Caveats for Cisco IOS Release 15.1(2)T

Caveats

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats, and only select severity 3 caveats are included in this section.

In this section, the following information is provided for each caveat:

- Symptoms—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.

Note If you have an account on Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com and go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl. (If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)

This document contains the following sections:

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Resolved Caveats—Cisco IOS Release 15.1(2)T5

Cisco IOS Release 15.1(2)T5 is a rebuild release for Cisco IOS Release 15.1(2)T. The caveats in this section are resolved in Cisco IOS Release 15.1(2)T5 but may be open in previous Cisco IOS releases.

- CSCsh39289

  Symptoms: A router may crash under a certain specific set of events.

  Conditions: The crash may happen under a combination of unlikely events when an IPv6 PIM neighbor that is an assert winner expires.

  Workaround: There is no obvious workaround, but the problem is unlikely to occur.

- CSCso41274

  Symptoms: A router crashes or shows the following traceback:

  ```
  % Not enough DSP resources available to configure ds0-group 1 on controller
  T1 1/0
  % The remaining dsp resources are enough for 14 time slots.
  % For current codec complexity, 1 extra dsp(s) are required to create this
  voice port.
  sip-cme(config-controller)#
  %ALIGN-3-SPURIOUS: Spurious memory access made at 0x40C627A8  reading 0x4
  %ALIGN-3-TRACE: -Traceback= 0x40C627A8 0x40D6769C 0x40D7281C 0x40D72E74
  0x4036B0E4 0x4036D4B4 0x414C78EC 0x414EB3FC
  ```

  Conditions: The symptom is observed on a router that has enough DSP resources to set up 14 signaling channels. When trying to configure a ds0-group for the 16 time-slot, you may get an error message that not enough DSP resources are available. Immediately after that the router shows the traceback or may crash.

  Example:

  ```
  sip-cme(config)#controller t1 1/0
  sip-cme(config-controller)#ds0-gr 1 time 1-16 type e&m-imm
  sip-cme(config-controller)#ds0-gr 1 time 1-16 type e&m-immediate-start
  ```

  Workaround: Ensure there are more DSPs in the router than signalling channels.

- 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.

- CSCsv30540

  Symptoms: The error message %SYS-2-CHUNKBOUNDSIB and a traceback are seen.

  Conditions: These symptoms are observed when the **show running-config/write memory** command is issued.

  Workaround: There is no workaround.

- CSCta11223

  Symptoms: A Cisco router may crash when the **show dmvpn** or **show dmvpn detail** commands are entered.

  Conditions: This symptom is observed when the device is running Cisco IOS and configured with DMVPN. The crash occurs when the **show dmvpn** or **show dmvpn detail** commands are entered two or more times.

  Workaround: There is no known workaround.

- CSCtb72734

  Symptoms: DHCP OFFER is not reaching the client when the unicast flag is set.

  Conditions: This symptom occurs only on ASR devices where creation or removal of the ARP entry does not maintain sequential ordering. As a result, the packet could arrive at the forwarding plane after the ARP entry has already been removed or before the ARP entry has been created.

  Workaround: There is no workaround.

- CSCtd15853

  Symptoms: When removing the VRF configuration on the remote PE, the local PE receives a withdraw message from the remote PE to purge its MDT entry. However, the local PE does not delete the MDT entry.

  Conditions:

  - mVPN is configured on the PE router.
  - Both Pre-MDT SAFI and MDT-SAFI Cisco IOS software is running in a Multicast domain.

  Multicast VPN: Multicast Distribution Trees Subaddress Family Identifier:

  http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6557/ps6604/ps6651/prod_white_paper0900aecd80581f3d.html

  Workaround: There is no workaround.

- CSCte53162

  Symptoms: In radius messaging, nas-port-id is not prepended to “acct-session- id” when the **nas-port format e** *encoding string* command is configured.

  Conditions: This symptom is observed when the **nas-port format e** *encoding string* command is configured.

  Workaround: Use the **nas-port format d** *encoding bits* command.

- CSCtf71673

  Symptoms: A Cisco router shows a PRE crash.

  Conditions: This issue is seen when the system is configured for PTA and L2TP access and running Cisco IOS Release 12.2(34)SB4 during a pilot phase.

  Workaround: There is no workaround.

- 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

- CSCtg72481

  Symptoms: Spurious memory access is seen with QoS configurations.

  Conditions: The symptom is observed only when sending the traffic for a while.

  Workaround: There is no workaround.

- CSCtg83804

  Symptoms: Router crashes when uploading or downloading files via WebVPN.

  Conditions: This symptom is observed on a Cisco 870 router, WebVPN, and BVI configuration.

  Workaround: There is no workaround.

- CSCth13415

  Symptoms: One way audio in call transfer due to 491 response during resume re- INV.

  Conditions: The symptom is observed when you have an UPDATE message passing through the CUBE and then a re-INV crossover happens. The re-INV crossover results in a 491 but the 491 is not correctly forwarded by the IPIP GW. This can result in one way audio issues if the crossed over re-INV was changing the media state from hold to resume.

  Workaround: There is no workaround.

- CSCth40506

  Symptom: A Cisco voice gateway does not have its GigabitEthernet link connected to the network, but the call is not cleared from the PRI when the Application Ack Timer expires.

  Conditions: This symptom is observed on a Cisco 2911 voice gateway with Cisco IOS Release 15.0(1)M and a Cisco 2951 voice gateway with Cisco IOS Release 15.0(1)M1.

  Workaround: There is no workaround.

  Further Problem Description: When a voice call is placed, a SIP INVITE is sent:

  ```
  -- Sent: INVITE sip:x@x.x.x.x:5060 SIP/2.0 --
  ```
  Because the Cisco gateway does not have network connectivity, no SIP reply is received from the network. Sixty seconds later, the Application Ack Timer expires:

  ```
  -- ISDN Se1/0:15 **ERROR**: CCPCC_TApplnAckExpiry: Application Ack Timer expired. b
  channel 1 cref 0x8021 call_id 0x0045
  ```
  The call, however, is not cleared from the PRI.

- CSCth45432

  Symptoms: Traffic that is CEF-switched through the router does not exit Async interfaces.

  Conditions: This symptom is observed with CEF enabled and in Cisco IOS Release 12.4(20)T and above with MFI.

  Workaround: Disable CEF or downgrade to Cisco IOS Release 12.4(15)T before MFI.

- CSCth61759

  Symptoms: In a SIP-SIP video call flow, CUBE may not correctly negotiate the video stream.

  Conditions: This symptom is observed in two scenarios:

  Scenario 1:

This symptom was observed in the following SIP-SIP Delayed Offer - Delayed Offer (DO-DO) call flow:

7985-- CUCM -- CUBE -- Tandberg VCS -- Tandberg Telepresence server

1. Call is originated by 7985
2. Tandberg Telepresence Server provides multiple video codecs in the SDP (Session Description Protocol) of the SIP "200 OK" response

```
m=video 53722 RTP/AVP 96 97 34 31
  b=AS:1920
  a=rtpmap:96 H264/90000
  a=fmtp:96 profile-level-id=42e016;max-mbps=108000;max-fs=3600
  a=rtpmap:97 H263-1998/90000
  a=fmtp:97 CIF4=1;CIF=1;CIF=1;QCIF=1
  a=rtpmap:34 H263/90000
  a=fmtp:34 CIF4=1;CIF=1;CIF=1;QCIF=1
  a=rtpmap:31 H261/90000
  a=fmtp:31 CIF=1;QCIF=1
  a=sendrecv
```

3. CUBE sets video m-line to 0 in the SDP of the SIP "ACK" response

```
m=video 0 RTP/AVP 96
```

Scenario 2: End to end SIP Flow Around call with Cisco Video Telephony Advantage (CVTA).

CVTA -- CUCM -- CUBE -- CUBE -- CUCM -- CVTA

Workaround: There is no workaround.

- CSCth66177

  Symptoms: The standby route processor (RP) triggers an active RP crash.

  Conditions: This problem is observed when the standby RP crashes due to a memory parity error.

  Workaround: There is no workaround.

- CSCth73173

  Symptoms: ASR may crash if a QoS policy applied using CoA through Service-Template is more than 256 characters in length.

  Conditions: This symptom is observed when a QoS Policy string length exceeds 256 characters.

  Workaround: Ensure that the QoS policy string length is less than 256 characters.

- CSCti01036

  Symptoms: A Cisco ASR1000 series router crashes on the Radius Process.

  Conditions: This symptom is observed on a Cisco ASR 1000 series router with Radius AAA services enabled. When the Radius server sends attributes with no information (empty VSA strings), it produces an unexpected reload on the router.

  Workaround: Prevent the AAA server from sending empty VSA strings.

- CSCti04919

  Symptoms: While unconfiguring and reconfiguring the VRF, PIM neighborship goes down in a specific scenario.

  Conditions: This symptom occurs if the PIM MDT GRE tunnel takes more time to come up compared to other interfaces in the VRF.

  Workaround: Toggle the default MDT.

- CSCti08811

  Symptoms: A router running Cisco IOS may reload unexpectedly when running commands through an Embedded Event Manager (EEM) policy.

  Conditions: This symptom is observed only with EEM policies.

  Workaround: There is no workaround.

- CSCti35326

  The Cisco IOS Software Network Address Translation (NAT) feature contains a denial of service (DoS) vulnerability in the translation of Session Initiation Protocol (SIP) packets.

  The vulnerability is caused when packets in transit on the vulnerable device require translation on the SIP payload.

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

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

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

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

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

- CSCti40660

  Symptoms: The following message is displayed:

  ```
  %FW-4-GLOBAL_SESSIONS_MAXIMUM: Number of sessions for the firewall exceeds the
  configured global sessions maximum value 2147483647
  ```
  Conditions: This symptom is observed when IP SLA is configured along with self zones.

  Workaround: There is no workaround.

- CSCti46171

  Cisco IOS Software contains four vulnerabilities related to Cisco IOS Zone-Based Firewall features. These vulnerabilities are as follows: * Memory Leak Associated with Crafted IP Packets * Memory Leak in HTTP Inspection * Memory Leak in H.323 Inspection *Memory Leak in SIP Inspection

  Workarounds that mitigate these vulnerabilities are not available.

  Cisco has released free software updates that address these vulnerabilities.

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

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 7.8/6.4:
  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C CVE ID CVE-2012-1315 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

- CSCti48014

  Symptoms: A device reloads after executing the “show monitor event <comp> ... all detail” command (where <comp> is an option listed under “show monitor event ?”).

  Conditions: This symptom is observed if the configurations are done in the order below,

  ```
  monitor event-trace <comp> stacktrace <depth>
  monitor event-trace <comp> size <size value>
  ```
  and any related event gets recorded in between the above two configurations.

  Workaround: To avoid the crash, change the order of the above configurations; that is, configure the “size” command first and then configure the “stacktrace” command.

- 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

- CSCtj46670

  Symptoms: IPCP cannot complete after dialer interface is moved out of standby mode. CONFREJ is seen while negotiating IPCP.

  Conditions: The symptom is observed when a dialer interface has moved out from standby mode.

  Workaround: Reload the router.

- CSCtj48387

  Symptoms: After a few days of operation, a Cisco ASR router running as an LNS box, crashes with DHCP related errors.

  Conditions: This symptom occurs when DHCP enabled and sessions get DHCP information from a RADIUS server.

  Workaround: There is no workaround.

- CSCtj56551

  Symptoms: The Cisco 7600 crashes in a very rare case.

  Conditions: This symptom is observed very rarely when route-churn/sessions come up.

  Workaround: There is no workaround.

- CSCtj79769

  Symptoms: LC crashes.

  Conditions: When disabling MLD snooping on an interface or disabling IPv6 multicast in general.

  Workaround: There is no workaround.

- CSCtj95685

  Symptoms: A router configured as a voice gateway may crash while processing calls.

  Conditions: The symptom is observed with a router configured as a voice gateway.

Workaround: There is no workaround.

- CSCtk32975

  Symptoms: The system crashes.

  Conditions: This symptom occurs when traffic is flowing through the device and fair-queue is configured on ATM PVC.

  Workaround: There is no workaround.

- CSCtl52854

  Symptoms: Client does not receive multicast traffic when it is connected to an EHWIC port in access mode.

  Conditions: The symptom is observed when a multicast server is connected to an EHWIC L2 interface.

  Workaround: Connect the multicast server to an on-board gig interface.

- CSCtn04357

  Symptoms: When applying the following netflow configuration in the same sequence, the standby supervisor module continuously reloads:

  ```
  vlan configuration 161
  ip flow monitor flowmonitor1 in
  ip flow monitor flowmonitor1 input
  ```

  Conditions: The symptom is observed on a Sup7-E that is running Cisco IOS XE Release 3.1.0(SG). The router must have a redundant RP. The monitor must be using a flow record that does not conform to V5 export format while being used with V5 exporter and be running on a distributed platform. When the flow monitor is applied to an interface the config sync will fail and the standby will reload.

  Workaround 1: Remove the flow monitor configuration.

  Workaround 2: Use netflow-v9 export protocol.

  Workaround 3: Use a record format exportable by netflow-v5.

- CSCtn16855

  Symptoms: The Cisco 7200 PA-A3 cannot ping across ATM PVC.

  Conditions: This symptom occurs due to a high traffic rate, and the output policy applied under PVC.

  Workaround: There is no workaround. Removing the policy will resolve this issue, but the QoS functionality will not be present in this case.

- CSCtn58128

  Symptoms: BGP process in a Cisco ASR 1000 router that is being used as a route reflector may restart with a watchdog timeout message.

  Conditions: The issue may be triggered by route-flaps in scaled scenario where the route reflector may have 4000 route reflector clients and processing one million+ routes.

  Workaround: Ensure “no logging console” is configured.

- CSCtn62287

  Symptoms: The standby router may crash while flapping the interface or while doing soft OIR of the SPA.

  Conditions: This symptom is observed when interfaces are bundled as a multilink and traffic flows across the multilink.

  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.

- CSCtn65116

  Symptoms: Some VPNv4 prefixes may fail to be imported into another VRF instance after a router reload or during normal operation.

  Conditions: The symptom is observed with a router that is running BGP and Cisco IOS Release 12.2(33)SB or Release 12.2(33)SRB or later. Earlier versions are not affected. This occurs with the same prefixes with different mask lengths, e.g.: 10.0.0.0/24 and 10.0.0.0/26 (but not for 10.0.0.0/24 and 10.0.0.1/32, because 10.0.0.0 is not the same prefix as 10.0.0.1). It is seen with the following process:

  1. Assume the prefix, 10.0.0.0/24, is imported from VPNv4 to VRF. It has been allocated a label of 16.
  2. The allocated label changes from 16 to 17, e.g.: due to interface flapping or BGP attribute change.
  3. However, before the BGP import happens, a more specific prefix (e.g.: 10.0.0.0/26) is added to the BGP radix tree, but it is denied for importing due to, say, RT policy.

  Workaround: Remove RT or import map and add it back. Note, however, that if the above conditions occur again, the issue could reappear.

- CSCtn74673

  Symptoms: After reload, incoming mcast traffic is punted into the CPU before MFIB is downloaded into line cards. Due to the CPU rate being high, the line cards are stuck in a continual loop of failing to complete MFIB download.

  Conditions: This symptom is observed when high CPU utilization is caused by multicast traffic and the **show mfib linecard** does not show cards in sync and tables are in “connecting” state. The **clear mfib linecard** command does not correct the line card table states.

  Workaround: There is no workaround other than line card reload.

- CSCto55643

  Symptoms: High CPU loading conditions can result in delayed download of multicast routes to line cards, resulting in multicast forwarding (MFIB) state on line cards out of sync with the RP. The **show mfib linecard** command shows line cards in sync fail state with many in LOADED state.

  Conditions: This symptom occurs during high CPU loading due to router reload or line card OIR events in a highly scaled multicast environment with high line rates of multicast traffic and unrestricted processed switched packets, before HW forwarding can be programmed.

  Workaround: There is no workaround. Ensure that mls rate limits are properly configured.

  Further Problem Description: IPC errors may be reported in the MRIB Proxy communications channel that downloads multicast routes to line cards.

