing (CoPP) is not matching or policing ICMP packets correctly.

  Conditions: This symptom is observed with routers that are configured with DMVPN and that are running Cisco IOS Release 12.4(15.3)T (or a later release).

  Workaround: There is no workaround.

- CSCsv15266

  Symptoms: A router that is running Cisco IOS Release 12.4 with QoS configured with a parent and child policy may experience a reset due to a software-forced crash displaying one of the following messages:

  ```
  %SYS-2-FREEFREE: Attempted to free unassigned memory at XXXXXXXX, alloc XXXXXXXX,
  dealloc XXXXXXXX
  ```
  or
  ```
  %SYS-6-BLKINFO: Corrupted magic value in in-use block blk XXXXXXXX, words XX, alloc
  XXXXXXXX, Free, dealloc XXXXXXXX, rfcnt X
  ```
  Conditions: The reset is triggered by a configuration change tied to QoS and has been seen while changing one of the following:

  - An access-list referenced by the map-class.
  - The DSCP/Precedence values being set by the service-policy.
  - Removing the service-policy from the interface.
  - Altering the shaping parameters within the service-policy.

  Workaround: Other than avoid making changes to the QoS outside of a maintenance window, there is no workaround.

- CSCsv20948

  Symptoms: The primary router may crash continually.

  Conditions: The symptom is observed with two Cisco 3825 routers with the same software and hardware and with a situation where one is working as a primary router and the other as a secondary. The issue is seen only with voice traffic. It is observed when running Cisco IOS Release 12.4(20)T (with this release the primary router crashes very frequently) and also with Cisco IOS Release 12.4(20)T1.

  Workaround: There is no workaround.

- CSCsv25088

  Symptoms: When the IMA group statement under the atm3/0 T1 interface is removed, the other T1s will still remain up in the IMA group, but the PVC will become inactive. This symptom happens only when the ATM Bandwidth Dynamic statement is under the atm1/ima main interface. When removing the IMA group under atm3/1 without the ATM Bandwidth Dynamic statement under the atm3/ima0 interface, the PVC stays up on line.

  Condition: This problem is seen in the Cisco 7206vxr with a npe-g1 or npe-400 with the 8-port PA IMA card PA-A3-8T1IMA. The problem is not see in Cisco IOS Release 12.3(28)M, but the problem is seen in Cisco IOS Release 12.4(6)T11 and 12.4(15)T6/T7 and also in Cisco IOS Release 12.4(20)T and 12.4(21)M.

  Workaround: Re-add ima-group 0 back under the atm3/1 interface and then shut down the atm3/1 interface.

  Further Problem Description: Steps to recreate the issue:

  configure terminal
  int atm3/1
  no ima-group 0 < Take out.
  int atm3/2
  ima-group 0
  int atm3/3
  ima-group 0

  atm3/ima0
  atm bandwidth dynamic

  atm3/ima0.1
  ip address x.x.x.x
  pvc 1/101
  vbr-nrt 4500 4500

  The **show atm vc** command will show the PVC as inactive.

- CSCsv28806

  Symptoms: When a dspfarm profile still has active calls, if the user manually shuts down the dspfarm profile, the router will crash.

  Conditions: The user manually shuts down a dspfarm profile when it is still in use with active calls. This includes the case where a dspfarm profile is manually shut down after a DSP crash occurs to the dspfarm service but the endpoint phones have not yet finished hanging up.

  Workaround: Do not shut down a dspfarm profile if it is still in use by active calls. Besides, if a DSP crash occurs, hang up all the phones using that dspfarm service and wait until the DSP sessions are released before manually shutting down the dspfarm profile.

- CSCsv31812

  Symptoms: Version: disk2:c7200-adventerprisek9-mz.124-22.T on KSs and GMs:

  ```
  Oct 26 18:41:50: %GDOI-5-KS_SEND_MCAST_REKEY: Sending Multicast Rekey for group
  DGVPN-ALPHA from address 10.32.178.56 to 239.192.1.190 with seq # 23 Oct 26 18:41:50:
  %SYS-3-MGDTIMER: Uninitialized timer, set_exptime, timer = 20A64C70. -Process= "Crypto
  IKMP", ipl= 0, pid= 201, -Traceback= 0x6147CC48 0x62E75F4C 0x6392E05C 0x6392E300
  0x63B25A70 0x63B25AF8 0x639308FC 0x63855544 0x6392F794 0x638100F4 0x638144E4
  ```

  Conditions: KS2, CE1, and m-gm are connected to PE1. s-gm is connected to PE2. PE1 and PE are in MPLS cloud.

Lower the priority of KS1 and change the primary KS role from KS1 to KS2 by entering the **clear crypto gdoi ks coop role** command in KS1. KS2 becomes the primary. Tracebacks are seen in the KS2.

Workaround: There is no workaround.

- CSCsv38166

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

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

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

  Cisco has released free software updates that address this vulnerability.

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

  This advisory is posted at the following link:

  http://www.cisco.com/warp/public/707/cisco-sa-20090325-scp.shtml

- CSCsv40404

  Symptoms: When DDNS is disabled on the router which is configured as the DHCP server, it sends option 81 in the DHCP ACK message with the N flag bit set to 1. However, the DHCP client fails to understand this and will not undertake a PTR update.

  Conditions: The issue is seen with a third-party vendor DNS server and a Cisco IOS DHCP server.

  Workaround: There is no workaround.

  Further Problem Description: The issue is not seen with the 12.3 code as it does not support DDNS and hence does not reply back with Option 81 in the DHCP ACK.

- CSCsv43444

  Symptoms: A router will run out of memory when SIP phones register.

  Conditions: Occurs when Cisco 3911 phones are installed

  Workaround: Disable MWI.

- CSCsv43658

  Symptoms: When a service-policy which is already in use by PDPs of an APN is applied to another APN, the Gateway Support Node (GGSN) to crash.

  Conditions: Occurs when the same service-policy is applied to different APNs.

  Workaround: Apply unique service-policies to each APN. For example if service-policy ggsn1 is applied to apn1.com, then service-policy ggsn2 should be applied to apn2.

- CSCsv45669

  Symptoms: EIGRP fails to send updates via the dialer when the ATM interface is flapped.

Conditions: The symptom is observed in a PPPoATM setup with cloned virtual-access subinterfaces and an EIGRP neighbor established over that PPPoATM connection. When the ATM interface carrying the PVC in use for the PPPoATM session is shutdown and reenabled after the EIGRP neighbor and PPPoATM session have timed out, we see a problem with reestablishing the EIGRP neighborship.