- CSCto55983

  Symptoms: After reload, incoming mcast traffic is punted into the CPU before MFIB is downloaded into line cards. Due to the high CPU rate, line cards are stuck in a continual loop of failing to complete MFIB download and retrying.

Conditions: This symptom occurs during high CPU utilization caused by multicast traffic. The **show mfib line summary** command does not show cards in sync.

Workaround: There is no workaround.

- CSCto63268

  Symptoms: A Cisco 3900e router may crash while configuring a PRI-group on a VWIC2 in a native HWIC slot.

  Conditions: The router must be a Cisco 3900e and the number of timeslots in the new PRI-group must be greater than the number of available DSPs. Additionally, a EVM-HD-8FXS/DID must be installed and the onboard DSPs must be configured for DSP sharing.

  Workaround: Remove the EVM or disable DSP sharing.

- CSCto72480

  Symptoms: The output of the **show mfib linecard** command shows that line cards are in "sync fail" state.

  Conditions: This symptom occurs usually when the last reload context displayed in the **show mfib linecard internal** command output is "epoch change". This indicates that an IPC timeout error has occurred in the MRIB communications channel that downloads multicast routing entries to the multicast forwarding information base (MFIB). In this condition, multicast routing changes are not communicated to the failed line cards and they are not in sync with the RP.

  Workaround: If this issue is seen, using the **clear mfib linecard** *slot* command may clear the problem. If the problem occurs on a Cisco 7600 SP, an RP switchover is required after clearing the problem on any affected line cards. The workaround may not completely work if high CPU loading continues to be present and IPC errors are reported.

  Further Problem Description: The IPC timeout errors could result from high CPU loading conditions caused by high rates of processed switched packets. High rates of multicast processed switched packets can be avoided if rate limits are applied after each router boot, especially after using the **mls rate-limit multicast ipv4 fib-miss** command.

- CSCto72629

  Symptoms: A MAXAGE LSA is repeatedly retransmitted bringing down the OSPFv3 adjacency.

  Conditions: This symptom occurs when the unadjusted age of the LSA in the OSPFv3 database (as opposed to the advertised age, which includes time spent in the database) is less than MAXAGE. Note that the age of the LSA in the database is not updated once it is installed unless maxaging is initiated by OSPFv3 process.

  Workaround: Use the **clear ipv6 ospf process** command to clear the OSPF state based on the OSPF routing process ID.

- CSCto72927

  Symptoms: Configuring an event manager policy may cause a Cisco router to stop responding.

  Conditions: This issue is seen when a TCL policy is configured and copied to the device.

  Workaround: There is no workaround.

- CSCto99523

  Symptoms: Convergence can take more time if there are a lot of VRF/routes and aggregation is configured in many VRFs. Massive route churn happens (for example, session reset with RR).

  Conditions: Convergence can take more time if there are a lot of VRF/routes and aggregation is configured in many VRFs. Massive route churn happens (for example, session reset with RR). There is no functionality impact.

Workaround: There is no workaround.

- CSCtq04117

  Symptoms: DUT and RTRA have IBGP-VPNv4 connection that is established via loop back. OSPF provides reachability to BGP next hop, and BFD is running.

  Conditions: This symptom occurs under the following conditions:

  1. DUT has learned VPNv4 route from RTRA, and the same RD import is done at DUT.
  2. When switchover is performed in RTRA and when GR processing is done, the route is never imported to VRF.

  Workaround: Use the **clear ip route vrf x *** command.

- CSCtq12007

  Symptoms: Using a c7200 VSA in a 15.0M image, when there are multiple shared IPsec tunnels using the same IPsec protection policy, removing the policy from one tunnel could cause other tunnels to stop working until the next rekey or tunnel reset.

  Using a c7200 VSA in a 15.1T or 15.2T image, you can also see a similar problem but one that is less sever; you may see one every other packet drop, until the next rekey or tunnel reset.

  Conditions: In a 15.0M, 15.1T, and 15.2T image, VSA is used as the crypto engine.

  Workaround: Force a rekey after removing the shared policy from any shared tunnels by using the **clear crypto session** command or resetting all the tunnels.

- CSCtq21234

  Symptoms: Label is not freed.

  Conditions: The symptom is observed after shutting down the link.

  Workaround: There is no workaround.

- CSCtq24557

  Symptoms: Router crash after deleting multiple VRFs. This happens very rarely.

  Conditions: The symptom is observed in a large scale scenario.

  Workaround: There is no workaround.

- CSCtq24733

  Symptoms: VXML gateway crash with “Unexpected exception to CPU: vector C”.

  Conditions: The symptom is observed with MRCP is enabled.

  Workaround: There is no workaround.

- CSCtq32896

  Symptoms: LSM entries stop forwarding traffic.

  Conditions: This symptom is observed after Stateful Switchover (SSO).

  Workaround: There is no workaround.

- CSCtq36153

  Cisco IOS Software contains four vulnerabilities related to Cisco IOS Zone-Based Firewall features. These vulnerabilities are as follows: * Memory Leak Associated with Crafted IP Packets * Memory Leak in HTTP Inspection * Memory Leak in H.323 Inspection * Memory Leak in SIP Inspection

  Workarounds that mitigate these vulnerabilities are not available.

  Cisco has released free software updates that address these vulnerabilities.

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

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 7.8/6.4:
https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C CVE ID CVE-2012-0387 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

- CSCtq45553

  Cisco IOS Software contains four vulnerabilities related to Cisco IOS Zone-Based Firewall features. These vulnerabilities are as follows:

  * Memory Leak Associated with Crafted IP Packets * Memory Leak in HTTP Inspection * Memory Leak in H.323 Inspection *Memory Leak in SIP Inspection

  Workarounds that mitigate these vulnerabilities are not available.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-zbfw
  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 7.8/6.4:
  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C CVE ID CVE-2012-0388 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

- CSCtq49325

  Symptoms: A router reloads when a graceful shutdown is done on EIGRP.

  Conditions: The router reload occurs only when multiple EIGRP processes redistributing each other run on two redundant LANs and a graceful shutdown is done on both EIGRP processes simultaneously.

  Workaround: Redundant LANs may not be necessary in first place. If it is required, if mutual redistribution is done, then while doing graceful shutdown, sufficient time should be given for one process to be shutdown completely before executing the second shutdown command. This should resolve the problem.

  Further Problem Description: In a normal scenario, a zombie DRDB or path entry (a temporary DRDB entry which is deleted as soon as processing of the packet is done) would be created only for reply message. But here, due to the redundancy in LAN and EIGRP processes in this scenario, a query sent on one interface comes back on the other which causes this zombie entry creation for the query also. In the query function flow it is expected that this zombie entry will not be deleted immediately, rather it is to be deleted only after a reply for the query is sent successfully. At this point, (i.e.: before a reply is sent) if a shutdown is executed on the EIGRP process, then all the paths and prefixes will be deleted. If a particular path is threaded to be sent - in this case it is scheduled for a reply message - the path is not deleted and an error message is printed. However the flow continues and the prefix itself is deleted. This results in a dangling path without the existence of any prefix entry. Now when the neighbors are deleted, the flushing of the packets to be sent will lead to crash since it does not find the prefix corresponding to the path. The solution is to unthread from the

paths from sending before deletion. A similar condition will occur if the packtization timer expiry is not kicked in immediately to send the DRDBs threaded to be sent and a topology shutdown flow comes to execute first.

- CSCtq55173

  Symptoms: A device that is configured with NAT crashes. SIP appears to be translated trough NAT. However, some cases report that the crash still occurs after redirecting SIP traffic elsewhere.

  Conditions: The crash is triggered when the **clear ip nat translation ***, **clear ip nat translation forced**, or **clear crypto ipsec client ezvpn** command is entered.

  Workaround: There is no workaround.

- CSCtq58383

  Symptoms: A crash occurs when modifying or unconfiguring a loopback interface.

  Conditions: This symptom occurs while attempting to delete the loopback interface, after unconfiguring the “address-family ipv4 mdt” section in BGP.

  Workaround: Unconfiguring BGP may prevent the issue from happening without reloading the router.

- CSCtq59923

  Symptoms: OSPF routes in RIB point to an interface that is down/down.

  Conditions: This symptom occurs when running multiple OSPF processes with filtered mutual redistribution between the processes. Pulling the cable on one OSPF process clears the OSPF database, but the OSPF routes associated with the OSPF process from that interface still point to the down/down interface.

  Workaround: Configure “ip routing protocol purge interface”.

- CSCtq62759

  Symptoms: CLNS routing table is not updated when LAN interface with CLNS router isis configured shuts down because ISIS LSP is not regenerated. CLNS route will be cleared after 10 minutes when isis ages out the stale routes.

  Conditions: This symptom is seen when only CLNS router ISIS is enabled on LAN interface. If IPv4/IPv6 ISIS is enabled, ISIS LSP will be updated.

  Workaround: Use the **clear clns route** command or the **clear isis *** command.

- CSCtq75008

  Symptoms: A Cisco 7206 VXR crashes due to memory corruption.

  Conditions:

  - The Cisco 7206 VXR works as a server for L2TP over IPsec.
  - Encryption is done using C7200-VSA.
  - More than two clients are connected.

  If client sessions are kept up for about a day, the router crashes.

  Workaround: There is no workaround.

- CSCtq77274

  Symptoms: FXS phones are not recognized as SCCP endpoints.

  Conditions: This symptom occurs when FXS phones are configured as SCCP endpoints.

  Workaround: There is no workaround.

- CSCtq78217

  Symptoms: A router crashes with the following information:

  ```
  System returned to ROM by address error at PC 0xZZZZZZZZ, address 0xZZZZZZZZ
  ```

  Conditions: The symptom is observed with CUBE + SIP.

  Workaround: There is no workaround.

- CSCtq80648

  Symptoms: If a user changes the VRF assignment, such as moving to another VRF, removing the VRF assignment, etc., on which a BGP ipv6 link-local peering (neighbor) is based, the BGP IPv6 link-local peering will no longer be able to delete or modify.

  For example:

  ```
  interface Ethernet1/0
    vrf forwarding vpn1
     ipv6 address 1::1/64
  !
   router bgp 65000
    address-family ipv6 vrf vpn1
     neighbor FE80::A8BB:CCFF:FE03:2200%Ethernet1/0 remote-as 65001
  ```

  If the user changes the VRF assignment of Ethernet1/0 from vpn1 to vpn2, the IPv6 link-local neighbor, FE80::A8BB:CCFF:FE03:2200%Ethernet1/0, under address-family ipv6 vrf vpn1, will no longer be able to delete or modify.

  Rebooting the router will reject this configuration. Also, if a redundant RP system and the release support config-sync matching feature, it will cause config-sync mismatch and standby continuous reload.

  Conditions: This symptom occurs when a user changes the VRF assignment.

  Workaround: Remove the BGP IPv6 link-local peering before changing the VRF assignment on the interface.

- CSCtq83629

  Symptoms: The error message is associated with a loss in multicast forwarding state on line cards under scaled conditions when an IPC error has occurred.

  Conditions: This symptom is observed during router boot or high CPU loading, which can cause IPC timeout errors. This issue is seen on line cards during recovery from an IPC error in the MRIB channel.

  Workaround: Line card reload is required to resolve the problem.

- CSCtq85728

  Symptoms: An EHWIC-D-8ESG card is causing an STP loop.

  Conditions: EHWIC-D-8ESG might not be blocking appropriate ports according to calculated STP topology that introduces the loop in the network.

  Workaround: There is no workaround.

- CSCtq88777

  Symptoms: VDSL controller and ATM interface remains up, however ATM PVC becomes inactive and virtual interface goes down.

  Conditions: The symptom is observed when the ATM PVC becomes inactive causing the virtual interface to go down.

  Workaround: Use a VBR-NRT value that is lower than trained upstream speed.

- CSCtq92182

  Symptoms: An eBGP session is not established.

  Conditions: This issue is observed when IPv6 mapped IPv4 addresses are used, such as ::10.10.10.1.

  Workaround: Use an IPv6 neighbor address with bits. Set some higher bits along with the IPv4 mapped address.

- CSCtq92940

  Symptoms: An active FTP transfer that is initiated from a Cisco IOS device as a client may hang.

  Conditions: This symptom may be seen when an active FTP connection is used (that is, the **no ip ftp passive** command is present in the configuration) and there is a device configuration or communication issues between the Cisco IOS device and the FTP server, which allow control connections to work as expected, but stopping the data connection from reaching the client.

  Workaround: Use passive FTP (default) by configuring the **ip ftp passive** command.

  Further Problem Description: Please see the original bug (CSCtl19967) for more information.

- CSCtq96329

  Symptoms: Router fails to send withdraws for prefixes, when bgp deterministic-med is configured. This could lead to traffic blackholing and routing loops. Could also result in memory corruption/crash in rare conditions.

  Conditions: This symptom can happen only when bgp deterministic-med is configured.

  The following releases are impacted:

  - Cisco IOS Release 15.0(1)S4
  - Cisco IOS Release 15.1(2)T4
  - Cisco IOS Release 15.1(3)S
  - Cisco IOS Release 15.2(1)T

  Workaround: Disable deterministic med in the network/AS by issuing the **no bgp deterministic-med** command and then the **clear ip bgp *** command or hardreset of BGP session to remove any stale prefixes.

  It is further recommended to do a SSO on routers that are running impacted software to eliminate any potential corruption that might have already existed on routers that are running impacted software.

  Further Problem Description: If deterministic med is enabled, withdraws are not sent.

- CSCtr04829

  Symptoms: A device configured with “ip helper-address” drops packets because of a zero hardware address check.

  Conditions: This symptom occurs when the hardware address is zero.

  Workaround: There is no workaround.

- CSCtr11620

  Symptoms: In a simple HSRP setup with Cisco 2900 devices, a ping to the virtual IP address fails intermittently.

  Conditions: This symptom is observed when a Cisco 2911 is used.

  Workaround: Replace the Cisco 2900 with a Cisco 18XX or Cisco 1941.

- 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.

- CSCtr18574

  Symptoms: H323-H323 video calls fail with cause code 47.

  Conditions: The symptom is observed when an H323-H323 video call fails to establish an H245 media connection. The following errors are seen:

  ```
  Received event H225_EV_H245_FAILED while at state H225_WAIT_FOR_H245
  cch323_send_passthru_out: Send passthru message retcode 15
  ```

  Workaround: There is no workaround.

- CSCtr26373

  Symptoms: Interface bounces and, after coming back up, hangs and does not pass traffic. The rx ring is stuck and it may be observed that all packets coming into the interface are counted as “input errors”.

  Conditions: This has been observed on onboard GE interfaces of Cisco 39xx and Cisco 2951 routers. It may be seen at random times and has thus far been observed to happen after an interface bounce. The interface will still show “up/up” in the **show interface** output.

  Workaround: Bounce the interface again to restore service.

- 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

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

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

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

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

- CSCtr29338

  Symptoms: A router crashes.

Conditions: The symptom is observed after an %ISDN-6-DISCONNECT message from “unknown” followed by a couple of “Illegal Access to Low Address” messages.

Workaround: There is no workaround.

- CSCtr44686

  Symptoms: There is a crash after matching traffic and resetting the connection using following maps:

```
policy-map type inspect smtp SMTP_L7_P1
 class type inspect smtp SMTP_L7_C1
  reset
policy-map type inspect smtp SMTP_L7_P2
 class type inspect smtp SMTP_L7_C2A
  reset
 class type inspect smtp SMTP_L7_C2B
  reset
```

  Conditions: The symptom is observed with the above maps.

  Workaround: Replace “reset” with “log”.

- CSCtr45608

  Symptoms: Referring an IPv6-only VRF on a route-map crashes the router.

  Conditions: The symptom is observed on a Cisco Catalyst 4000 Series Switch when “set vrf” is configured on the route-map and the VRF is IPv6 only.

  Workaround: Configure “ipv4 vrf” along with “ipv6 vrf” and refer “ipv6 vrf” on the route-map by configuring “ipv6 policy” on the ingress interface.