Workaround: In global configuration mode, use the following command: **no virtual-template** *subinterface*. This instructs the router to clone only the main interfaces, not the virtual-access subinterfaces.

- CSCsv49731

  Symptoms: Cisco IOS automatically adds the violate-action to the configuration when policing traffic.

  For instance, the intended config is as follows:

  policy-map p1
  class c1
  police 20000 4470 conform-action transmit exceed-action set-clp-transmit

  Instead, Cisco IOS software additionally configures the violate-action on its own as follows:

  policy-map p1
  class c1
  police 20000 4470 conform-action transmit exceed-action set-clp-transmit
  violate-action set-clp-transmit

  This causes the counters to count the number of exceeded/violated packets incorrectly.

  Conditions: This condition occurs in QoS configuration. Occurs on routers running Cisco IOS Release 12.4(20)T1. It was observed across all fixed and modular platforms.

  Workaround: There is no workaround.

- CSCsv54130

  Symptoms: Ping fails in HWIC-2T and WIC-2T when the physical mode is changed to “Async” from “Sync” with PPP encapsulation.

  Conditions: The symptom is observed when the initial configuration is in Sync mode as shown:

  interface Serial0/1/0
  ip address x.x.x.x 255.0.0.0
  encapsulation ppp
  end

  Then the configuration is changed to Async mode:

  interface Serial0/1/0
  physical-layer async
  ip address x.x.x.x 255.0.0.0
  encapsulation slip
  async mode dedicated
  end

  Workaround: Toggling the encapsulation to PPP sometimes fixes the issue. This may have to be done multiple times until the interface comes up.

- CSCsv58300

  Symptoms: Classification is not done correctly. It is matching the IPSec header instead of matching parameters in the original header despite “qos pre-classify” configuration.

Conditions: It has been observed in a Dynamic Multipoint VPN (DMVPN) spoke, GRE tunnel with IPSec protection configured with **qos-preclassify** and applying service policy to the physical interface.

Workaround: Classify traffic in ingress service-policy marking the traffic. Classify traffic in the egress with the mark inserted in ingress policy.

- CSCsv59334

  Symptoms: Upon entering the **no network 0.0.0.0 0.0.0.0** configuration command under EIGRP router configuration mode, all the EIGRP routes that were redistributed be withdrawn.

  Conditions: The symptom is observed when using explicit network prefixes as well as network 0.0.0.0/32, which includes unspecified, directly connected networks to enable EIGRP on various interfaces of a router. These EIGRP routes are also redistributed into BGP. In such a case, on entering the **no network 0.0.0.0 0.0.0.0** configuration command under EIGRP router configuration mode, all the EIGRP routes that were redistributed get withdrawn. For example:

```
router eigrp 1
 network 10.0.0.0
 network 0.0.0.0

show ip eigrp topo

EIGRP-IPv4 Topology Table for AS(1)/ID(10.1.1.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply, r - reply Status, s
- sia Status
P 10.1.1.1/32, 1 successors, FD is 128256 via Connected, Loopback1 P 10.1.1.0/24, 1
successors, FD is 281600 via Connected, Ethernet1/0 P 10.147.204.64/26, 1 successors,
FD is 281600 via Connected, Ethernet0/2 P 10.147.204.0/26, 1 successors, FD is 281600
via Connected, Ethernet0/0
```

  In the above configuration, network 10.0.0.0/24 is explicitly included under EIGRP by the network 10.0.0.0 configuration. The other networks (13, 20 etc) are included by the network 0.0.0.0 configuration. If EIGRP routes are redistributed into BGP, the three networks 10, 13 and 20 can be seen by BGP. Upon entering a **no network 0.0.0.0 0.0.0.0** command, we would expect the redistribution of networks 13 and 20 to stop while network 10 continues to be redistributed. However, all the networks 10, 13, and 20 do not get redistributed into BGP.

  Workaround: Clear the IP route and reload to allow the networks to get in the BGP table.

- CSCsv62225

  Symptoms: Router crashed when PPPoE sessions were cleared and policy was removed.

  Conditions: This symptom occurs while removing policy using **no policy-map name**

  Workaround: There is no workaround.

- CSCsv62777

  Symptoms: A VTY session may get stuck after some extended pings are done and the CPU process may go high.

  Conditions: The symptom is observed when an extended ping with CLNS is done and the command is left incomplete until the vty session times out.

  Workaround: Issue can be prevented by not leaving the extended **ping clns** command incomplete for long time in the vty session.

- CSCsv63799

  Symptoms: A router may reload if PfR is enabled and the number of flows exceeds the size of the NetFlow cache. This is a stress condition.

Conditions: This symptom is observed when PfR is enabled (which also enables NetFlow).

Workaround: A possible workaround is to configure the following:

ip flow-cache timeout active 1

- CSCsv65867

  Symptoms: NM-CEM-4SER modules installed in Cisco 3845 routers will not use network clock if one is available. Instead, they will use the local oscillator. This can be observed by using the **show cem** *slot*/*port*/*0* command.

  Conditions: This behavior is observed on a NM-CEM-4SER module installed in Cisco 3845 routers running Cisco IOS Release 12.4(20)T or later.

  Workaround: Use adaptive clocking to improve clock accuracy.

- CSCsv66513

  Symptoms: When an external interface is shutdown (on a controlling border router) all the applications (controlled) on that interface do not go to DEFAULT state.

  Conditions: The symptom is observed when PfR is enabled with applications that are configured to be controlled. It is seen when more than one application that is controlled (on same border router) exits.

  Workaround: There is no workaround.

- CSCsv66827

  Symptoms: Clearing the SSH sessions from a VTY session may cause the router to crash.

  Conditions: The symptom is observed when a Cisco 7300 series router is configured for SSH and then an SSH session is connected. If the SSH session is cleared every two seconds using a script, the symptom is observed.

  Workaround: There is no workaround.

- CSCsv67618

  Symptoms: The **show ip bgp vpnv4 all** command does not display all routes in the routing table.

  Conditions: This symptom occurs on a Cisco 7200 that is running a Cisco IOS Releas 12.4(15)T8.fc2 image.

  Workaround: There is no workaround.

- CSCsv69784

  Symptoms: A middle buffer leak is observed when using the combination of RIP and multipoint frame relay.

  Conditions: Currently the trigger is unknown.

  Workaround: There is no workaround.

- CSCsv73509

  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.

- CSCsv77441

  Symptoms: Memory fragmentation occurs in CDAPI-RawS.

Conditions: The conditions under which this symptom occurs are unknown.

Workaround: There is no workaround.

- CSCsv77531

  Symptoms: A device that is running affected versions of Cisco IOS software may reload.

  Conditions: Device is performing either CBAC traffic inspection or Zone Based Firewall Inspection on TFTP.

  Example vulnerable configuration for CBAC traffic inspection:

```
!
! TFTP inspection rule is configured. !
ip inspect name example_name tftp
!
! Apply inspection rule to the interface !
interface Ethernet1/1
 ip inspect example_name in
!
```

  Further information on CBAC is available at:

  http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_cfg_content_ac.html

  Example vulnerable configuration for Zone-Based Policy Firewall inspection:

```
!
! Create a CBAC Class Map !
class-map type inspect match-all tftp-traffic
 match protocol tftp
 match access-group 100
!
! Create a CBAC Policy Map !
policy-map type inspect tftp-inspection
 class type inspect tftp-traffic
  inspect
!
```

  Further information on Zone-Based Policy Firewalls are available at the following link:

  http://www.cisco.com/en/US/products/ps6441/products_feature_guide09186a008060f6dd.html

  Workaround: Disable ios-firewall inspection for tftp.

- CSCsv77851

  Symptoms: Display IE contained in connect message is not passing through H323 to ISDN interworking at Voice Gateway (vGW).

  Conditions: This happens when call Initiator makes an ISDN call to end device passing through OGW and VGW having Cisco IOS interim Release 12.4(15)T8.fc2 images.

  Workaround: There is no workaround.

- CSCsv79592

  Symptoms: Zone Based Firewall ESMTP inspection is not working, ESMTP connections fail. When looking at the EHLO command when it exits the firewall router, it will have been changed to EHLX.

  Conditions: This has been seen when ESMTP inspection is enabled on a router that is running Cisco IOS Release 12.4(15)T5.

  Workaround: Match on tcp instead of on smtp extended to allow the connections to go through.

  For example:

class-map type inspect match-any sdm-cls-insp-traffic
no match protocol smtp extended
match protocol tcp
end

- CSCsv85530

  Symptoms: When accounting is enabled for virtual private dial-up network (VPDN), there might be messages with termination cause “nas-error” and displaying impossible values in Acct-Input-Octets, Acct-Output-Octets, Acct-Input-Packets and Acct-Output-Packets.

  This causes accounting to be unreliable.

  Conditions: Occurs with Cisco IOS Release 12.4T and with a PPTP/L2TP plus accounting configuration.

  Workaround: There is no workaround.

- CSCsv87146

  Symptoms: Clearing of NAT translation either manually or automatically through timeout results in crash.

  Conditions: Occurs when a dynamic translation mapping is removed while traffic is running.

  Workaround: Stop traffic before removing dynamic NAT translation.

- CSCsv90106

  Symptoms: A router may write a crashinfo that lacks the normal command logs, crash traceback, crash context, or memory dumps.

  Conditions: This might be seen in a memory corruption crash depending on precisely how the memory was corrupted.

  Workaround: There is no workaround.

- CSCsv91602

  Symptoms: Cisco 7201 with Gi0/3 experienced communication failure.

  Conditions: This problem does not occur with Gi0/0 or Gi0/2.

  Workaround: Perform a **shut/no shut** on the Gi0/3. The problem will occur again.

- CSCsv92292

  Symptoms: The following error mesg is observed when RITE is applied to the interface:

  ```
  011419: Nov 19 17:53:15.422 CST: %SYS-2-BADBUFFER: Attempt to use contiguous buffer as
  scattered src, ptr= 83C60298, pool= 83C6010C -Process= "<interrupt level>", ipl= 4,
  -Traceback= 0x808DF468 0x80059428 0x8139A9C0 0x8139AEA4 0x80374540 0x8079DD5C
  0x803DEB54 0x8040E938 0x8041235C 0x803FAFB0 0x804D0BA8 0x800AEF4C 0x8001A964
  0x8001A964 0x800AF008 0x800B6D80
  ```

  Conditions: The error is observed at a c181x device with c181x-advipservicesk9-mz.124-15.T6 when RITE is configured on the interface.

  Workaround: Remove the RITE from the interface configuration.

- CSCsv94099

  Symptoms: Traceback may be seen in relay.

  Conditions: The symptom is observed in an unnumbered scenario when the client releases the address.

  Workaround: There is no workaround.

- CSCsv94905

  Symptoms: A Cisco 2800 crashes at xpfGetACLPATNodeFromMessage.

  Conditions: This symptom is observed under normal Cisco IOS operation.

  Workaround: There is no workaround.

- CSCsv97772

  Symptoms: The System Activity (SYS ACT) LED may keep blinking even though there are no configurations or traffic.

  Conditions: The symptom is observed on a Cisco 2800 series router with an NM-16A/S, which is connected to another device through a CAB-SS-X21MT. The problem is only seen on a couple random ports on a few random modules.

  Workaround: Use RS-232 cables instead of X.21 cables.

- CSCsw14681

  Symptoms: The Sync Timer is not running after using the command **clear crypto gdoi**.

  Conditions: The symptom is observed with the following steps:

  1. Configure two cooperative KSs.

  2. Use the Cisco IOS 12.4(23.7)T image.

  3. Either reload or issue the **clear crypto gdoi** command in both routers.

  4. Let the election process complete.

  5. When the **sh crypto gdoi ks replay** command is issued, the following is shown:

```
%GDOI-5-COOP_KS_ELECTION: KS entering election mode in group GetvpnAdvanced1 (Previous
Primary = NONE) %GDOI-5-COOP_KS_TRANS_TO_PRI: KS 10.10.1.1 in group GetvpnAdvanced1
transitioned to Primary (Previous Primary = NONE) KS1#sh crypto gdoi ks replay
Anti-replay Information For Group GetvpnAdvanced1: Timebased Replay: Replay Value :
89.01 secs Remaining sync time : Timer is not running <------------
Anti-replay Information For Group GetvpnAdvanced2: Timebased Replay: Replay Value :
70.36 secs Remaining sync time : Timer is not running <--------------------
Anti-replay Information For Group GetvpnAdvanced3: Timebased Replay: is not enabled
```

  Workaround: There is no workaround.

- CSCsw15188

  Symptoms: Router crashes when enabling **debug isdn q931**

  Conditions: Problem happens when logging debugs from **debug isdn q931** to an external syslog server.

  Workaround: Disable the syslog server when doing the debugs.