- CSCtr46123

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

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

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

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

- 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

- CSCtr51926

  Symptoms: IPv6 packets are not classified properly in a subinterface when a service-policy is applied on the main interface.

  Conditions: The symptom is observed when a service-policy is applied on the main interface.

Workaround 1: Enable IPv6 explicitly on the main interface:

```
interface x/y
  ipv6 enable
```

Workaround 2: Reconfigure the IPv6 address on the subinterface:

```
interface x/y.z
  no ipv6 address
  ipv6 address ...
```

- CSCtr54269

  Symptoms: CUBE sends an RTCP BYE message to MS OCS R2, causing loss of audio for about 20 seconds.

  Conditions: CUBE sends an RTCP BYE message only upon reINVITE due to session refresh timer.

  Workaround: Downgrade to Cisco IOS Release 12.4(22)YB.

- CSCtr54327

  Symptoms: A Cisco router may crash due to a SegV exception or may have spurious access when a fax comes in.

  Conditions: This symptom is observed on a voice gateway that is configured with transcoding and fax passthrough. When a fax call comes in for a codec, but is not configured for a codec, then the "a=silenceSupp:off" option is set in SDP.

  Workaround: Disable fax by going into the "voice service voip" mode and configuring the **fax protocol none** command.

- CSCtr58140

  Symptoms: PFR-controlled EIGRP route goes into Stuck-In-Active state and resets the neighbor.

  Conditions: This symptom is observed when the PFR inject route in an EIGRP topology table after the policy decision. The issue was first seen on an MC/BR router running PFR EIGRP route control and with EIGRP neighbors over GRE tunnels.

  Workaround: There is no workaround.

- CSCtr79347

  Symptoms: A router crashes at BGP task without a BGP configuration change or BGP neighbor up/down event.

  ```
  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = BGP Task
  Traceback summary % 0x80e7b6 : __be_bgp_tx_walker_process % 0x80e3bc :
  __be_bgp_tx_generate_updates_task % 0x7f8891 : __be_bgp_task_scheduler
  ```

  Conditions: No conditions but this is a rarely observed issue.

  Workaround: There is no workaround.

- CSCtr86328

  Symptoms: A device running Cisco IOS might reload when the web browser refreshes/reloads the SSL VPN portal page.

  Conditions: Cisco IOS device configured for clientless SSL VPN.

  Workaround: None.

  Further Problem Description: This problem has been seen when the stock Android browser visits the SSL VPN portal (after authentication) and refreshes (reloads) the page. However, the issue is not browser-specific and other browsers might trigger the issue too.

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 6.8/6.5: 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:U/RC:C

CVE ID CVE-2012-1344 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

- CSCtr86437

  Symptoms: NAT-PT function does not work properly after an interface flap occurs.

  Conditions: The symptom is observed when you configure NAT-PT on the router.

  Workaround: Reconfigure "ipv6 nat prefix."

- CSCtr88739

  Symptom 1: Routes may not get imported from the VPNv4 table to the VRF. Label mismatch may also be seen.

  Symptom 2: The routes in BGP may not get installed to RIB.

  Conditions: The symptoms are only observed with routes with the same prefix, but a different mask length. For example, X.X.X.X/32, X.X.X.X/31, X.X.X.X/30 ..... X.X.X.X/24, etc. These issues are not easily seen and are found through code walkthrough.

  For symptom 1, each update group is allocated an advertised-bit that is stored at BGP net. This issue is seen when the number of update groups increases and if BGP needs to reallocate advertised-bits. Also, this symptom is observed only with a corner case/timing issue.

  For symptom 2, if among the same routes with a different prefix length, if more specific routes (15.0.0.0/32) do not have any bestpath (for example, due to NH not being reachable or inbound policy denying the path, but path exists due to soft-reconfiguration), then even if a less specific route (15.0.0.0/24) has a valid bestpath, it may not get installed.

  Workaround for symptom 1: Remove "import-route target" and reconfigure route-target.

  Workaround for symptom 2: Clear ip route x.x.x.x to resolve the issue.

- 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

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

- CSCtr97640

  Symptoms: Start-up configuration could still be retrieved bypassing the “no service password-recovery” feature.

  Conditions: None.

  Workaround: None--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

- CSCts16285

  Symptoms: The system may experience delays in updating multicast information on the line cards. MFIB/MRIB error messages may be observed when IPC messages from the line card to the RP time out. In the worst case, the line card may become disconnected if timeouts continue for a long period.

  Conditions: This symptom occurs when the system has a very heavy IPC load or CPU load.

  Workaround: Take necessary actions, if possible, to reduce the IPC load. Sometimes, the IPC load could be due to noncritical processes.

- CSCts28315

  Symptoms: A DHCP PD request does not accept a specific server.

  Conditions: The symptom is observed because the router does not include any IA Prefix option in Request message. This is correct behavior of RFC:

  http://tools.ietf.org/html/rfc3633#section-10

  A requesting router may set the IPv6 prefix field to zero and a given value in the prefix-length field to indicate a preference for the size of the prefix to be delegated.

  Workaround: There is no workaround.

- CSCts33952

  Symptoms: An rsh command fails from within TclScript. When rsh command constructs are used within TclScript, bad permissions are returned and the rsh aspect fails to execute, causing the script to fail.

  Conditions: This symptom is observed in Cisco IOS releases after 12.4(15)T14.

  Workaround: There is no workaround.

- 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

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

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

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

- CSCts39535

  Symptoms: BGP IPv6 routes that originate from the local router (via network statements or redistribute commands) fail to match any specified condition in an outbound route map used on a neighbor statement, regardless of the expected matching results. Thus, the route map may not be applied correctly, resulting in erroneous filtering or advertising of unintended routes.

  Further testing revealed that the “suppress-map” and “unsuppress-map” commands (used in conjunction with the “aggregate-address” command) are also broken, in the sense that the route-map filtering will fail to correctly suppress or unsuppress a subnet under the aggregated prefix.

  Conditions: An outbound route map with a match statement is used in a “neighbor” statement for an IPv6 or VPNv6 neighbor in BGP, and there are locally originated routes, either through network statements or by redistribution. All “match” statements except for “as-path”, “community,” and “extcommunity” are impacted; this includes match ipv6 address, protocol, next-hop, route-source, route-type, mpls, tag.

  Workaround: None for the same router. However, inbound route maps work fine, so configuring inbound route maps on the neighboring router can compensate.

  Another way to handle it would be to configure prefix lists directly on the network statement. So filtering will be preserved. But, there will not be a way to “set” anything as route maps can typically do.

- CSCts40771

  Symptoms: Device goes into a hang state and requires a power cycle. If “scheduler isr-watchdog” is configured, the device will crash and reload the system.

  Conditions: This issue has been seen with “ip nbar protocol-discovery” configured on tunnel interfaces.

  Workaround: Remove “ip nbar protocol-discovery” from the device.

- CSCts59014

  Symptoms: Only one ATM VC shaper token is updated per cycle in a high-scale scenario.

  Conditions: This symptom is observed with HQOS on ATM VC with many ATM VCs per interface.

  Workaround: There is no workaround.

- CSCts64539

  Symptoms: The BGP next hop is inaccessible. The **show ip route** command output in the global and VRF routing tables shows that the next hop is reachable. The **show ip bgp vpnv4 all attr next-hop** command output shows max metric for the next hop.

  Conditions: This symptom occurs when an import map uses the “ip vrf name next-hop” feature while importing single-hop eBGP routes from the global routing table to the VRF routing table.

  Workaround 1: If “set ip next-hop” is not configured in import route map, this issue does not occur.

  Workaround 2: If “neighbor x.x.x.x ebgp-multihop” is configured, this issue does not occur. The knob needs to be configured for all eBGP peers, where routes are imported to the VRF with “set ip next-hop”.

  Workaround 3: If “neighbor x.x.x.x disable-connected-check” is configured for a single-hop eBGP, this issue does not occur. The knob needs to be configured for all eBGP peers, where routes are imported to the VRF with “set ip next-hop”.

- CSCts70790

  Symptoms: A Cisco 7600 router ceases to advertise a default route configured via “neighbor default-originate” to a VRF neighbor when the eBGP link between a Cisco 7600 router and its VRF eBGP peer flaps.

  Conditions: This symptom is observed when another VPNv4 peer (PE router) is advertising a default route to the Cisco 7600 router with the same RD but a different RT as the VRF in question. When the VRF eBGP connection flaps, the VRF default is no longer advertised.

  Workaround: Remove and re-add the **neighbor default- originate** command on the Cisco 7600 router and do a soft clear for the VRF neighbor.

- CSCts76410

  Symptoms: Tunnel interface with IPSec protection remains up/down even though there are active IPSec SAs.

  Conditions: The symptom is observed during a rekey when the IPSec lifetime is high and the control packets do not reach the peer. The issue was observed on Cisco IOS Release 12.4(20)T and Release 15.0(1)M7.

  Workaround: Shut/no shut the tunnel if the situation occurs. You can use EEM to recover automatically.

- CSCts80643

  Cisco IOS Software and Cisco IOS XE Software contain a vulnerability in the RSVP feature when used on a device configured with VPN routing and forwarding (VRF) instances. This vulnerability could allow an unauthenticated, remote attacker to cause an interface wedge, which can lead to loss of connectivity, loss of routing protocol adjacency, and other denial of service (DoS) conditions. This vulnerability could be exploited repeatedly to cause an extended DoS condition.

  A workaround is available to mitigate 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-rsvp

- CSCtt02313

  Symptoms: When a border router (BR) having a parent route in EIGRP is selected, “Exit Mismatch” is seen. After the RIB-MISMATCH code was integrated, RIB-MISMATCH should be seen, and the TC should be controlled by RIB-PBR, but they are not.

  Conditions: This symptom is observed when two BRs have a parent route in BGP and one BR has a parent route in EIGRP. The preferable BR is the BR which has a parent route in EIGRP. The BRs having BGP have no EIGRP configured.

  Workaround: There is no workaround.

- CSCtt11210

  Symptoms: Routers enrolled to hierarchical PKI on different subordinate CAs, may be unable to establish tunnels using IKEv1/IKEv2.

  The “debug crypto isakmp” debugs will show that the certificate-request payload contains the issuer-name of the subordinate CA certificate, not the subject-name as it would be expected.

  Conditions: The symptom is observed when the router does not have the Root CA certificate installed.

  Workaround: Install the Root CA certificate in a separate trustpoint on all involved routers.

- CSCtt17879

  Symptoms: The **bgp network backdoor** command does not have any effect.

  Conditions: This symptom occurs:

  - On 64-bit platform systems.
  - When the network is learned after the backdoor has been configured.

  Workaround: Unconfigure and reconfigure the network backdoor.

- CSCtt20215

  Symptoms: Controller goes down after reload.

  Conditions: The symptom is observed with a VWIC3-2MFT-T1E1 (in E1/CAS mode) connected to a PBX.

  Workaround: Unplug/plug the cable, or reset link from PBX side.

- CSCtt94391

  Symptoms: A Cisco wireless router may unexpectedly reboot due to a bus error with the following error leading up to the crash:

  ```
  ASSERTION FAILED: file ''../dot11t/t_if_dot11_hal_ath.c'', line XXXX
  ```

  Conditions: This issue relates to the wireless on the router. This crash can be seen on the following platforms: Cisco 870W, 1800W, UC500W, and 2800 and 3800 routers with HWIC-AP. The crash is only seen when an iPhone 4S is connected to the router. The crash has most commonly been triggered by running a video call application on the phone, but there may be other triggers. Other than the wireless configuration and other generic configurations needed to provide connectivity to the router, no other specific configuration is needed to see the crash.

  Workaround: No workaround on the router. However, this issue is not seen with an iPhone 4s running iOS 5.1. The issue is only seen on iOS 5.0.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.1/5.8:
  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:A/AC:L/Au:N/C:N/I:N/A:C/E:F/RL:U/RC:C

  CVE ID CVE-2012-1327 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

- CSCtw45055

  Symptoms: A Cisco ASR router may experience a crash in the BGP scheduler due to a segmentation fault, if BGP dynamic neighbors have been recently deleted due to link flap. For example:

  ```
  %BGP-5-ADJCHANGE: neighbor *X.X.X.X Up
  %BGP-3-NOTIFICATION: received from neighbor *X.X.X.X (hold
  time expired) x bytes
  %BGP-5-ADJCHANGE: neighbor *X.X.X.X Down BGP Notification
  received
  %BGP_SESSION-5-ADJCHANGE: neighbor *X.X.X.X IPv4 Unicast
  topology base removed from session  Neighbor deleted
  %BGP_SESSION-5-ADJCHANGE: neighbor *X.X.X.X IPv4 Unicast
  topology base removed from session  Neighbor deleted
  %BGP-5-ADJCHANGE: neighbor *X.X.X.X Up

  Exception to IOS Thread:
  Frame pointer 0x3BE784F8, PC = 0x104109AC

  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = BGP Scheduler
  ```

The scheduler process will attempt to reference a freed data structure, causing the system to crash.

Conditions: This symptom is observed when the Cisco ASR router experiences recent dynamic neighbor removals, either because of flapping or potentially by manual removal. This issue only happens when BGP dynamic neighbor is configured.

Workaround: There is no workaround.

- CSCtw99290

  Symptoms: The source or destination group-address gets replaced by another valid group-address.

  Conditions: The symptom is observed during the NVGEN process if it suspends (for example: when having a huge configuration generating the running-config for local viewing or during the saving of the configuration or during the bulk sync with the standby and the NVGEN process suspends). The global shared buffer having the address gets overwritten by another process before the NVGEN completes.

  Workaround: There is no workaround.

- CSCtx09973

  Symptoms: Voice quality on the network deteriorates after 10 minutes.

  Conditions: This symptom is observed when voice traffic is not classified properly and is classified as web or other kind of traffic.

  Workaround: There is no workaround. However, use ACL to correctly tag the traffic.

- CSCtx29543

  Symptoms: A Cisco router may crash when an IPv4 default route update occurs or when doing the **show ip route** command.

  Conditions: This symptom occurs under the following conditions:

  1. At least one IPv4 route associated with each of the 23 possible supernet mask lengths exist.
  2. A default route exists.
  3. All routes corresponding to one of the 23 possible supernet mask lengths are removed.

  The router may now crash when doing **show ip route** command or when default route is updated.

  Workaround: There are two possible workarounds:

  1. Insure that not all 23 supernet mask lengths are populated by doing route filtering.
  2. If workaround #1 is not possible, then insure that at least one supernet route for all possible mask lengths exists at all times, for example by configuring summary routes that do not interfere with normal operation.

- CSCtx32628

  Symptoms: When a primary BGP path fails, the prefix does not get removed from the BGP table on the RR/BGP peer although a withdrawal message is received.

  Conditions: This symptom is observed on an L3vpn CE which is dual homed via BGP to a PE under the following conditions:

  - BGP full mesh is configured.
  - BGP cluster-id is configured.
  - **address family vpnv4** is enabled.
  - **address family ipv4 mdt** is enabled.

  - The sending peer is only mcast RD type 2 capable, the receiving peer is MDT SAFI and RD type 2 capable.

  Workaround: Remove the cluster-id configuration or hard-reset the bgp session on the affected Cisco router. However, removing the cluster-id does not guarantee protection.

- CSCtx38806

  Symptoms: SSL VPN users lose connectivity as soon as Windows machine gets updated with security update KB2585542. This affects Cisco AnyConnect clients and may also affect IE browsers.

  This can affect any browser that has the BEAST SSL vulnerability fix, which uses SSL fragmentation (record-splitting). (Chrome v16.0.912 browser is affected for clientless WebVPN on Windows and MAC.)

  The problem affects Firefox also (version 10.0.1) displaying the following message:

  ```
  "The page isn't redirecting properly"
  ```
  Conditions: This symptom is observed on Cisco IOS that is acting as head end for SSL VPN connections.

  Workaround: Any of the following workarounds will work:

  1. Use the clientless portal to start the client. This only works in some versions of Cisco IOS.
  2. Uninstall the update.
  3. Use rc4, which is a less secure encryption option. If this meets your security needs, then you may use it as follows:

  ```
  webvpn gateway gateway name ssl encryption rc4-md5
  ```
  4. Use AC 2.5.3046 or 3.0.3054.
  5. Use older versions of Firefox (9.0.1).