- CSCsw21960

  Symptoms: A router crashes while executing some NAT commands.

  Conditions: The symptom is observed under the following conditions:

  - Try and configure “inside destination translation” with the command before configuring the pool or the access list “ip nat inside destination list ABC pool pool1.”
  - While you configure the above, keep traffic ON.
  - Make sure some active dynamic translations are present while you are configuring this.

  The router does not crash all the time. A combination of the above commands and removing and reconfiguring with traffic can cause the router to crash.

  Workaround: There is no workaround.

Further Problem Description: The crash is not consistently reproducible.

- CSCsw22791

  Symptoms: The router may crash if Group Domain of Interpretation (GDOI) configurations are removed concurrently with the execution of the **show crypto gdoi** command (that is, they are running on different TTY sessions).

  Conditions: The symptom is observed when the removal of the configurations and the execution of the show command are concurrent.

  Workaround: Avoid removing the configuration and executing the **show crypto gdoi** command concurrently.

- CSCsw23397

  Symptoms: A Cisco Communication Media Module (CMM) may leak memory in the chunk manager.

  Conditions: The symptom appears to be triggered by calls that disconnect prematurely.

  Workaround: There is no workaround.

  Further Problem Description: Though this problem is seen and reported on CMM, it may occur on any Cisco IOS gateway that supports voice (28xx, 38xx, 5xxx).

- CSCsw23664

  Symptoms: Reverse Route Injection (RRI) is not working as expected with VPN routing/forwarding (VRF) aware IPSec. Routes are created but may not be removed leaving them stranded in the routing tables.

  Conditions: Occurs on routers running Cisco IOS Release 12.4(15)T and above.

  This issue is resolved in the following releases:

  - 12.4(22)T1
  - 12.4(20)T2
  - 12.4(15)T9

  Workaround: There is no workaround.

- CSCsw24542

  Symptoms: A router may crash due to a bus error after displaying the following error messages:

  ```
  %DATACORRUPTION-1-DATAINCONSISTENCY: copy error, %ALIGN-1-FATAL: Illegal access to a
  low address < isdn function decoded>
  ```

  Conditions: The symptom is observed on a Cisco 3825 router that is running Cisco IOS Release 12.4(22)T with ISDN connections.

  Workaround: There is no workaround.

  Further Problem Description: When copying the ISDN incoming call number for an incoming call from Layer2, the length of the call number was somehow exceeding the maximum allocated buffer size (80). PBX has pumped a Layer2 information frame with call number exceeding the maximum number length limit. It leads to memory corruption and a crash.

- CSCsw29842

  Symptoms: A router may reload or crash at resource_owner_set_user_context while adding and removing MTU in the ATM main interface and subinterface.

  Conditions: The symptom is observed when the command **no mtu** on the ATM subinterface modifies the minimum MTU size to zero.

Workaround: Set the MTU size of the subinterface to a default value or the value of the main interface's MTU instead of using **no mtu**.

Further Problem Description: The command **no mtu** on the ATM subinterface will modify the MTU size to zero. It should inherit the default value or value from the main interface if the main interface has an MTU value set. This issue does not affect any functionality of MTU.

- CSCsw30627

  Symptoms: A router crashes at mpoa_client_config when simultaneous users try to access the mpoa client configuration.

  Conditions: The router is loaded with rsp-jsv-mz.124-23.10.

  Workaround: There is no workaround.

- CSCsw31019

  Symptoms: A Cisco router crashes.

  Conditions: This symptom is observed if the **frame-relay be 1** command is issued under "map-class frame-relay <name>" configuration.

  Workaround: There is no workaround.

- CSCsw37279

  Symptoms: When using PKI for identifying group members a group member may fail to register with the key server if the certificate is not installed at the time GDOI is enabled.

  Conditions: SCEP is used for certificate enrolment.

  Workaround: Clear the current GDOI registration:

  clear crypto gdoi

  Remove all server addresses listed under a group on the GM except for one:

  config t
  crypto gdoi group GDOI_GROUP_1234
  no server address ipv4 <ip address>

  Limitation: This would leave only one KS available for the GM to register to.

- CSCsw39039

  Symptoms: A fax relay call may fail.

  Conditions: The symptom is observed with an MGCP Gateway Controlled T38 fax-relay call. MGCP is configured for CA control T38. The output of the command **show call active voice brief** will give the remote address to be 0.0.0.0. When this happens, all fax packets on the ingress gateway are dropped.

  Workaround: Use Cisco IOS Release 12.4(15)T7.

- CSCsw42244

  Symptoms: Traceback may be observed on a Cisco 3845 MGCP gateway.

  Conditions: The symptom is observed with a Cisco 3845 MGCP gateway during an SNMP walk.

  Workaround: There is no workaround.

  Further Problem Description: In order to set isdnBearerOperStatus during an SNMP walk, false-busy out condition of B channel is checked. In order to check the false-busy status for all interfaces, DSL information is extracted from the idb list. The idb list for the particular DSL can be NULL with a bulk SNMP query, and it is not checked for NULL before accessing. In this scenario, isdnBearerOperStatus should have only default value which is D_isdnBearerOperStatus_idle.

- CSCsw43948

  Symptoms: A Cisco 3845 router that is running Cisco IOS Release 12.4(13) may bounce the frames (which are not destined for itself) on the same interface that receives them.

  Conditions: The symptom is observed if there is bridging configured on an Ethernet subinterface in the following way:

  ```
  ip cef
  !
  bridge irb
  !
  interface GigabitEthernet0/1
   no ip address
   no shut
  !
  !
  interface GigabitEthernet0/1.100
   encapsulation dot1Q 100
   ip address x.x.x.x x.x.x.x
   no ip redirects
   no ip unreachables
   no ip proxy-arp
   ip rip advertise 10
  !
  interface GigabitEthernet0/1.509
   encapsulation dot1Q 101
   bridge-group 1
  ```

  Workaround: If the command **bridge-group 1** is removed from the subinterface, it will behave as expected.

- CSCsw44230

  Symptoms: High CPU observes with SIP call through NAT. NAT entry timeout timer causes slow entry deletion.

  Conditions: When high volume of SIP calls go through the NAT box.

  Workaround: Fine-tune UDP timeout value.

- CSCsw45320

  Symptoms: Router crashes after it has shown many tracebacks:

  ```
  %SYS-2-BADSHARE: Bad refcount in retparticle, ptr=xyz, count=0, -Traceback= ...
  %SYS-2-BADSHARE: Bad refcount in retparticle, ptr=xyz, count=0, -Traceback= ...
  %SYS-2-BADSHARE: Bad refcount in retparticle, ptr=xyz, count=0, -Traceback= ...
  ```

  Conditions: Router is terminating SSLVPN client sessions.