  Further Problem Description: For AnyConnect users, the following user error message is seen:

  ```
  "Connection attempt has failed due to server communication errors. Please retry the
  connection"
  ```
  The AnyConnect event log will show the following error message snippet:

  ```
  Function: ConnectIfc::connect Invoked Function: ConnectIfc::handleRedirects
  Description: CONNECTIFC_ERROR_HTTP_MAX_REDIRS_EXCEEDED
  ```
  PSIRT Evaluation: The Cisco PSIRT has evaluated this issue and does not meet the criteria for PSIRT ownership or involvement. This issue will be addressed via normal resolution channels.

  If you believe that there is new information that would cause a change in the severity of this issue, please contact psirt@cisco.com for another evaluation.

  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

- CSCtx88093

  Symptoms: A dialer idle timeout is not initiated after the watched route is installed back in the routing table while using a dialer watch list, causing the watch disconnect timer to not start.

  Conditions: This symptom occurs while using the "dialer-list x protocol ip deny" command to define interesting/uninteresting traffic and while there is traffic flowing over the dialer interface.

  Workaround: Use the method that follows to define interesting traffic instead of "dialer-list x protocol ip deny":

  ```
  access-list x protocol ip deny
  dialer-list 1 protocol ip list x
  ```

- CSCty43587

  Symptoms: Crash observed with memory corruption similar to the following:

  ```
  %SYS-2-FREEFREE: Attempted to free unassigned memory at XXXXXXXX, alloc XXXXXXXX,
  dealloc XXXXXXXX
  ```

  Conditions: The symptom is observed when SIP is configured on the router or SIP traffic is flowing through it.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 15.1(2)T4

Cisco IOS Release 15.1(2)T4 is a rebuild release for Cisco IOS Release 15.1(2)T4. The caveat in this section is open in Cisco IOS Release 15.1(2)T4. This section describes only select open caveats.

- CSCtq96329

  Symptoms: Router fails to send withdraws for prefixes, when “bgp deterministic-med” is configured. This could lead to traffic blackholing and routing loops. Could also result in memory corruption/crash in rare conditions.

  Conditions: This symptom can happen only when “bgp deterministic-med” is configured.

  The following releases are impacted:

  - Cisco IOS Release 15.0(1)S4
  - Cisco IOS Release 15.1(2)T4
  - Cisco IOS Release 15.1(3)S
  - Cisco IOS Release 15.2(1)T

  Workaround: Disable deterministic med in the network/AS by issuing the **no bgp deterministic-med** command and then the **clear ip bgp *** command or hardreset of BGP session to remove any stale prefixes.

  It is further recommended to do a SSO on routers that are running impacted software to eliminate any potential corruption that might have already existed on routers that are running impacted software.

  Further Problem Description: If deterministic med is enabled, withdraws are not sent.

Resolved Caveats—Cisco IOS Release 15.1(2)T4

Cisco IOS Release 15.1(2)T4 is a rebuild release for Cisco IOS Release 15.1(2)T. The caveats in this section are resolved in Cisco IOS Release 15.1(2)T4 but may be open in previous Cisco IOS releases.

- 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.

- CSCtb24959

  Symptoms: The router may crash while clearing a large number of RP mappings.

Conditions: This symptom occurs when you configure the router as an RP agent and candidate RP for a large number of RPs. This issue is seen when you run the **clear ip pim rp-map** command several times.

Workaround: Do not run the **clear ip pim rp-map** command several times in succession.

- CSCtb74547

  Symptoms: A Cisco ASR 1000 DMVPN HUB reloads at the process IPSEC key engine.

  Conditions: This symptom is observed when the "Dual DMVPN with Shared Tunnel-Protection" feature is enabled and the interface is shut down and brought up again.

  Workaround: There is no workaround.

- CSCtd23069

  Symptoms: A crash occurs because of a SegV exception after configuring the ip virtual-reassembly command.

  Conditions: This symptom is observed on a Cisco 7206VXR router that is configured as an LNS and that is running Cisco IOS Release 12.4(15)T7 and Cisco IOS Release 12.4(24)T2.

  Workaround: There is no workaround.

- CSCte89130

  Symptoms: Router experiences a memory leak.

  Conditions: The router is running out of memory due to the CCSIP_SPI_CONTROL process (as shown by the **sh mem alloc total** command).

  Workaround: There is no workaround.

- CSCtf32100

  Symptoms: Packets are dropped.

  Conditions: This symptom is observed with router-destined traffic on an interface with VRF and crypto map configured, when the hardware is 7200 G2 with VSA.

  Workaround: There is no workaround.

- CSCtf39056

  Symptoms: RRI route will not be deleted even after IPsec SA has been deleted.

  Conditions: This symptom was first observed on the Cisco ASR1k running Cisco IOS Release 12.2(33)XND, but is not exclusive to it. The conditions are still under investigation.

  Workaround: Reload the router to alleviate this symptom temporarily. One possible workaround would be set up an EEM script to reload the device at night. In this case, the reload should occur at 3:00 a.m. (0300) in the morning. For example (the syntax may vary depending on the versions used):

```
############
configure terminal
!
event manager applet SR_000000526
event timer cron name SR_000000526 cron-entry "0 3 * * *"
action 1 cli command "en"
action 2 cli command "reload"
!
end
############
```

- CSCtf41721

  Symptoms: A DMVPNv6 hub might crash upon doing a shut/no shut on the tunnel interface of the other hub.

  Conditions: This symptom is observed with the following steps:

  1. Configure DMVPNv6 with two hubs and two spokes.
  2. Hub 2 tunnel is shut and unshut.
  3. Hub 1 crashes.

  Workaround: There is no workaround.

- CSCtg59328

  Symptoms: When IPCP renegotiates for an existing PPPoE session, the new IPv4 address does not get synced up with the standby.

  Conditions: This symptom is observed when the following tasks are completed:

  - Bring up a PPPoE session and ensure that it is synced to standby.
  - From the PPPoE client run the **no ip address** command, followed by the **ip address negotiated** command under the Virtual-template interface.
  - As part of the **no ip address** command, the session would first go down on both active and standby. The **ip address negotiated** command would then trigger IPCP renegotiation and the session would come up on active. On standby, the session remains down and the new IP address is not synced.

  Workaround: There is no workaround.

- CSCtg72652

  Symptoms: On Cisco 2900 series routers, the following warning message might display on the console:

  ```
  %ENVMON-1-POWER_WARNING: : Chassis power is not good in the PSU 1
  ```

  Conditions: Under rare conditions, the power supply sometimes sends a false alarm status to the system, even though the system power is working fine.

  Workaround: There is no workaround.

- CSCtg84969

  Symptoms: The output of the **show ip mfib vrf** *vrf-name* **verbose** command may show the line "Platform Flags: NP RETRY RECOVERY HW_ERR", and multicast traffic may not be hardware switched.

  Conditions: This symptom is observed on a dual RP Cisco 7600 series router with line cards after multiple reloads or SSOs. When the issue occurs, the output of the **show ip mfib vrf** *vrf-name* **verbose** command on the standby SP will show some lines preceded with "###" where an interface name is expected.

  Workaround: There is no workaround.

- CSCtg89555

  Symptoms: There is no forwarding interface seen in the mfib output on a DFC.

  Conditions: This symptom is observed when configuring an IP address after multicast has been configured on a dot1Q interface.

  Workaround: Performing a shut/no shut of the interface will fix the problem.

- CSCtg91572

  Symptoms: A router with an SSM (S,G) entry consisting of a NULL outgoing list sends a periodic PIM Join message to the upstream RPF neighbor, thereby pulling unnecessary multicast traffic.

  Conditions: This symptom is observed when the router has a NULL outgoing list for an SSM (S,G) entry either due to PIM protocol action (Assert) or when the router is not the DR on the downstream access interface receiving IGMPv3 reports.

  Workaround: There is no workaround.

- CSCth01526

  Symptoms: The MDT interface is deactivated and activated after an SSO.

  Conditions: This symptom occurs after an SSO, when the PIM register tunnel or MDT tunnel may go down briefly on switching to the standby RP.

  Workaround: There is no workaround.

- CSCth08505

  Symptoms: PPPoE sessions may not sync to the standby-RP.

  Conditions: This symptom is observed after the first attempt at establishing a PPPoE session fails.

  Workaround: Reloading the standby-RP may resolve this issue.

- 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat

- CSCth20018

  Symptoms: On a Cisco ISR G2 or Cisco 8xx product line, unconfiguring a subinterface (via config CLI, for example, **no interface g0/0.100** or **no interface atm0/0.100**) may sometimes crash the system.

  Conditions: This symptom occurs during basic configuration.

  Workaround: Do not unconfigure a subinterface.

- 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.

- CSCth36114

  Symptoms: A crash is seen after executing the **write memory** command via SDM.

Conditions: The symptom is observed on a Cisco 1841 platform that is running Cisco IOS Release 15.1(1)T.

Workaround: Use Cisco IOS 12.4 versions.

- CSCth37092

  Symptoms: A crash is observed in the PKI-HA feature when the standby tries to sync up with the active router.

  Conditions: This symptom occurs when the PKI server is created on the active router with a "database archive password" configuration, and the PKI server is cloned on the standby. Soon after, the active router crashes.

  Workaround: There is no workaround.

- CSCth45731

  Symptoms: PPPoE sessions get synced partially to the standby RP and later never get cleaned up. The **show** command for the sessions looks on a standby RP like the following:

```
Sby#show ppp all
Interface/ID   OPEN+ Nego* Fail-      Stage     Peer Address     Peer Name
------------   --------------------  --------   ---------------  ------------------
--
0xB400008A LCP+ CHAP+ IPV6CP+ Undefine 0.0.0.0
```

  The peer address is 0 and the interface will show the PPP handle instead of the virtual interface of PPP.

  Conditions: This symptom is seen when IPCP is getting renegotiated and terminated before the full session sync is done for the upcoming PPPoE session.

  Workaround: There is no workaround.

- CSCth46888

  Symptoms: When the ARP entry is refreshed due to timeout or use of the **clear arp** command, the router sends ARP request for cached MAC address. However, the request message does not use virtual MAC for Source (Sender) MAC.

  Conditions: This symptom is observed when the router is VRRP master and VRRP IP is configured the same as the interface IP.

  Workaround: There is no workaround.

- CSCth58576

  Symptoms: The router crashes with traceback, indicating cce_dp_named_db_sip_free_token_results_data.

  Conditions: This symptom occurs with Cisco IOS Release 15.1(2)T or later releases. This issue is seen when the device is configured with a zone-based firewall and has SIP Application inspection configured. In addition, the device is configured with "crypto" and "ip virtual-reassembly".

  Workaround: There is no workaround.

- CSCth64271

  Symptoms: Routers in redundant configuration end up in Manual Swact = disabled.

  Conditions: This symptom is observed with Cisco IOS Release 15.0(1)M2.

  Workaround: There is no workaround.

- CSCth66251

  Symptoms: You are not able to configure a policy-map for the second time in a Cisco 860 router. An “internal data base error” message is seen.

  Conditions: This symptom is observed when configuring a policy-map for the second time, and with a Cisco 860 router.

  Workaround: There is no workaround.

- CSCth74953

  Symptoms: The SPI value is shown as 0x0; hence, the ipsec sa validation is failing.

  Conditions: This symptom is observed when the crypto profiles are being applied. The symptom is not observed with simple crypto maps.

  Workaround: There is no workaround.

- CSCth85294

  Symptoms: A PIM neighborship is not established with the remote PE and RP for the MVRFs.

  Conditions: This symptom is observed with traffic, after removal and restoration of MVRFs. Traffic does not flow properly since the PIM neighborship is not established with the remote PE and RP for those MVRFs.

  Workaround: There is no workaround.

- CSCth87458

  Symptoms: Memory leak is detected in ssh_buffer_get_string.

  Conditions: This symptom occurs when you use test tool Codenomicon to test SSH verification against UUT (SSH-Server test). After the test, the memory leak is seen in ssh_buffer_get_string.

  Workaround: There is no workaround.

- CSCti06686

  Symptoms: On the Cisco 2900, the async interface drops all outbound packets.

  Conditions: This symptom is observed with data packets that are exiting the async interface through the CEF path.

  Workaround: Disable hardware framing under the async interface using the hidden command **no ppp microcode**.

- CSCti07805

  Symptoms: The router reloads @sipSPIUpdSrtpSession.

  Conditions: This symptom is observed during Hold/Resume on a basic SRTP call with Cisco IOS Release 15.1(2.3)T.

  Workaround: There is no workaround.

- CSCti18615

  Symptoms: Reloading a router which has multicast forwarding configured can result in the standby RP being out of sync with the active RP. The A and F flags are missing from the multicast forwarding base entries.

  Conditions: This symptom occurs when multicast forwarding is operational and configured in the startup configuration, and when the router is in HA mode SSO and is reloaded from the RP.

  Workaround: Perform a shut/no shut of the affected interfaces.

- CSCti22544

  Symptoms: IKE fails to come up while using RSA signature. PKI debugs show the following message:

  ```
  PKI-4-CRL_LDAP_QUERY: An attempt to retrieve the CRL from
  ldap://yni-u10.cisco.com/CN=nsca-r1 Cert Manager,O=cisco.com using LDAP has failed
  ```

  Conditions: This symptom is observed when the VRF-aware IPsec feature is used and vrf-label is configured under trustpoint; for example, crypto pki trustpoint yni-u10 enrollment url http://yni-u10:80 vrf coke.

  Workaround: There is no workaround.

- CSCti36310

  Symptoms: A Cisco ASR 1000 Series Aggregation Services router is leaking memory when IKE attributes are pulled by SNMP.

  Conditions: This symptom is observed on a Cisco ASR 1000 Series Aggregation Services router with SNMP enabled. The leak has been observed with the asr1000rp1-adventerprisek9.03.01.00.S.150-1.S and asr1000rp1-adventerprisek9.02.06.01.122-33.XNF1 images.

  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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat

- CSCti48504

  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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-sip

- CSCti64685

  Symptoms: Users may not be able to configure SLA MPLS configuration.

  Conditions: This symptom occurs when the router is booted up and may be random.

  Workaround: There is no workaround.

- CSCtj05903

  Symptoms: Some virtual access interfaces are not created for VT, on reload.

  Conditions: This symptom occurs on scaled sessions.

  Workaround: There is no workaround.

- CSCtj23189

  Symptoms: Packet drops on low rate bandwidth guarantee classes even if the offered rate is less than guaranteed rate.

  Conditions: This symptom occurs only when highly extreme rates are configured on the classes of the same policy. An example of extreme rates would be a policy-map with three classes: one with 16kbps, the second one with 1Mbps, and the third one with 99Mbps.

  Workaround: There is no workaround.

- CSCtj30155

  Cisco IOS Software is affected by two vulnerabilities that cause a Cisco IOS device to reload when processing IP version 6 (IPv6) packets over a Multiprotocol Label Switching (MPLS) domain. These vulnerabilities are:

  - Crafted IPv6 Packet May Cause MPLS-Configured Device to Reload
  - ICMPv6 Packet May Cause MPLS-Configured Device to Reload

  Cisco has released free software updates that address these vulnerabilities.

  Workarounds that mitigate these vulnerabilities are available.

  This advisory is posted at
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-ipv6mpls

- CSCtj35792

  Symptoms: The onboard GE on a Cisco 3900 (driver PQ3_TSEC) with “media-type sfp” goes to 1000/HD when it is connected by fiber to a gig port that is not doing autonegotiation.

  Conditions: This symptom is observed when the onboard GE is connected by fiber to a gig port that is not doing autonegotiation.

  Workaround: Configure autonegotiation on the other side, if possible.

  Further Problem Description: It is impossible to disable autonegotiation on the Cisco 3900 because of CSCth72105.

  The Cisco 3945E has an issue with autonegotiation in Cisco IOS Release 15.1(1)T2. This issue is not seen in Cisco IOS Release 15.1(1)T and Cisco IOS Release 15.1(4)M.

- CSCtj36521

  Symptoms: IPv4 MFIB stays enabled on interfaces even when IPv4 CEF is disabled. The output of the **show ip mfib interface** command shows the interface as configured and available, when it should be disabled.

  Conditions: This symptom is observed only if IPv6 CEF is enabled at the same time.

  Workaround: Make sure that IPv6 CEF is always disabled when running only IPv4 multicast. There is no workaround if running a mixed IPv4/IPv6 environment.

- CSCtj84234

  Symptoms: With multiple next-hops configured in the set ip next-hop clause of route-map, when the attached interface of the first next-hop is down, packets are not switched by PBR using the second next-hop.

Conditions: This symptom is seen only for packets switched in software and not in platforms where packets are PBR'd in hardware. This symptom is observed with route-map configuration, as given below:

```
route-map <RM name>
    match ip address <acl>
    set ip next-hop <NH1> <NH2>
```

Workaround: There is no workaround.

- CSCtj87846

  Symptoms: Performance Routing (PfR) traffic class fails to transition out of the default state.

  Conditions: When a subinterface is used as an external interface and the corresponding physical interface goes down and comes up, the PfR master is not notified that the subinterface is back up.

  Workaround: Do shut/no shut on PfR master or PfR border.

- CSCtj94297

  Symptoms: The "F" flag gets set in the extranet receiver MFIB forwarding entry, resulting in unexpected platform behavior.

  Conditions: This symptom is observed when the forwarding entry RPF transitions from a NULL/local interface to an interface belonging to a different MVRF.

  Workaround: Use the **clear ip mroute** command in the affected mroute.

- CSCtk02814

  Symptoms: The **show pppoe throttled subinterfaces** command output is truncated, and does not show throttled ATM VC or QinQ subinterfaces during throttling.

  Conditions: This symptom occurs when pppoe throttling is configured and active.

  Workaround: There is no workaround.

- CSCtk46363

  Symptoms: A device running Cisco IOS and acting as a DHCP server crashes.

  Conditions: This symptom is observed when a client requests a specific IP address.

  Workaround: Disable duplicate address detection check using the **ip dhcp ping packet 0** command.

- CSCtk67073

  The Cisco IOS IP Service Level Agreement (IP SLA) feature contains a denial of service (DoS) vulnerability. The vulnerability is triggered when malformed UDP packets are sent to a vulnerable device. The vulnerable UDP port numbers depend on the device configuration. Default ports are not used for the vulnerable UDP IP SLA operation or for the UDP responder ports.

  Cisco has released free software updates that address this vulnerability.

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

- CSCtk74660

  Symptoms: The Network Time Protocol (NTP) tries to resync after the server clock changes its time and after the NTP falls back to the local clock.

  Conditions: This symptom is observed when the server clock time drifts too far away from the local clock time.

  Workaround: There is no workaround.

- CSCtl00467

  Symptoms: A Cisco router crashes.

  Conditions: This symptom is observed when call monitoring is enabled and the “conference call” feature is used.

  Workaround: There is no workaround.

- CSCtl05684

  Symptoms: Xauth user information remains in the **show crypto session summary** command output.

  Conditions: This symptom is observed when running EzVPN and if Xauth is performed by different usernames during P1 rekey. This issue is seen when NAT is used in the VPN path.

  Workaround: Use the ave-password feature (without interactive Xauth mode) to avoid sending the different username and password during P1 rekey.

- CSCtl43156

  Symptoms: When using a BVI interface configured for IPv6 on a Cisco ISR-G2 series router, IPv6 neighbors are never discovered over the BVI. Neighbors will never be seen in the **show ipv6 neighbors** command output and all traffic to/through the BVI will fail.

  Conditions: This symptom occurs when IPv6 is configured on Cisco ISR-G2 router images running on the “datak9” package.

  Workaround: Use the “uck9” technology package, where the IPv6 feature is already present.

- CSCtl45684

  Symptoms: A Cisco device may crash due to “CPU Signal 10” preceded by the following messages in the logs:

  ```
  ASSERTION FAILED: file "../hwic/shdsl_efm/if_hwic_shdsl_efm_io.c", line 726
  ASSERTION FAILED: file "../hwic/shdsl_efm/if_hwic_shdsl_efm_io.c", line 30
  ```

  Conditions: This symptom is observed only when the HWIC-4SHDSL-E card is present in the router.

  Workaround: There is no workaround.

- CSCtl67079

  Symptoms: The following error message is seen on a Cisco router with HWIC_1GE_SFP inserted:

  ```
  %HWIC_1GE_SFP-3-INTERNAL_ERROR: GigabitEthernet0/0/0 SNMP high capacity
  counter register failed
  ```

  Conditions: This symptom is observed during bootup.

  Workaround: There is no workaround.

- CSCtl94813

  Symptoms: When using iLBC, the VG224 fails to play audio out the FXS port. The call uses iLBC when the analog phone on the VG224 attends a conference bridge. It causes one-way audio.

  - When the IP capture is decoded from the VG224, the iLBC audio packet received and sent to the VG224 Fast Ethernet interface is clearly seen.
  - For the same call, the PCM trace shows no audio in the RIN stream.

  Conditions: This symptom occurs with Cisco IOS Release 15.1(2)17T. As per the HPI logs, the Cisco IOS does not send any packets to the dsp:

  ```
  *Mar 10 23:36:54.988: //1944/9948BD1D87E7/HPI/[0/1:1]/hpi_receive_query_rx:
     Got RX stats
  ```

```
    Packet details:
      Packet Length=188, Channel Id=1, Packet Id=200
      RX Packets=0: Signaling=0, ComfortNoise=0
      Receive Duration=129180(ms): Voice=0(ms), FAX=0(ms)
      Packet Counts: OOSequence=0, Bad header=0, Late=0, Early=0Receive
inactive duration=129(ms)
```

Workaround: Downgrade the Cisco IOS to Cisco IOS Release 12.4(4)T8.

- CSCtl95752

  Symptoms: HWIC-4SHDSL-E reports erroneous EOC and PBO values over time.

  Conditions: This symptom is observed when the HWIC-4SHDSL-E port is connected to the Alcatel-Lucent DSLAM.

  Workaround: There is no workaround.

- CSCtn08208

  Symptoms: Clicking on the Citrix bookmark causes multiple windows of the browser to open. The web page tries to refresh itself a few times, and finally the browser window hangs.

  Conditions: This symptom occurs when upgrading to Cisco IOS Release 15.0(1)M4.

  Workaround: Downgrade to Cisco IOS Release 15.0(01)M2.4.

- CSCtn08258

  Symptoms: The router crashes.

  Conditions: This symptom is observed with Cisco IOS Release 15.1(2)T2 and Cisco IOS Release 15.1(3)T1 when SIP calls are made.

  Workaround: There is no workaround. However, this issue is not seen in Cisco IOS Release 15.1(4)M.

- CSCtn10922

  Symptoms: A router configured with “atm route-bridged ip” on an ATM subinterface may drop multicast traffic, and in some cases, may undergo a software initiated reload due to memory corruption. This issue is also evidenced by the presence of an incomplete multicast adjacency on the ATM subinterface.

  Conditions: This symptom is observed on ATM subinterfaces that are configured with “atm route-bridged ip” and forwarding multicast traffic.

  Workaround: Configure the **ip pim nbma-mode** command on the point-to-point ATM subinterfaces.

- CSCtn12119

  Symptoms: There is no change in functionality or behavior from a user perspective. This DDTS brings in changes to padding used during signing/verification from PKCS#1 v1.0 to PKCS #1v1.5.

  Conditions: This symptom is observed during signing/verification for releases prior to Cisco IOS Release 15.1(2)T4.

  Workaround: The Rommon is capable of verifying images signed using both v1.0 and v1.5. As such no workaround is necessary from a usability perspective, the image boots and runs as expected. However, it will not be in compliance with FIPS 140-3 requirements.

- CSCtn19178

  Symptoms: If you are running an Inter-AS MPLS design across two autonomous systems, the router may clear the local label for a working vrf “A” and a new local label will not be reassigned.

  Conditions: This symptom occurs on the MPLS Edge LSR when you remove the configuration of an unused vrf “B”, including:

  - The vrf interface, for example, **no interface Gi1/0/1.430**.
  - The same vrf process, for example, **no router ospf** *process id* vrf *vrf name*.

  Run the following commands to verify whether you are facing this issue:

  - **show ip bgp vpnv4 vrf A** *subnet* (this is for the working vrf)
  - **show mpls forwarding-table labels** *local label*

  Workaround: To reprogram a new local label on the PE router, clear the MP-BGP session by using either of the following commands:

  - **clear ip bgp** *mp-bgp neighbor* **soft in**
  - **clear ip bgp** *mp-bgp neighbor* **soft out**

- CSCtn22728

  Symptoms: See the following:

```
Router(config)#monitor session 1 type erspan-source
Router(config-mon-erspan-src)#destination ?
<cr>

Router(config-mon-erspan-src)#destination int g11/48
Router(config-if)#
Config Sync: Line-by-Line sync verifying failure on command:
    destination int g11/48
due to parser return error
```

  Conditions: This symptom is seen when using an unsupported interface CLI option with the **destination** keyword in ERSPAN source session configuration, which may result in Config-Sync failure between Active and Standby-RP, therefore reloading Standby-RP.

  Workaround: Do not issue not applicable commands.

- CSCtn26785

  Symptoms: Incoming traffic on DS3 atm 1/0 is process-switched:

```
3845#sh int atm 1/0 stat
ATM1/0
Switching path    Pkts In    Chars In     Pkts Out    Chars Out
Processor         98170      10995040     1           68
Route cache       0          0            98170      10995040
Total             98170      10995040     98171      10995108
3845#

3845#sh cef int atm 1/0
ATM1/0 is up (if_number 5)
    Corresponding hwidb fast_if_number 5
    Corresponding hwidb firstsw->if_number 5
    Internet address is 64.65.248.174/30
    ICMP redirects are never sent
    Per packet load-sharing is disabled
    IP unicast RPF check is disabled
    Input features: Ingress-NetFlow
    Output features: Post-Ingress-NetFlow
    IP policy routing is disabled
    BGP based policy accounting on input is disabled
    BGP based policy accounting on output is disabled
    Hardware idb is ATM1/0
    Fast switching type 9, interface type 138
    IP CEF switching enabled
    IP CEF switching turbo vector
    IP prefix lookup IPv4 mtrie 8-8-8-8 optimized
```

```
    Input fast flags 0x0, Output fast flags 0x0
    ifindex 5(5)
    Slot Slot unit 0 VC -1
    IP MTU 4470
3845#
```

Conditions: Conditions are unknown at this time.

Workaround: There is no workaround.

- CSCtn27599

  Symptoms: The OIR of NM-1T3/E3 line card crashes the router.

  Conditions: This symptom is observed only on the Cisco 3945 router.

  Workaround: There is no workaround.

- CSCtn38996

  Symptoms: All MVPN traffic is getting blackholed when peer is reachable using a TE Tunnel, and an interface flap is done so that secondary path can be selected. The multicast route does not contain a native path using the physical interface.

  Conditions: This symptom is seen when **mpls traffic-eng multicast-intact** is configured under OSPF.

  Workaround: Issue the **clear ip ospf process** command on the core router.

- CSCtn48744

  Symptoms: Memory leaks on OER border router while running PfR-IPSLA configuration.

  Conditions: This symptom is seen on a Cisco 7200 router that is running Cisco IOS Release 15.1(4)M.

  Workaround: There is no workaround.

- CSCtn53094

  Symptoms: The router crashes or generates the following error:

  ```
  %SYS-3-MGDTIMER: Timer has parent, timer link, timer = 8796350. -Process=
  "Mwheel Process", ipl= 2, pid= 315
  ```

  Conditions: This symptom is observed when toggling very fast between the **ip pim** *mode* and **no ip pim** commands on an interface when that interface is the only one where PIM is being enabled. The most common way this can happen in a production network is through the use of “config replace”, which results in the toggling of the command from ON to OFF and then ON on a different interface.

  Workaround: Avoid fast toggling of the **pim** *mode* command if possible when it is only present on a single interface.

- CSCtn72939

  Symptoms: The L2tpv3 feature is not working on Cisco c181x platforms.

  Conditions: This symptom occurs with Cisco c1812 running Cisco IOS Release 15.(0)M and later releases.

  Workaround: Configure bridge-group under that xconnect interface.

- CSCtn76183

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

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

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

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

- CSCtn77154

  Symptoms: The Stateful Inspection Feature is enabled after reload when an “ip nat outside” statement is configured on two interfaces, which results in packets being punted to the CPU. This causes overall performance degradation.

  Conditions: This symptom is observed when two outside NAT interfaces are configured and “no ip nat service nbar” is configured on the interface.

  Workaround: Configure “ip nbar protocol discovery” on the interface.

- CSCtn87012

  Symptoms: FXS ports that are SCCP-controlled stay in the “ringing” state, and the DSP thermal alarm pops up.

  Conditions: This symptom is observed on a Cisco VG200 series voice gateway running Cisco IOS Release 15.0(1)M4 if the phone is answered during the ringing ON cycle.

  Workaround: Pick up the phone during the ringing OFF cycle.

- CSCtn93891

  Symptoms: Multicast traffic is getting blocked.

  Conditions: This symptom occurs after SSO with mLDP and P2MP-TE configurations.

  Workaround: There is no workaround.

- CSCtn96521

  Symptoms: When the Spoke (dynamic) peer group is configured before the iBGP (static) peer group, the two iBGP (static) neighbors fail to establish adjacency.

  Conditions: This symptom is observed when the Spoke (dynamic) peer group is configured before the iBGP (static) peer group.

  Workaround: If the order of creation is flipped, the two iBGP (static) neighbors will establish adjacency.

- CSCtn97451

  Symptoms: The bgp peer router crashes after executing the **clear bgp ipv4 unicast** *peer* command on the router.

  Conditions: This symptom occurs with the following conditions:

```
Router3 ---ebgp--- Router1 ---ibgp--- Router2

ROUTER1:
--------
interface Ethernet0/0
  ip address 10.1.1.1 255.255.255.0
  ip pim sparse-mode
!

router ospf 100
  network 0.0.0.0 255.255.255.255 area 0
!
router bgp 1 bgp log-neighbor-changes
  network 0.0.0.0
  neighbor 10.1.1.2 remote-as 1
  neighbor 10.1.1.3 remote-as 11
```

```
!

ROUTER2:
--------
interface Ethernet0/0
  ip address 10.1.1.2 255.255.255.0
  ip pim sparse-mode
!
router ospf 100
  redistribute static
  network 0.0.0.0 255.255.255.255 area 0
!
router bgp 1
  bgp log-neighbor-changes
  network 0.0.0.0
  redistribute static
  neighbor 10.1.1.1 remote-as 1
!
ip route 192.168.0.0 255.255.0.0 10.1.1.4

ROUTER3:
-------
interface Ethernet0/0
  ip address 10.1.1.3 255.255.255.0
  ip pim sparse-mode
!
router bgp 11
bgp log-neighbor-changes
  network 0.0.0.0
  network 0.0.0.0 mask 255.255.255.0
  redistribute static
  neighbor 10.1.1.1 remote-as 1
!
ip route 192.168.0.0 255.255.0.0 10.1.1.4
```

Crash reproduce steps are as follows:

1. Traffic travel from ROUTER3 to ROUTER2.
2. “clear bgp ipv4 unicast 10.1.1.1” on ROUTER2.

Workaround: There is no workaround.

- CSCto00796

  Symptoms: In a rare and still unreproducible case, the RR (also PE) misses sending RT extended community for one of the redistributed vpnv4 prefix to the PE (also and RR) that is part of a peer-group of PE (+RR).

  Conditions: This symptom occurs when a new interface is provisioned inside a vrf and the configuration such that the connected routes are redistributed in the vrf. This redistributed route fails to tag itself with the RT when it reaches the peering PE(+RR)

  Workaround: Soft clear the peer that missed getting the RT.

- 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.