  Workaround: There is no workaround.

- CSCsw47543

  Symptoms: A router may loses all its free memory and crash.

  Conditions: The symptom is observed when the voice mail system sends a notification to the gateway regarding the availablity of any voice messages. The memory leaks occurs in CDAPI_RawS.

  Workaround: Use the **signalling forward none** command under the global configuration “voice service voip”.

- CSCsw49170

  Symptoms: VG20X with SCCP controlled FXS ports have switchover to CME-SRST and then switchback to Cisco Unified CallManager (CCM), and then one-way audio in calls is experienced.

  Conditions:

  – VG20X running Cisco IOS Release 12.4(22)T.
  – CME-SRST running Cisco IOS Release 12.4(15)T7.
  – CallManger running 7.0.

  The VG20X global configuration has the UCM set for version 7.0, as follows:

  sccp ccm <*call-manager-ip-address*>**id** <*identifier*> **version 7.0**

  The VG20X global configuration has the CME-SRST set for version 4.1, as follows:

  sccp ccm <*cme-srst-ip-address*> **id** <*identifier*> **version 4.1**

  Workaround: Enter the following commands:

  no sccp
  sccp

- CSCsw49297

  Symptoms: Packet drops and/or delays are observed when sending traffic over a multilink bundle interface.

  Conditions: This symptom may occur during periods of bursty traffic.

  Workaround: Increase the amount of data that a multilink will queue to a member link at any given time using the interface configuration command **ppp multilink queue depth qos** (default = 2). This command may be configured on the serial interfaces or, if the interface is a multilink group member, it may be configured on the multilink interface. For example:

  interface Multilink1
  ppp multilink queue depth qos 3

- CSCsw52932

  Symptoms: Group members' rekey SAs that have the same IKE SA endpoints (source/destination addresses) are mistakenly deleted when one of the group members has to re-register.

  Conditions: This occurs when one of the group members has to re-register.

  Workaround: Have all the group members re-register at the same time (e.g., reapply the crypto map or use the **clear crypto gdoi** command).

- CSCsw62997

  Symptoms: Traceback is seen while configuring a policy in the virtual-template on LAC.

  Conditions: The symptom is observed when the class-map under the policy has the following filter:

  match vlan <vlan-id>

  Workaround: There is no workaround.

- CSCsw63356

  Symptoms: The following messages may be seen when bringing up a WIC-1DSU-T1-V2:

  ```
  %SERVICE_MODULE-4-WICNOTREADY: (with traceback)
  ```
  and/or
  ```
  WARNING - timeslots command not accepted by service-module % Service module
  configuration command failed: LOCK OBTAIN TIMEOUT.
  ```

Conditions: The symptom is observed with a Cisco 3825 and a 3845 router where WIC-1DSU-T1-V2 or HWIC-1DSU-T1 is present in one or more WIC/HWIC slots and one WIC-1DSU-T1-V2 is in any of the NM slots. In this setup, the problem will be seen on the highest number WIC/HWIC slot where WIC-1DSU-T1-V2 or HWIC-1DSU-T1 is present.

Workaround: Use WIC-1DSU-T1-V2 in either WIC slots or NM slots (not in both).

Alternate workaround: Use a Cisco IOS release prior to 12.4(15)T7.

- CSCsw66086

  Symptoms: A router may crash with a segmentation violation (SegV) exception in MPLS code.

  Conditions: The symptom is observed when “ip route-cache flow” is configured on an MPLS interface.

  Workaround: There is no workaround.

- CSCsw68022

  Symptoms: A router crashes after unconfiguring SCCP group using the following command:

  no sccp ccm group #

  Conditions: The symptom is observed when SCCP group is configured on the router, and DSPfarm profiles (conference and transcoding) are configured and active on the router. If the commands **no sccp ccm group #** and **dspfarm profile <id> conference** followed by **shutdown** are entered at the same time, the router crashes.

  Workaround: Do not enter the commands **no sccp ccm group #** and **dspfarm profile <id> conference** followed by **shutdown** at the same time.

- CSCsw70204

  Symptoms: WISPr attributes could cause memory leak in ProxyLogon situation.

  Conditions: The symptom is observed when the subscriber logs on using WISPr attributes.

  Workaround: There is no workaround.

- CSCsw70566

  Symptoms: User is experiencing port block when using STCAPP. Behavior is that when going offhook, no dialtone can be heard. Only performing a shut/no shut on the voice port can bring it back to IDLE and get the dialtone.

  Conditions: Customer is using CUCM and VG224 gateway to connect to analog phones. Skinny is the control protocol.

  Workaround: There is no workaround.

  Root Cause Analysis: Before PI9, the VPM layer will never send the disconnect confirmation and the setup_ind at the same time (or within 4 milliseconds). But after PI9, a ddts fix CSCsq97697 changed the behavior. In the case when the user goes onhook. Then, immediately after the hookflash duration is passed, he offhook the phone. Before PI9, this behavior will cause the new call’s setup be postponed until the next time the user goes onhook. But now, the setup_ind of the new call will be immediately sent right after the previous call’s disconnect confirmation. So, when messages traversed to VTSP layer, because of the nature of the DSMP dsp process, the disconnect_done event has more chance to come later than the new call’s setup_ind.

  In STCAPP, our design is based on the behavior of the time when it was developed (PI2). So we do not handle that sequence. But now, since this is the behavior, we will have to handle that case when disconnect_done comes after the new call’s setup_ind.

  Fix and Unit Test: The fix is to enhance the disconnect_done handler to make it more robust and more fault tolerant to accommodate this situation.

Unit test is done and the results are passed.

- CSCsw71188

  Symptoms: A Cisco 7200 series router may lose connectivity to the SDH link.

  Conditions: The symptom is observed under the following conditions:

  1. The Cisco 12416 router receives a PAIS Alarm from the Optical Network.

  2. The interfaces go down and up and the ALARM is cleared from the Cisco 12416 router side.

  3. The Cisco 7200 series router loses connectivity.

  4. The Cisco 12416 router interface POS is still UP, but the ping fails.

  5. After interface is shutdown and re-enabled, it is in serial UP but protocol DOWN from the Cisco 12416 router side.

  6. The link is recovered when the fiber is disconnected and reconnected from the Cisco 7200 series router side.

  Workaround: Disconnect and re-connect the fibers from the Cisco 7200 series router side.