- CSCto03446

  Symptoms: When a flat bandwidth policy is attached to a serial subinterface via frame-relay map-class, all packets are dropped and no traffic goes through.

  Conditions: This symptom occurs with a flat policy attached to the frame-relay interface with traffic shaping enabled.

  Workaround: Remove traffic shaping from the interface and attach a hierarchical policy.

- CSCto07586

  Symptoms: An IPV4 static BFD session does not get established on a system which does not have IPV6 enabled.

  Conditions: This symptom occurs with the following conditions:

  1. Create an IOS image that does not IPV6 enabled.
  2. Enable BFD on an interface.
  3. Configure an IPV4 static route with BFD routing through the above interface.

  The IPV4 BFD session does not get established, so the static route does not get installed.

  Workaround: Unconfigure BFD on the interface, and then reconfigure it. Then, the session will come up.

- CSCto07919

  Cisco IOS Software is affected by two vulnerabilities that cause a Cisco IOS device to reload when processing IP version 6 (IPv6) packets over a Multiprotocol Label Switching (MPLS) domain. These vulnerabilities are:

  – Crafted IPv6 Packet May Cause MPLS-Configured Device to Reload
  – ICMPv6 Packet May Cause MPLS-Configured Device to Reload

  Cisco has released free software updates that address these vulnerabilities.

  Workarounds that mitigate these vulnerabilities are available.

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-ipv6mpls

- 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.

- CSCto11238

  Symptoms: OSPF cannot be enabled on a tunnel interface by using either the network statement under OSPF or by enabling OSPF directly under the interface.

```
Router#show ip osp neighbor tunXXX
%OSPF: OSPF not enabled on TunnelXXX
```

Conditions: This symptom is observed in both Cisco IOS Release 15.1S and Cisco IOS Release 15.1T IOS software trains. The problem is triggered by configuring either WCCP, L3VPN, or mGRE. A tunnel configured with any of these will have dynamic routing disabled on it. If this is then deleted, the idb is reused by a new tunnel created via the CLI. This newly created tunnel will still have dynamic routing disabled on it and therefore ospf cannot run on it.

Workaround: Once the problem has occurred, the only way to recover is to reload the router. If WCCP, L3VPN, or mGRE are never configured, the issue will not be seen.

- CSCto13254

  Symptoms: Anyconnect fails to connect to a Cisco IOS headend. The Anyconnect event log shows the following error:

  ```
  Hash verification failed for file <temp location of profile>
  ```

  Conditions: This symptom is observed with Anyconnect 3.x when connecting to a Cisco IOS headend that is configured with a profile.

  Workaround: Remove the profile from the Cisco IOS headend.

- CSCto14435

  Symptoms: A Cisco 7200 router with a C7200-VSA module may crash when the tunnel interface is enabled.

  Conditions: This symptom is observed on a Cisco 7200 router with a C7200-VSA module enabled. This issue is seen with Cisco IOS Release 12.4(24)T4 and Cisco IOS Release 15.0(1)M.

  Workaround: Disable ip route-cache and ip route-cache cef on the tunnel source interface.

- CSCto15361

  Symptoms: MF: Active Supervisor crashes after removing the “router eigrp” configuration.

  Conditions: This symptom occurs when the Active Supervisor crashes while disabling the Ipv6 router eigrp because the EIGRP Hello process gets killed. This issue occurs because the EIGRP Hello process calculates the size of the packet. After investigation, it was found that this is purely a timing-based issue. During cleanup, which is done by the EIGRP PDM process, the peer list is cleaned up first, and then an attempt is made to kill the Hello process. In case the peer list is cleaned up, and then the Hello process tries to calculate the size of a particular peer, then it finds the peer as NULL and crashes.

  Workaround: Modify the igrp2_procinfo_free function to kill the EIGRP Hello process prior to cleaning up the peer list.

- CSCto16597

  Symptoms: When using the voluntary PPP feature with L2TP, a memory leak is seen. The leak is of AAA memory that is allocated on behalf of the voluntary PPP.

  Conditions: This symptom occurs when there is a disconnect of the L2TP or voluntary PPP connection.

  Workaround: There is no workaround.

- CSCto24338

  Symptoms: Router reload occurs due to the following bus error when the processor reads data from an invalid memory location:

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

  Conditions: This symptom occurs with NAT+SIP.

Workaround: Disable the NAT SIP multipart processing by executing the **no ip nat service allow-multipart** command.

- CSCto31265

  Symptoms: ABR does not translate Type7 when primary Type7 is deleted even if another Type7 LSA is available.

  Conditions: This symptom occurs with OSPFv3. ABR receives multiple Type7 LSA for the same prefix from Multiple ASBR.

  Workaround 1: Delete/readd the static route that generates Type7.

  Workaround 2: Execute the **clear ipv6 ospf force-spf** command on ABR.

  Workaround 3: Execute the **clear ipv6 ospf redistribution** command on ASBR.

- CSCto41165

  Symptoms: The standby router reloads when you use the **ip extcommunity-list 55 permit | deny** command, and then the **no ip extcommunity-list 55 permit | deny** command.

  Conditions: This symptom occurs when the standby router is configured.

  Workaround: There is no workaround.

- CSCto44581

  Symptoms: The router crashes on high call volume.

  Conditions: This symptom occurs on high call volume.

  Workaround: There is no workaround.

- CSCto46716

  Symptoms: Routes over the MPLS TE tunnel are not present in the routing table.

  Conditions: This symptom occurs when the MPLS TE tunnel is configured with forwarding adjacency. In “debug ip ospf spf”, when the SPF process link for the TE tunnel is in its own RTR LSA, the “Add path fails: no output interface” message is displayed. Note that not all tunnels are affected. It is unpredictable which tunnel is affected, but the number of affected tunnels grows with the number of configured tunnels.

  Workaround: If feasible, use autoroute announce instead of forwarding adjacency. Otherwise, upgrade to the fixed version.

- CSCto47524

  Symptoms: A Cisco ASR 1002 router that is running Cisco IOS Release 15.1(1)S1 may have a processor pool memory leak in IP SLAs responder.

  A **show process memory sorted** command may initially show “MallocLite” growing. By disabling malloclite with the following:

  ```
  config t
  no memory lite
  end
  ```

  one may start to see process “IP SLAs Responder” growing. In at least one specific case, the leak rate was 80mb per day.

  Conditions: This symptom is observed on a Cisco ASR 1002 router.

  Workaround: Disable IP SLA on the affected router, if possible.

- CSCto50255

  Symptoms: Memory leak occurs while running UDP echo operation.

Conditions: This symptom is observed when an UDP echo operation successfully runs. Leak is seen on every 100th run of the UDP echo operation. Using the **show memory debug leaks** command will not capture this. The only way is monitoring and decoding the PC via the **show processes memory** *pid* command.

Workaround: There is no workaround.

- CSCto53332

  Symptoms: A router configured for IPSEC accounting may display the following error message:

  ```
  %AAA-3-BUFFER_OVERFLOW: Radius I/O buffer has overflowed
  ```

  This does not seem to result in any impact apart from intermittently lost accounting messages.

  Conditions: This symptom occurs when ipsec accounting is active.

  Workaround: There is no workaround.

- CSCto63954

  Symptoms: A router with GETVPN configurations is continuously crashing.

  Conditions: This symptom is seen with GETVPN related configurations with the fail-close feature activated.

  Workaround: There is no workaround.

- CSCto68554

  The Cisco IOS Software contains two vulnerabilities related to Cisco IOS Intrusion Prevention System (IPS) and Cisco IOS Zone-Based Firewall features.

  These vulnerabilities are:

  - Memory leak in Cisco IOS Software
  - Cisco IOS Software Denial of Service when processing specially crafted HTTP packets

  Cisco has released free software updates that address these vulnerabilities.

  Workarounds that mitigate these vulnerabilities are not available.

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

- CSCto81814

  Symptoms: When SSH is attempted over an IKEv2 tunnel using ECDSA certificates, the router crashes.

  Conditions: This symptom is only observed when ECDSA certificates are used for IKEv2, and not with RSA certs or with IKEv1.

  Workaround: There is no workaround.

- CSCto86833

  Symptoms: The router's CPU spikes to 100 percent, leading to voice call failures, among other problems.

  Conditions: This symptom occurs with the Cisco 3945e router configured with SRST (call-manager-fallback) to the maximum supported capacity of 1500 phones, 2500 DNs with octo-line capability, and PRI interfaces controlled via ccm-manager. Under these conditions, MGCP call processing consumes a significant amount of CPU. Even at 0.5cps MGCP call arrival rate, the router's average CPU will be around 50 to 60 percent.

Workaround: If possible, reduce the number of voice ports automatically generated by the number DNs and octo-line. Also, if possible, use dual-line support instead. The lower the number of voice ports, the lower the CPU impact of this defect. Use the **show voice port summary** command to view the total number of voice ports created on the router after SRST configuration.

- 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-sip

- CSCtq05636

  Symptoms: When sending calls between two SIP endpoints, alphanumeric characters (non-numeric) are stripped when forwarding the invite to the outgoing leg.

  For example:

  ```
  Received: INVITE sip:18 669863384**83782255@10.253.24.35:5060 SIP/2.0
  Sent: INVITE sip:18 669863384**83782255@10.253.24.35:5060 SIP/2.0
  ```

  In Cisco IOS Release 15.1.3T1, the * character is not forwarded.

  Conditions: This symptom is observed when CUBE performs SIP to SIP interworking. This issue is seen only with Cisco IOS Release 15.1.3T1.

  Workaround: Upgrade the code to Cisco IOS Release 15.1.3T or Cisco IOS Release 15.1(M4).

- CSCtq09899

  Symptoms: The VXML gateway crashes.

  Conditions: This symptom occurs during the load test, when the **show mrcp client session active** is used.

  Workaround: There is no workaround.

- CSCtq10684

  Symptoms: The Cisco 2800 crashes due to a bus error and the crash points to access to free internal structures in ipsec.

  Conditions: This symptom occurs when tunnel flap is observed before the crash.

  Workaround: A possible workaround is to reload the box.

- CSCtq15247

  Symptoms: The router crashes when removing the virtual-ppp interface. The crash is more common if the l2tp session is flapping when the virtual-ppp interface is removed.

  Conditions: This symptom occurs if the l2tp session is flapping when the virtual-ppp interface is removed.

  Workaround: Remove the **pseudowire** command from under the **virtual-ppp interface** command before removing the interface.

  For example:

```
LAC1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
LAC1(config)#interface virtual-ppp1
LAC1(config-if)#no pseudowire
LAC1(config-if)#exit
LAC1(config)#no interface virtual-ppp1
```

- CSCtq27180

  Symptoms: After a Cisco IOS upgrade, any permanent licenses are erased and eval licenses do not work.

  Conditions: This symptom is observed only on IOS internal releases.

  Workaround: There is no workaround.

  Further Problem Description: The following LOG messages and errors are found:

```
Mar 30 01:27:38.003: %LICENSE-2-LIC_STORAGE: Storage validation failed
-Traceback= 604D93C0z 637CE110z 637CE1BCz 637CE334z 61C73250z 61C734E0z 63765DE4z
63765DC8z
Mar 30 01:27:38.447: %LICENSE-2-VLS_ERROR: 'VLSsetInstallLicenseStorage'
failed with an error - rc = 136 - 'Error[136]: Specified license store
doesn't exists.'
-Traceback= 604D93C0z 637CE110z 637CE1BCz 637CE334z 61C73250z 61C734E0z
63765DE4z 63765DC8z
```

- CSCtq28732

  Symptoms: Memory leak is observed when device is configured **parameter-map type inspectglobal**.

  Conditions: Device is configured with **parameter-map type inspect global**.

  See also Cisco Security Advisory: Cisco IOS Software IPS and Zone Based Firewall Vulnerabilities, at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-zbfw

  Workaround: There is no workaround.

- CSCtq29554

  Symptoms: All multicast routes may be missing from the multicast forwarding information base (MFIB) after SSO and MFIB/MRIB error messages may be generated, indicating failure to connect MFIB tables to the MRIB. The output of the **show ipc port | in MRIB** command on a failed line card does not display a port.

  Conditions: This symptom can occur on a line card of a distributed router such as the Cisco 7600 if an IPC local error has occurred before switchover. The MRIB IPC port to the new RP is not created after switchover and the MFIB tables cannot connect to the MRIB and download multicast routes.

  Workaround: Reload the failing line card to recover it.

- CSCtq30875

  Symptoms: A Cisco ISR G1 will display "March 11, 2011" when the **show clock** command is entered. This will effect the functionality that depends on the clock to be accurate (for example, certificates to make secure connections or calls).

  Conditions: This symptom is observed only on Cisco ISR G1 routers running ISR licensing software.

  Workaround: The clock can be set manually via CLI.

- CSCtq36726

  Symptoms: Configuring the **ip nat inside** command on the IPSEC dVTI VTEMP interface does not have any effect on the cloned Virtual-access interface. The NAT functionality is thus broken, because the V-access interface does not get this command cloned from its respective VTEMP.

  Conditions: This symptom is observed on Cisco ASR1006 (RP2/FP20) routers with ikev2 dVTI. This issue may be service impacting and is easily reproducible.

  Workaround: Reconfigure the Virtual-template interface such that the **ip nat inside** command is applied first, followed by other commands.

- CSCtq39406

  Symptoms: When you set up an energywise domain via the CLI and then set the energywise level to zero on a SM or ISM, the module shuts down after 2 minutes. Then, all IP connectivity and console connectivity to the router is lost.

  Conditions: This symptom occurs when you set up an energywise domain via the CLI, and then set the energywise level to zero on a SM or ISM.

  Workaround: Remove the HWIC-3G-HSPA. When you remove the 3G module from the system, energywise works as expected. You can shut down power modules using the above configuration. As soon as the 3G card is installed in slot 2 or 3 and the energywise level is set to zero, the service module shuts down and the entire router crashes. It has no IP connectivity and the console is inactive. The only workaround is a hard reset (along with removal of the card).

- CSCtq49408

  Symptoms: Analog phone calls (fxs) cannot be made with CME/SCCP.

  Conditions: This symptom occurs when SCCP support for FXS is missing in IAD2435.

  Workaround: There is no workaround.

- CSCtq61850

  Symptoms: When the SNR call is forwarded to CUE after the SNR call-forward noan timer (cfwd-noan) expires, the call gets dropped unexpectedly after CUE answers the call.

  Conditions: This symptom occurs when calls to the SCCP SNR phone and SNR call-forward noan timer (cfwd-noan) are configured. Both SNR and mobile phones do not answer the call and the call is forwarded to voice mail.

  Workaround: There is no workaround.

- CSCtq64951

  Symptoms: The following message is displayed:

  ```
  %CERM-4-TUNNEL_LIMIT: Maximum tunnel limit of 225 reached for Crypto
  functionality with securityk9 technology package license.
  ```

  The **show platform cerm** command output shows all tunnels in use by SSLVPN.

  ```
      Number of tunnels       225
  ...
      SSLVPN D D             225     N/A
  ```

  The **show webvpn session context all** command output shows no or very few active sessions.

  ```
  WebVPN context name: SSL_Context
  Client_Login_Name Client_IP_Address No_of_Connections Created Last_Used
  ```

  Conditions: This symptom occurs on SSLVPN running Cisco IOS Release 15.x. This issue is seen only on ISR G2 platforms.

Workaround: Upgrade to Cisco IOS Release 15.1(4)M1 or later releases.

- CSCtq91176

  Symptoms: When the Virtual-PPP interface is used with L2TP version 2 and the topology uses an L2TP Tunnel Switch (LTS) (multihop node) and L2TP Network Server (LNS), and PPP between the client and LNS does renegotiation, then the PPP session cannot be established.

  Conditions: This symptom occurs when the LTS forwards the call based on the domain or full username from the PPP authentication username, and the LNS does PPP renegotiation.

  Workaround 1: Disable lcp renegotiation on the LNS and clear the L2TP tunnel at the LNS and LTS.

  Workaround 2: Forward the call on the LTS using an L2TP tunnel name instead of the PPP username/domain name.

- CSCtl22737

  Symptoms: The config replace feature fails to remove “hold-queue” interface subcommands.

  Conditions: This symptom occurs when the config replace feature fails to remove “hold-queue” interface subcommands.

  Workaround: Manually remove the “hold-queue” configuration. With this fix,

  the behavior has changed for the “no” form of this command.

  In short,

```
no hold-queue <any random value(not necessarily the same configured value)>
out [for out queue]

no hold-queue <any random value(not necessarily the same configured value)>
in [for in queue]
```

Resolved Caveats—Cisco IOS Release 15.1(2)T3

Cisco IOS Release 15.1(2)T3 is a rebuild release for Cisco IOS Release 15.1(2)T. The caveats in this section are resolved in Cisco IOS Release 15.1(2)T3 but may be open in previous Cisco IOS releases.

- 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat

- CSCtd10712

  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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat

- CSCtd90030

  Symptoms: A Cisco 2851 router may crash with a bus error.

  Conditions: The symptom is observed when the function calls involve Session Initiation Protocol (SIP) and it is possibly related to an IPCC server. It is seen with Cisco IOS Release 12.4(24)T1 or Release 12.4(24)T2.

  Workaround: There is no workaround.

- CSCtd91542

  Symptoms: The **show ip multicast rpf tracked** command may cause a crash.

  Conditions: The symptom is observed on a Cisco 10000 series router that is running all Cisco IOS 12.2(33) releases and after executing the **show ip multicast rpf tracked** command.

  Workaround: Avoid using the **show ip multicast rpf tracked** command.

  Further Problem Description: The command **show ip multicast rpf tracked** is not intended for customer use and is being deprecated.

- CSCte01606

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

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

  Workaround: Disable BFD.

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

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

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

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

  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtf36402

  Symptoms: A Cisco router crashes when the user telnets and Transmission Control Block is cleared for that session before entering the password.

  Conditions: This symptom is observed when aaa authentication protocol is set to TACACS.

  Workaround: Do not clear the Transmission Control Block for a session before entering the password.

- CSCtf54561

  Symptoms: A MPLS TE FRR enabled router can encounter a crash if the **show ip cef vrf** *vrf-name* command is issued.

  Conditions: This symptom occurs when the VRF contains many entries (17k) in which the outgoing interface changes due to a topology change.

  Workaround: Command should not be issued when many topology changes occur on interface flaps.

- 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.

- CSCtf72328

  Symptoms: BFD IPv4 Static does not fully support AdminDown.

  Conditions: The symptom is observed with the following setup and configuration:

```
Router 1:
interface e0/0
ip address 192.168.1.1 255.255.255.0
bfd interval 51 min_rx 51 multiplier 4
bfd echo
no shut
exit

interface loopback 0
ip address 10.10.1.1 255.255.0.0
exit
ip route static bfd e0/0 192.168.1.2
ip route  10.20.0.0 255.255.0.0 e0/0 192.168.1.2

Router 2:
interface e0/0
ip address 192.168.1.2 255.255.255.0
bfd interval 51 min_rx 51 multiplier 4
bfd echo
no shut
exit

interface loopback 0
ip address 10.20.1.1 255.255.0.0
exit

ip route static bfd e0/0 192.168.1.1
ip route  10.10.0.0 255.255.0.0 e0/0 192.168.1.1

interface e0/0
no ip route static bfd e0/0 192.168.1.1
```

  Though the BFD state is DOWN the static has the route active. If the BFD peer signals AdminDown on a session being used to monitor the gateway for a static route, no action will be taken.

  Workaround: Perform a shut/no shut the interface on which the BFD session is configured.

- CSCtg31210

  Symptoms: A router may reload.

Conditions: The symptom is observed when using the PfR feature to control path selection with EIGRP and when **debug oer border routes eigrp detail** is enabled.

Workaround: Do not configure debugs **debug oer border routes eigrp** or **debug oer border routes eigrp detail**.

Further Problem Description: The issue is not seen in Cisco IOS Release 15.0 (1)M4.

- CSCtg42279

  Symptoms: A Cisco label switch router (LSR) crashes when an MPLS traceroute is issued.

  Conditions: This symptom is observed when executing MPLS traceroute over a IPsec-protected GRE tunnel.

  Workaround: There is no workaround.

- CSCtg63096

  Symptoms: The **deny ip any any fragments** command shows a high number of hits for traffic that may not be truly fragmented.

  Conditions: This symptom occurs when “deny ip any any fragments” may be configured at the top of the ACL.

  Workaround: There is no workaround.

- CSCtg64175

  Symptoms: The ISIS route is missing the P2P link, it is mistakenly marked as “parallel p2p adjacency suppressed”.

  Conditions: The symptom is observed when the ISIS neighbor is up and multiple topologies are enabled on P2P interfaces. It is seen if you enable a topology on a P2P interface of the remote router and send out the serial IIH packet with the new MTID to the local router where the topology has not been enabled on the local P2P interface yet.

  Workaround: Do a **shut** and **no shut** on the local P2P interface.

- CSCtg67346

  Symptoms: After some time of normal operation, a dialer interface (dialer profile configuration) might become stuck. Debugs would only show “Di1 DDR: dialer_fsm_pending() di1”.

  Conditions: The conditions are unknown at this time.

  Workaround: Remove the affected dialer and put the configuration on another dialer.

- CSCtg73631

  Symptoms: Spurious access or crash.

  Conditions: EIGRP undergoes a route delete event for a route that is both redistributed and learned as an external. The redistributed route is deleted and external route promoted. An error in the route deletion codepath may result in spurious access or crash.

  Workaround: There is no workaround.

  Further Problem Description: Issue is not present in Cisco IOS Release 15.0(1) M4.

- CSCth01394

  Symptoms: On a Cisco 7606 router that is running Cisco IOS Release 12.2(33) SRD3 with SIP200/SPA-4XCT3/DS0, when you have ppp multilink interface(s) configured with member links from same SPA (software based multilink) and you physically remove SPA, you will see that upon executing the **show ppp multilink** command, the multilink interface still has reference for member links. If you do the **sh run int serialx/y** command, you will get message interface not found.

Conditions: This issue is consistently reproducible.

Workaround: There is no workaround.

- CSCth05778

  Symptoms: Router is showing memory leaks.

  Conditions: The symptom is observed when the remote end is sending LCP conf_req messages to a Cisco 10000 series router a lot frequently (1 per 4 msec) than the normal scenario (1 per 2 seconds).

  Workaround: Shut down the PPP link that is flapping.

- CSCth06812

  Symptoms: A Cisco ASR 1000 sees a hang followed by a crash.

  Conditions: This symptom is observed on a Cisco ASR 1000 with Cisco IOS Release 2.5.1. (XNE1) and the following configuration:

```
R1(config)#parser view SUPPORT
R1(config-view)# secret cisco
R1(config-view)# commands exec include ping
R1(config-view)# commands exec include configure terminal
R1(config-view)# commands exec include show ip ospf neighbor       <--Where
we see the hang
```

  Workaround: Do not configure “commands exec include show ip ospf neighbor” command in parser view configuration.

- CSCth14305

  Symptoms: Having a bandwidth statement on a multilink bundle interface will cause problems with QoS and BQS if linkmembers flap as the changes in bandwidth will not be handled correctly.

  Conditions: The symptom is observed when you have a bandwidth statement on a multilink bundle.

  Workaround: Avoid bandwidth statements on multilink bundle interfaces.

- 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.

- CSCth37580

  Symptoms: Dampening route is present even after removing “bgp dampening”.

  Conditions: The symptom is observed under the following conditions:

  – DUT connects to RTRA with eBGP + VPNv4.

  – eBGP + VPNv4 peer session is established and DUT.

  – Also DUT has VRF (same RD) as route advertised by RTRA.

  In this scenario, when DUT learns the route it will do same RD import and the net’s topology will be changed from VPNv4 to VRF. When dampening is unconfigured, we do not clear damp info.

  Workaround: There is no workaround.

- CSCth59784

  Symptoms: Process watchdog timeout crashinfo file not written into flash for Cisco 887 router.

  Conditions: The symptom is observed on a Cisco 887 router.

Workaround: There is no workaround.

- CSCth84233

  Symptoms: Router may crash due to Redzone memory block corruption (I/O) when “qos pre-classify” is configured under tunnel interfaces. The packet is overwriting the next block.

  Conditions: The trigger for this issue is configuring “qos pre-classify”.

  Workaround: Remove “qos pre-classify”.

- CSCth93218

  Symptoms: The error message “%OER_BR-4-WARNING: No sequence available” displays on PfR BR.

  Conditions: The symptom is observed in a scale setup with many PfR application prefixes and when PfR optimizes the application prefixes.

  Workaround: There is no workaround.

- CSCth94814

  Symptoms: Crash is seen in static route component.

  Conditions: The symptom is observed when changing IVRF on a virtual-template when there are about 100 active sessions.

  Workaround: There is no workaround.

- CSCth94827

  Symptoms: IDBINDEX_SYNC-STDBY tracebacks are seen when unconfiguring ima- group on a SONET-ACR controller.

  Conditions: This symptom is observed on a standby supervisor when unconfiguring and configuring ima-group on a SONET-ACR controller.

  Workaround: There is no workaround.

- CSCti01971

  Symptoms: The active router crashes during a switchover in a scaled BFD IPv6 setup.

  Conditions: The router is configured with a larger number of IPv6 routes with BFD sessions configured. (The test was done with 500 BFD IPv6 sessions.)

  Workaround: There is no workaround.

- CSCti03261

  Symptoms: A Cisco router may crash due to a WATCHDOG timeout.

  Conditions: The symptom is observed with Cisco IOS Release 15.0(1)M3 and when attempting to remove a line from a Named Access List that is being used by a QoS service policy.

  Workaround: There is no workaround.

- CSCti04754

  Symptoms: PPPoE sessions are stuck at attempting state forever.

  Conditions: This symptom is seen when sessions are triggered during SSO time, which get stuck at attempting state.

  Workaround: Clear attempting state sessions by the **clear** command from box.

- CSCti05663

  Symptoms: A DHCP ACK which is sent out in response to a renew gets dropped at relay.

Conditions: The symptom is observed in the case of an numbered relay.

Workaround: There is no workaround.

- CSCti10518

  Symptoms: Under very rare circumstances, EIGRP could exhibit a memory leak of NDB structures in the RIB.

  Conditions: If redistribution is occurring into EIGRP and the route ownership is changing in the middle of the redistribution process, EIGRP may leak the NDB in process.

  Workaround: There is no workaround.

- CSCti17841

  Symptoms: Removing “match condition” from a class map crashes the router.

  Conditions: The symptom is observed when you remove “match condition” from a class map.

  Workaround: There is no workaround.

- CSCti22091

  Symptoms: Traceback will occur after a period of use and when the **show oer master** command is used a few times. The traceback is always followed by the message “learning writing data”. The traceback causes the OER system to disable. Manually reenabling PfR will not work. A reboot is required.

  Conditions: The symptom is observed when PfR is configured with the following conditions:

  1. list > application > filter > prefix-list
  2. Learn > traffic-class: keys
  3. Learn > traffic-class: filter > ACL

  Workaround: There is no workaround.

- CSCti24577

  Symptoms: System crashes on active or hangs on standby.

  Conditions: The symptom is observed when a banner command is in the configuration.

  Workaround: Remove all banner commands.

- 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

- CSCti25780

  Symptoms: One of the case values in the EIGRP registry is corrupted. This is seen right after bootup.

  Conditions: This symptom is observed when some of the files are compiled with optimization.

  Workaround: The corruption is not seen if the files are compiled with optimization disabled.

- CSCti34396

  Symptoms: The router distributes an unreachable nexthop for a VPNv4 or VPNv6 address as an MVPN tunnel endpoint.

  Conditions: The symptom is seen when “next-hop-unchanged allpaths” is configured for an external neighbor of the VPNv4 or VPNv6 tunnel endpoint, and the previous hop is an unreachable.

  Workaround 1: Configure a route-map to rewrite routes so that the tunnel endpoint is an address reachable from both inside the VRF and outside of it. For example, to rewrite statically configured routes so that the nexthop is set to a visible address, you would configure:

```
route-map static-nexthop-rewrite permit 10
match source-protocol static
 set ip next-hop <router ip address>
!
router bgp <asn>
 address-family ipv4 vrf <vrf name>
 redistribute static route-map static-nexthop-rewrite
 exit-address-family
 exit
exit
```

  Workaround 2: Instead of configuring static routes with a next-hop, specify an interface name.

  For example, if you had: ip route x.x.x.x 255.255.255.0 y.y.y.y And y.y.y.y was on the other end of the interface serial2/0, you would replace this configuration with: ip route x.x.x.x 255.255.255.0 interface serial2/0

  Further Problem Description: You may also need to override the standard behavior of next-hop-unchanged allpaths in a generic manner with a single standard configuration which could be applied to all the routers. In order to solve this problem, the configuration “set ip next-hop self” is added to route-maps.

  When used in conjunction with the newly added configuration:

```
router bgp <asn>
 address-family vpnv4 unicast
  bgp route-map priority
```

  The “set ip next-hop self” will override “next-hop unchanged allpaths” for the routes which match the route-map where it is configured, allowing the selective setting of the next-hop.

- CSCti36393

  Symptoms: Spurious memory access messages and tracebacks appear on console after disabling and re-enabling WAAS on an interface.

  Conditions: The symptom is observed when open flows are on the router while the configuration commands are given.

  Workaround: There is no workaround.

- CSCti50607

  Symptoms: A Cisco 7200 SRE1 router drops GRE packet size 36-45.

  Conditions: The symptom is observed on a Cisco 7200 series router with SRE1 code.

Workaround: There is no workaround.

- CSCti51145

  Symptoms: After a reload of one router, some or all of the BGP address families do not come up. The output of **show ip bgp all summary** will show the address family in NoNeg or idle state, and it will remain in that state.

  Conditions: In order to see this problem, ALL of the following conditions must be met:

  - The non-reloading device must have a "neighbor x.x.x.x transport connection- mode passive" configuration, or there must be an ip access list or packet filter which permits connections initiated by the reloading device, but not by the non-reloading device. In Cisco IOS, such ip access-lists typically use the keyword **established** or **eq bgp**.
  - It must be configured with a BGP hold time which is less than the time required for the neighbor x.x.x.x to reload.
  - When the neighbor x.x.x.x reloads, no keepalives or updates must be sent on the stale session during the interval between when the interface comes up and when the neighbor x.x.x.x exchanges BGP open messages.
  - Both peers must be multisession capable.
  - "transport multi-session" must not be configured on either device, or enabled by default on either device.
  - "graceful restart" must not be configured.

  Workarounds:

  1. Remove the configuration "neighbor x.x.x.x transport connection-mode passive" or edit the corresponding filter or ip access list to permit the active TCP opens in both directions.
  2. Configure "neighbor x.x.x.x transport multi-session" on either the device or its neighbor.
  3. Configure a very short keepalive interval (such as one second) on the non-reloading device using the **neighbor x.x.x.x timers 1 holdtime** command.
  4. Configure graceful restart using the command **neighbor x.x.x.x ha- mode graceful-restart**.
  5. If the issue occurs, use the **clear ip bgp *** command to cause all sessions stuck in the NoNeg state to restart. You can also use **clear ip bgp x.x.x.x addressFamily** to bring up individual stuck sessions without resetting everything else.

  Further Problem Description: This is a day one problem in the Cisco IOS multisession implementation which impacts single-session capable peers. CSCsv29530 fixes a similar problem for some (but not all) situations where "neighbor x.x.x.x transport single-session" is configured and NSF is not configured.

  The effect of this fix is as follows: when the neighbor is in single-session mode, AND the router sees an OPEN message for a neighbor which is in the ESTABLISHED state, then the router will send a CEASE notification on the new session and close it (per section 6.8 of RFC 4271). Additionally, it will send a keepalive on the ESTABLISHED session. The keepalive is not required, but will cause the established session to be torn down if appropriate.

  Note that the fix does not solve the problem when interacting with Cisco IOS Release 12.2(33)SB based releases if the 12.2(33)SB router is the one not reloading.