- CSCsw77293

  Symptoms: Upon unconfiguring “channel-group” in one controller, the ping fails in another controller.

  Conditions: The symptom is observed when a controller is configured and then unconfigured with “channel-group”.

  Workaround: Configure “channel-group” again.

- CSCsw78699

  Symptoms: RTP compression does not work when only RTP traffic is flowing across the interface. The counters show ip rtp header-compression remains static throughout.

  Conditions: This has been observed on the Cisco 7200 platform with NPE-G2 and 12.4(15)T8 code.

  Workaround: Start sending out TCP traffic at the same time and we will see the compression work fine.

- CSCsw78939

  Symptoms: No new sessions can come up using VPDN after a few days.

  Conditions: The root cause is that we leak and run out of SSM switch IDs.

  Workaround: There is no workaround.

- CSCsw79696

  Symptoms: A call over the FXO loop-start cannot be established as the gateway’s DSP detects a reverse-battery signal.

  Conditions: The symptom is observed when the far-end is able to generate a reverse-battery signal when the called side is ringing. In addition, it is seen when “supervisory disconnect” is configured to either anytone or dualtone.

  Workaround: There is no workaround.

- CSCsw85121

  Symptoms: Microsoft Windows XP with SP3 (and possibly others OS flavors) is unable to connect via L2TP over IPsec onto a Cisco router running Cisco IOS Release 12.4(15)T8. ISAKMP Quick Mode Packet 1# debugs are revealing:

```
*Jan 6 10:37:30.691: IPSEC(validate_proposal_request): proposal part #1 *Jan 6
10:37:30.691: IPSEC(initialize_sas): invalid IPv4 proxy IDs *Jan 6 10:37:30.691:
ISAKMP:(2004): IPSec policy invalidated proposal with error 32 *Jan 6 10:37:30.691:
ISAKMP:(2004): phase 2 SA policy not acceptable! (local 10.48.67.119 remote
10.48.66.216) *Jan 6 10:37:30.691: ISAKMP: set new node -1705183588 to QM_IDLE *Jan 6
10:37:30.695: ISAKMP:(2004):Sending NOTIFY PROPOSAL_NOT_CHOSEN protocol 3 spi
1708235448, message ID = -1705183588
```

Conditions: L2TP client needs to be behind a NAT/PAT to get NAT-T negotiated.

L2TP over IPsec from a Microsoft OS to a router running Cisco IOS Release 12.4(15)T8. So far we have not found other affected versions.

Workaround: There is no workaround.

- CSCsw90055

  Symptoms: An FXO port with “supervisory disconnect tone” configured is unable to be released while receiving disconnect tone.

  Conditions: The symptom is observed when FXO is handling a fax call which will disable the FXO port “supervisory disconnect tone” capability and cause the FXO to be unable to detect the disconnect tone.

  Workaround: There is no workaround.

- CSCsw95531

  Symptoms: If hook flash occurs during a call that is not connected, interaction between gateway and CallManager will cause large number of zero duration call detail records to be written.

  Conditions: Occurs on VG224 running SCCP STCAPP and with Callmanager 4.2.

  Workaround: There is no workaround.

- CSCsw95670

  Symptoms: With Ethernet over MPLS configured in VLAN interface, End-to-End connectivity is broken between CE routers.

  Conditions: The issue is seen on router loaded with an internal build of 12.2(33)SR.

  Workaround: There is no workaround.

- CSCsw98414

  Symptoms: The **ip nat inside source ... match-in-vrf** command is not working without the *overload* option.

  Conditions: Occurs on a router running Cisco IOS Release 12.4(15)T8.

  Workaround: There is no workaround.

- CSCsx06457

  Symptoms: A router configured with BGP may generate IPRT-3-NDB_STATE_ERROR log messages. An additional symptom when **bgp suppress-inactive** is configured is that the router CPU usage may get close to 100%.

  Conditions: When both BGP and an IGP are advertising the same prefix, the error condition may occur. When in addition **bgp suppress-inactive** is configured high CPU usage by BGP may be seen.

  Workaround: Removing the **bgp suppress-inactive** configuration should eliminate the high CPU problem. Removing either the BGP or IGP conflicting routes from the system should clear both symptoms.

- CSCsx09343

  Symptoms: PKI daemon is stuck in DNS resolution attempt for the hostname used in the CDP.

Conditions: The symptom is observed when using name resolution for automatic actions taken by the router during non-interactive sessions (CRL download using name in CDP URI). This issue has been seen to occur only on a Cisco Catalyst 6500 running Cisco IOS SXH software.

Workaround: There is no workaround.

- CSCsx15358

  Symptoms: A router may crash after receiving DNS TCP queries.

  Conditions: The symptom is observed on a router with “ip dns server” configured.

  Workaround: There is no workaround.

- CSCsx15370

  Symptoms: EIGRP commands may disappear from the interface configuration.

  Conditions: The symptom is observed on Cisco routers that are running Cisco IOS Release 12.4T and following an interface flap.

  Workaround: There is no workaround.

- CSCsx18860

  Symptoms: Traffic does not pass.

  Conditions: The symptom is observed with a Cisco VPN Acceleration Module 2+ (VAM2+) originating traffic and with process switching.

  Workaround: There is no workaround.

- CSCsx19184

  Symptoms: Cisco 2821 got bus error crash even though there was no configuration change or hardware change.

  Conditions: Happens while running an internal image with potential fix for CSCsv20948 and CSCsw44230.

  Workaround: There is no workaround.

- CSCsx29605

  Symptoms: A QSIG-rose memory leak is observed with the QSIG MWI feature enabled. The topology is:

  Third-Party Phones----Third-Party PBX---QSIG----ISR----SIP-----IP Unity Voice Mail

  Conditions: The leak is observed per call during the following call scenario:

  Leave Message -> MWI ON -> Retrieve Message -> MWI OFF

  Workaround: There is no workaround.

- CSCsx35306

  Symptoms: Router crashes at “t3e3_ec_safe_start_push”.

  Conditions: The crash is seen immediately after removing the channel-group of the PA-MC-2T3/E3-EC card.

  Workaround: There is no workaround.

- CSCsx40747

  Symptoms: A specific configuration of “ip casa” followed by a subsequent use of the command **show running-config** can cause the router to go into an infinite loop and hang.

Conditions: The symptom is observed when “ip casa” is configured and you enter into config-casa mode. The command **show running-config** will cause the router to hang.

Workaround: There is no workaround.

Further Problem Description: This issue is specific to the usage of ip casa. If you do not use casa, you are not vulnerable to the issue described here.

- CSCsx41496

  Symptoms: When the Fast Ethernet interface is up, the **reload** command takes the card to an empty state. You need to enter **resetcd** from the PXM to bring the card to an active state.

  Conditions: The symptom is observed when the Fast Ethernet interface is connected to a Cisco 3750 router, a Cisco 2950 switch, and an RPMXF card. The Fast Ethernet interface should be up.

  Workaround: Enter **resetcd** from the PXM.

- CSCsx42261

  Symptoms: Memory leak at CCSIP_SPI_CONTROL process.

  Conditions: The error is found on a Cisco 3825 with the c3845-spservicesk9-mz.124-20.T1.bin image. Customer does not have SIP phones but SCCP phones.

  Workaround: There is no workaround. The box has to be reloaded regularly.

- CSCsx44172

  Symptoms: A privilege 15 user being authorized against a TACACS server can issue certain commands containing the arguments “**full**” or “**brief**” although these commands are disallowed in the TACACS server. For instance:

  – **show running-config brief**

  – **show running-config full**

  Conditions: When running TACACS debugs when the commands are executed, we can see that the privilege level is set to 0 for these commands, although the correct level should be 15. The router is configured with the following:

  aaa authorization config-commands
  aaa authorization exec default group tacacs+ if-authenticated
  aaa authorization commands 0 default none
  aaa authorization commands 1 default group tacacs+ if-authenticated
  aaa authorization commands 15 default group tacacs+ if-authenticated

  Workaround: There is no workaround.

- CSCsx45429

  Symptoms: The GM crashes when trying to display VSA policy detail using the command **show pas vsa policy detail** and when traffic is being sent through the GM.

  Conditions: The symptom is observed when using the command **show pas vsa policy detail**. It may affect all recent software releases.

  Workaround: There is no workaround.

- CSCsx46297

  Symptoms: EZVPN across DVTI is broken after rekey.

  Conditions: This symptom is observed only across DVTI. It is not observed with static interfaces.

  Workaround: There is no workaround.

- CSCsx48272

  Symptoms: A router acting as an EasyVPN client may fail to build the IPSec tunnel and hang in the IPSEC_ACTIVE state, as shown in the **show crypto ipsec client ezvpn** command output.

  Conditions: It is not clear at this point what triggers this failure.

  Workaround: There is no workaround.

- CSCsx51135

  Symptoms: In GETVPN scenarios, on VSA we keep both the SA and the corresponding ACE entry until the SA expires though that ACE entry was removed from the KeyServer. Whereas on S/W they keep the SA but remove the ACE entry.

  Conditions: When an ACE entry from the KS ACL is removed.

  Workaround: Enter the **clear crypto gdoi** command on the Group Members.

- CSCsx54460

  Symptoms: An RP abnormally restarts when the **show crypto ipsec sa identity** command is issued.

  Conditions: Simple configuration with site-to-site and no traffic.

  Workaround: There is no workaround.

- CSCsx55741

  Symptoms: Transit IPsec traffic is dropped on GM GETVPN. The following message is shown:

  ```
  %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for
  destaddr=192.168.6.1, prot=50, spi=0xC39A071A(3281651482), srcaddr=192.168.6.2
  ```

  Conditions: The symptoms are observed under the following conditions:

  1. A Cisco 7200 series router in combination with VSA as HW-accelerator.

  2. GDOI policy defined to not perform double encryption.

  3. R1 connects to R2[GM], connects to R3[GM], connects to R4. (R2 and R3 are two group members of a GETVPN networks.) The GDOI policy is: Deny R1=>R4; Deny R4=>R1; Permit any any.

  Workaround: Permit double encryption with the following caveat: If transitting ESP packet are near the IPsec path MTU then, after encapsulation into GETVPN IPSEC, they will be fragmented. The receiving side of the transit IPsec flow (R1 or R4 in above scenario) will have to reassemble these packets which can lead to high CPU on the receiving end.

  This makes the workaround more or less applicable depending on the transiting traffic partern.

- CSCsx59039

  Symptoms: Router crashes at SCCP SPI functions when handling events from STCAPP.

  Conditions: This is a corner case that occurs rarely. Only if STCAPP unregisters its SCCP device (forced by a DSP problem, in this case) while the corresponding voice-port is still active (having some internal event in the SCCP SPI queue to be processed after the unregistration), the crash can occur.

  Workaround: There is no workaround.

- CSCsx62644

  Symptoms: A router that was running Cisco IOS Release 12.4(15)T8 experienced a chunk corruption crash after issuing the **show ip ospf rib redist** command.

  ```
  %SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header, chunk 68309014 data 68310F78
  chunkmagic 682C3DD4 chunk_freemagic 0 -Process= "Virtual Exec", ipl= 0, pid= 265,
  -Traceback= 0x615F16EC 0x6015C908 0x62405ECC 0x624060CC 0x62C5B418 chunk_diagnose,
  code = 1 chunk name is OSPF redist RI
  ```

```
current chunk header = 0x68310F68 data check, ptr = 0x68310F78
next chunk header = 0x68310FB8 data check, ptr = 0x68310FC8
previous chunk header = 0x68310F18 data check, ptr = 0x68310F28
Corrupted magic value in in-use chunk
```

Conditions: This symptom is observed in the show_one_redist_entry S/W: 12.4(15)T throttle.

Workaround: There is no workaround.

- CSCsx63982

  Symptoms: A router configured for SNMP might unexpectedly crash with a bus error code.

  Conditions: This issue occurs when you query cSipCfgPeerTable of CISCO-SIP-UA-MIB. To be more specific, cSipCfgPeerPrivacy MIB object.

  Workaround: Do not poll cSipCfgPeerPrivacy MIB object.

- CSCsx68254

  Symptoms: Device will crash when loading the configuration with service policies with ACLs.

  Conditions: This is seen when more than 200 ACL filters are used in a service policy.

  Workaround: Remove unused ACLs in class-maps to get under the 200 limit. (The fix allows for 512 filters.)

- CSCsx73867

  Symptoms: A router that is running Cisco IOS Release 12.4(22)T and that is configured for L2L tunnels may intercept pass-through UDP 4500 packets destined to an internal client. Logged on the fault router is:

  ```
  %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for
  destaddr=x.x.x.x, prot=50, spi=0xDD8DEB2(232316594), srcaddr=y.y.y.y.
  ```

  Conditions: The symptom is observed on a router that is running Cisco IOS Release 12.4(22)T configured for IPsec. Internal IPsec client is natted on the router using NAT-T.

  Workaround: There is no workaround.

- CSCsx74657

  Symptoms: Multiple issues are seen on multicast NAT. NAT is adding the number of dynamic entry statistics for every new multicast packet, even though there is already an existing NAT flow entry. This causes the number of dynamic entries to be inconsistent with the output from **show ip nat trans**. Also, dynamic NAT entries cannot be deleted with **clear ip nat trans ***. Finally, every fragmented multicast packet creates a separate NAT entry.

  Conditions: This symptom is observed when the **ip pim sparse-dense-mode** command is configured on the interfaces with NAT overload.

  Workaround: There is no workaround.

- CSCsx82690

  Symptoms: A voice gateway placing ISDN calls will exhibit a memory leak. The effects of this memory leak can be seen with the **show process memory** command. It shows that the amount of memory the ISDN process is holding continues to increase without being released.

  Conditions: The symptom is observed on a voice gateway that is processing ISDN calls on a PRI interface. Switchtype is set to be primary-QSIG and the calls that leak memory are QSIG-GF (connection-oriented calls) and not regular voice calls. Such calls are typically used when implementing supplementary services such as MWI.

  Workaround: There is no workaround.

- CSCsx95906

  Symptoms: Call fails when a third-party endpoint is at remote end.

  Conditions: Third-party endpoint sends a long Contact header field value, which exceeds our maximum limit, in establishing a call. This remote contact over write memory for the from header and resulting a dialog mismatch for the new message generated by the GW.

  Workaround: There is no workaroud.

- CSCsy05162

  Symptoms: A Cisco 851W has rate-limit applied on an interface with an ACL, but the **show int rate-limit** command shows no traffic is matching.

  Conditions: This symptom is observed when a Cisco 851W has rate-limit applied on an interface with an ACL.

  Workaround: There is no workaround.

- CSCsy06128

  Symptoms: When a router is about to renew a certificate, the following syslog message is seen:

  ```
  %PKI-6-CERTRENEWAUTO: Renewing the router certificate for trustpoint xxx
  ```
  But no certificate is received until a few hours later.

  Conditions: The issue only happen on 871 platform, with image 15T8, 22T1, or earlier. Also, issue is only seen with a very short certificate lifetime (in this case, 1 hour).

  Workaround: Increase the certificate lifetime to a few days or more. Use another platform.

- CSCsy09101

  Symptoms: Cisco Configuration Professional (CCP) is unable to load signatures from the router. IOS-IPS signatures cannot be viewed or modified using CCP.

  Conditions: The symptom occurs when using CCP to manage IPS5.0 in routers that are running Cisco IOS Release 12.4(20)T2, 12.4(24)T, and 12.4(22)T1.

  Workaround: There is no workaround from CCP. Use CLI to view or modify IPS signatures.

- CSCsy15227

  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/warp/public/707/cisco-sa-20090923-auth-proxy.shtml

- CSCsy15468

  Symptoms: Crash keyserver reloads.

  Conditions: The symptom is observed if test case 1 in TBAR sanity regression on the VSA is configured and then unconfigured. When configuring the second one, the keyserver crashes.

  Workaround: There is no workaround.

- CSCsy24642

  Symptoms: Multiple tracback reporting Malloc Due to memory fragmentation.

  Conditions: This happens in a scenario with LNS MLPP and QoS. There could be another scenario, not seen in the lab.

Workaround: Suppress QoS.

- CSCsy29828

  Symptoms: A Cisco router may reload due to a bus error. The error indicates trying to read address 0x0b0d0b**, where ** is around 29.

  Conditions: This has been experienced on a Cisco 2800 series router running Cisco IOS Release 12.4(24)T. The router must be configured with NAT, and SIP traffic is passed through the NAT router.

  Workaround: Enter the following commands:

  - **no ip nat service sip tcp port 5060**
  - **no ip nat service sip udp port 5060**

  Or

  - **ip nat translation timeout never**

- CSCsy70619

  Symptoms: A router may crash when multipath is enabled and when the MR is registered with two or more of its roaming interfaces.

  Conditions: The symptom is observed when using the **no ip mobile router-service roam** command on any one of the MR's roaming interfaces.

  Workaround: There is no workaround.

- CSCsy71006

  Symptoms: When the configured TEK lifetime is greater than 65,000, the remaining TEK lifetime on the secondary KS shows zero remaining lifetime.

  Conditions: GDOI keyserver with TEK lifetime configured greater than 65,000.

  Workaround: Use a TEK lifetime less than 65,000.

- CSCsy71258

  Symptoms: Unable to boot a Cisco 850 series router using Cisco IOS Release 12.4(15)T9.

  Conditions: This symptom is observed on a Cisco 850 series router with 64 MB of DRAM. The image requires more DRAM to boot.

  Workaround: There is no workaround.

- CSCsy95484

  Symptoms: Ping fails from gen to ref.

  Conditions: This symptom is observed when the router is loaded with Cisco IOS Release 12.4(24.6)T5.

  Workaround: Perform a **shut** and **no shut** on the VLAN interface, and the ping passes.

- CSCsz16635

  Symptoms: One-way audio may be experienced on a call that traverses a transcoder hosted on an ISR platform (for example, Cisco 2800, Cisco 3800) after a hold, resume, or transfer.

  Conditions: When the call is held or resumed, there is a significant change in the RTP Sequence Numbers but the SSRC does not change.

  This behavior may cause the receiving device to assume that the RTP packets are out of sequence (that is, late, early, or lost), and therefore the receiving device may drop them.

This problem looks very similar to CSCsi27767 which was opened and resolved against the cat6k's Communications Media Module (CMM). But the fix for CSCsi27767 was only intended for the CMM platform.

Workarounds:

User-Level Workaround: A hold/resume from the phone receiving the out-of-sequence RTP audio packets will restore normal reception of audio.

System-Level Workarounds:

1. If possible, use a CMM module for transcoding while ensuring that IOS version on the CMM module has the fix for CSCsi27767.

2. If possible, eliminate the need for a trancoder in the audio path for affected call flows.

3. This problem does not affect Cisco IOS Software Media Termination Points (MTPs) nor SW MTPs hosted on a Cisco Unified Communications Manager (CUCM) server. So, if like-to-like capabilities (for example, codec and packetization) are being used, then using a SW MTP via Cisco IOS or CUCM may be an option.