- CSCti61949

  Symptoms: Unexpected reload with a "SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header" and "chunk name is BGP (3) update" messages.

Conditions: The symptom is observed when receiving BGP updates from a speaker for a multicast-enabled VRF.

Workaround: Disable multicast routing on VRFs participating in BGP or reduce the number of extended communities used as route-target export.

- CSCti66076

  Symptoms: A standby HSRP router could be unknown after reloading the ES20 module that configured HSRP.

  Condition: This symptom is observed under the following conditions:

  - HSRP version 1 is the protocol that must be used.
  - Use HSRP with sub-interfaces on ES20 module *Reload the ES20 module

  Workaround: Change to HSRPv2, which is not exposed to the issue.

  Alternate Workarounds:

  1. econfigure HSRP on all subinterfaces
  2. Configure multicast or igmp configuration on the interface where HSRP is configured (like ip pim sparse-mode).

- CSCti67102

  Symptoms: Tunnel disables due to recursive routing loop in RIB.

  Conditions: The symptom is observed when a dynamic tunnel which by default is passive in nature is created. EIGRP will get callback due to address change (dynamic tunnel come-up). EIGRP tries to run on this interface and install EIGRP route in the RIB which will replace tunnel next-hop result in tunnel disable and routing chain loop result in RIB.

  Workaround: There is no workaround.

- CSCti67447

  Symptoms: During an SSO, an 8 to 12 second packet drop may occur on EoMPLS VCs.

  Conditions: The symptom is observed under the following conditions:

  1. EoMPLS port-based or VLAN-based configuration; VC between PE1 and PE2.
  2. Enable MPLS LDP GR.

  Workaround: There is no workaround.

- CSCti67905

  Symptoms: A Cisco router may experience a crash.

  Conditions: This has been experienced on Cisco routers running Cisco IOS Release 15.1(2)T and Release 15.1(2)T1. The routers are configured with IOS firewall and are inspecting FTP packets.

  Workaround: There is no workaround.

- CSCti68721

  Symptoms: The output of show performance monitor history interval <all | given #> will appear to have an extra column part way through the output.

  Conditions: This symptom is observed sporadically while traffic is running on a performance monitor policy at the time when a user initiates the CLI show command.

  Workaround: If the symptom occurs, repeat the command.

- CSCti75666

  Symptoms: Calls from CUCM through H.323 to SIP CUBE get disconnected when remote AA does transfer.

  Conditions: The symptom is observed on CUCM 4.1.3 and 6.1.3. It is seen on an ISR gateway that is running Cisco IOS Release 12.4(24)T2.

  Workaround: Convert H.323 leg to SIP.

- CSCti79848

  The Cisco IOS Software contains two vulnerabilities related to Cisco IOS Intrusion Prevention System (IPS) and Cisco IOS Zone-Based Firewall features. These vulnerabilities are:

  - Memory leak in Cisco IOS Software
  - Cisco IOS Software Denial of Service when processing specially crafted HTTP packets

  Cisco has released free software updates that address these vulnerabilities.

  Workarounds that mitigate these vulnerabilities are not available.

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

- CSCti84762

  Symptoms: Update generation is stuck with some peers held in refresh started state (SE).

  Conditions: This is seen with peer flaps or route churn and with an interface flap.

  Workaround: Do a hard reset of the stuck peers.

- CSCti85446

  Symptoms: A nexthop static route is not added to RIB even though the nexthop IP address is reachable.

  Conditions: The symptom is observed with the following conditions:

  1. Configure a nexthop static route with permanent keyword.
  2. Make the nexthop IP address unreachable (e.g.: by shutting the corresponding interface).
  3. Change the configuration in such a way that nexthop is reachable.
  4. Configure a new static route through the same nexthop IP address used in step 1.

  Workaround: Delete all the static routes through the affected nexthop and add them back.

- CSCti87502

  Symptoms: CP Express does not launch. A blank or garbage characters appear in the browser.

  Conditions: This symptom is observed when attempting to launch CP Express.

  Workaround: A power cycle fixes the issue temporarily.

- CSCti91036

  Symptoms: Performance drop has been seen between Cisco IOS Release 15.1(1)T and Release 15.1(2)T.

  Conditions: The symptom is observed when you upgrade from Cisco IOS Release 15.1(1)T to Release 15.1(2)T.

  Workaround: There is no workaround.

- CSCti98219

  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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat

- CSCtj00039

  Symptoms: Some prefixes are in PE router EIGRP topology although those routes are not being passed to the CE router.

  Conditions: The symptom is observed when EIGRP is configured as a routing protocol between PE and CE routers.

  Workaround: Clear the route on the PE router using **clear ip route vrf** *xxx x.x.x.x*.

- CSCtj05198

  Symptoms: When there are two EIGRP router processes (router eigrp 7 and router eigrp 80), PfR is unable to find the parent route. The problem occurs only if one of the processes has the parent route and other one does not. As a result, probe and route control fail.

  Conditions: This symptom is observed when there are two EIGRP router processes.

  Workaround: Use one EIGRP process. There is no workaround if two processes are used.

- CSCtj07904

  Symptoms: EIGRP neighbor relationship goes down with “no passive interface” configured.

  Conditions: The symptom is observed when “no passive interface” is configured.

  Workaround: Do not configure “passive-interface default” and allow the interface to be non-passive by default. Configure “passive-interface *interface*” for the interface to be passive.

- CSCtj17545

  Symptoms: Immediately after a switchover, the restarting speaker sends TCP- FIN to the receiving speaker, when receiving speaker tries to establish (Active open). It can cause packet drops after a switchover.

  Conditions: The symptom can occur when a lot of BGP peers are established on different interfaces.

  Workaround: When the receiving speaker is configured to accept passive connections, the issue will not be observed:

  template peer-session ce-v4 transport connection-mode passive

- CSCtj20163

  Symptoms: On a PE1-P-PE3 setup, a crash is seen on P (core) router with scaled MLDP configurations.

  Conditions: The symptom is observed with the following conditions:

  1. Execute **show mpls mldp database**.

2. Reload Encap PE.
3. Crash seen on P router when MLDP neighbors go down.

Workaround: There is no workaround.

- 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.

- CSCtj21696

  Symptoms: The virtual access interface remains down/down after an upgrade and reload.

  Conditions: The issue occurs on a router with the exact hardware listed below (if HWIC or the VIC card is different the problem does not happen):

```
Router1#sho inv
NAME: "chassis", DESCR: "2801 chassis" PID: CISCO2801 , VID: V04 , SN: FTX1149Y0KF
NAME: "motherboard", DESCR: "C2801 Motherboard with 2 Fast Ethernet" PID: CISCO2801 ,
VID: V04 , SN: FOC11456KMY
NAME: "VIC 0", DESCR: "2nd generation two port EM voice interface daughtercard" PID:
VIC2-2E/M= , VID: V , SN: FOC081724XB
NAME: "WIC/VIC/HWIC 1", DESCR: "4 Port FE Switch" PID: HWIC-4ESW , VID: V01 , SN:
FOC11223LMB
NAME: "WIC/VIC/HWIC 3", DESCR: "WAN Interface Card - DSU 56K 4 wire" PID:
WIC-1DSU-56K4= , VID: 1.0, SN: 33187011
NAME: "PVDM 1", DESCR: "PVDMII DSP SIMM with one DSP with half channel capcity" PID:
PVDM2-8 , VID: NA , SN: FOC09123CTB
```

  Workaround: Do a shut/no shut the serial interface.

- CSCtj24453

  Symptoms: The following traceback is observed when **clear ip bgp *** is done:

```
%SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header, chunk 0  data
5905A0A8  chunkmagic 120000  chunk_freemagic 4B310CC0
-Process= "BGP Scanner", ipl= 0, pid= 549
with call stack
0x41AC033C:chunk_refcount(0x41ac02ec)+0x50
0x403A44E0:bgp_perform_general_scan(0x403a3e2c)+0x6b4
0x403A4E84:bgp_scanner(0x403a4c50)+0x234
```

  Conditions: It is rarely observed, when **clear ip bgp *** is done with lot of routes and route-map-cache entries.

```
Router# show ip bgp sum
BGP router identifier 10.0.0.1, local AS number 65000
BGP table version is 1228001, main routing table version 1228001 604000
network entries using 106304000 bytes of memory
604000 path entries using 31408000 bytes of memory
762/382 BGP path/bestpath attribute entries using 94488 bytes of memory
381 BGP AS-PATH entries using 9144 bytes of memory
382 BGP community entries using 9168 bytes of memory
142685 BGP route-map cache entries using 4565920 bytes of memory
```

  The **clear ip bgp *** command is not a very common operation in production network.

  Workaround: Use **no bgp route-map-cache**. This will not cache the route-map cache results and the issue will not be observed.

- CSCtj27251

  Symptoms: A router may crash when modifying a QoS class-map.

  Conditions: The symptom is observed when modifying a QoS class-map which is being referenced by two or more policy-maps while traffic is matching the class-map and traversing the router.

  Workaround: Remove the policy-maps that match the class-map to be modified by issuing **no service-policy input/output** *policy-map name*, make changes to the class-map, then re-apply the policy-maps by issuing **service-policy input/output** *policy-map name*.

- CSCtj28747

  Symptoms: Route control of prefix and application are out-of-order thereby making application control ineffective. As a result, an "Exit Mismatch" message will be logged on the MC and the application will be uncontrolled for a few seconds after it is controlled.

  Conditions: The symptom is observed only if PIRO control is used where prefixes are also controlled using dynamic PBR. PIRO control is used when the routing protocol is not BGP, STATIC, or EIGRP, or when two BRs have different routing protocol, i.e.: one has BGP and the other has EIGRP.

  Workaround: There is no workaround.

- CSCtj32574

  Symptoms: Deleting the **redistribute** command into EIGRP does not get synchronized to the standby. For example:

  ```
  router eigrp 1
    redistribute connected
    no redistribute connected
  ```

  The **no redistribute connected** command is not being backed up to the standby.

  Conditions: The symptom is observed with any redistribute-related commands.

  Workaround: There is no workaround.

- CSCtj39558

  Symptoms: Sub-interface queue depth cannot be configured.

  Conditions: The symptom is observed when the policy is attached to ethernet subinterfaces.

  Workaround: There is no workaround.

- CSCtj39664

  Symptoms: A router that is running Cisco IOS Release 15.1(2)T1 may crash when attempting to configure Zone-Based Firewall.

  Conditions: The symptoms are observed when attempting to configure zone-pair. It occurs only with a Cisco 861 router.

  Workaround: There is no workaround.

- CSCtj41016

  Symptoms: The assertion failures below will appear on the console continuously in Cisco 888E platform and the router prompt will not do any configurations:

  ```
  ASSERTION FAILED: file "../src-m8300-c880/c880_shdsl_efm_io.c", line 653
  ASSERTION FAILED: file "../src-m8300-c880/c880_shdsl_efm_io.c", line 653
  ASSERTION FAILED: file "../src-m8300-c880/c880_shdsl_efm_io.c", line 653
  ASSERTION FAILED: file "../src-m8300-c880/c880_shdsl_efm_io.c", line 653
  ```

  Conditions: The symptom is observed on Cisco 888E routers.

Workaround: There is no workaround.

- CSCtj41194

  Cisco IOS Software contains a vulnerability in the IP version 6 (IPv6) protocol stack implementation that could allow an unauthenticated, remote attacker to cause a reload of an affected device that has IPv6 enabled. The vulnerability may be triggered when the device processes a malformed IPv6 packet.

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

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-ipv6

- CSCtj47736

  Symptoms: Router crash is seen when doing a **show eigrp service ipv4 neighbor**.

  Conditions: The symptom is observed when the neighbor is learned, then you add a max-service limit on an address family. Then do a shut/no shut on the interface.

  Workaround: There is no workaround.

- CSCtj48629

  Symptoms: Though “ppp multilink load-threshold 3 either” is set, the member links are not added by the inbound heavy traffic on the PRI of the HWIC- 1CE1T1-PRI.

  Conditions: The symptom is observed with Cisco IOS Release 15.0(1)M2.

  Workaround: There is no workaround.

- CSCtj52077

  Symptoms: Policy at subinterface is not accepted with CBWFQ.

  Conditions: This symptom is observed when policy is used in Ethernet subinterface.

  Workaround: There is no workaround.

- CSCtj53363

  Symptoms: Router hangs and console does not respond indefinitely.

  Conditions: The symptom is observed with the following conditions:

  - AIM-VPN in ISR + ZBFW; or
  - A Cisco 2811/2821 Onboard VPN + ZBFW.
  - Once traffic starts, router hangs within minutes.

  Workaround 1: If running a Cisco 2811/2821, use sw crypto + ZBFW.

  Workaround 2: If running with a Cisco 2851 and higher ISRs, use onboard crypto + VPN instead of AIM-VPN + ZBFW.

- CSCtj58943

  Symptoms: Standby RP reloads due to line by line sync failure for **encapsulation dot1q 1381** command:

  ```
  Config Sync: Line-by-Line sync verifying failure on command: encap dot1Q 1381 due to
  parser return error
  rf_reload_peer_stub: RP sending reload request to Standby. User: Config-Sync, Reason:
  Configuration mismatch
  ```

  Conditions: Symptom occurs when issuing a configuration command under a sub-interface mode.

Workaround: There is no workaround.

- CSCtj65553

  Symptoms: Static route that is installed in default table is missing.

  Conditions: Static route is missing after Route Processor (RC) to Line Card (LP) to Route Processor transition on Cisco Catalyst 3000 series switching module.

  Workaround: Configure the missing static route.

- CSCtj66235

  Symptoms: A UC540 that is running Cisco IOS Release 15.1(2)T1 reloads due to software-forced crash while experiencing the following error:

  ```
  %SYS-6-STACKLOW: Stack for process voice file acct dump running low, 0/6000
  ```

  Conditions: The crash suggests that the issue is just one of inefficient stack usage.

  Workaround: There is no workaround.

- CSCtj69577

  Symptoms: When congestion occurs on a QoS-enabled output interface, output rate significantly decreases.

  Conditions: The symptoms are observed under the following conditions:

  1. 3945E outbound interface is connected to 100M link.
  2. QoS (LLQ/Fair Queue) is configured on 3945E outbound interface.
  3. Congestion occurs on outbound interface.

  Workaround: Reload the router.

  Further Problem Description: This issue is resolved after a reload but the shutdown/no shutdown commands can cause the same issue.

- CSCtj69886

  Symptoms: NTP multicast over multiple hops.

  Conditions: This symptom is observed when a multicast server is multiple hops away from multicast clients.

  Workaround: There is no workaround.

- CSCtj77004

  Symptoms: Archive log configuration size impacts CPU utilization during PPPoE establishment. Also, only some configuration lines from the virtual-template are copied to archive (some lines missing).

  Conditions: The symptom is observed when “archive log config” is configured.

  Workaround: There is no workaround.

- CSCtj77477

  Symptom: High delay in priority queue when using CBWFQ/LLQ.

  For example: EFM rate 2304 kbps

  888E Average delay: 42ms
  888E Max delay: 63ms
  HWIC-4SHDSL-E Average delay: 216ms
  HWIC-4SHDSL-E Max delay: 361ms

Conditions: The symptom occurs only on G.SHDSL EFM platforms 888E and ISR with HWIC-4SHDSL-E.

Workaround: Configure hierarchical QoS on WAN G.SHDSL EFM interface.

For example: EFM rate 2304 kbps

```
policy-map CHILD
 class voice
    priority percent 25
 class business
    bandwidth percent 50
policy-map PARENT
 class class-default
    shape average 2100000 8400 0
  service-policy CHILD
```

- CSCtj77819

  Symptoms: When dialer idle-timeout is not explicitly configured on a dialer interface (with PPP multilink configuration), then it is not effective. It is not resetting the idle timeout when outgoing interesting traffic is seen.

  Conditions: The symptom is observed when dialer idle-timeout is not explicitly configured on a dialer interface (with PPP multilink configuration).

  Workaround: Reconfigure “dialer idle-timeout” with any value (even default of 120 secs).

- CSCtj77963

  Symptoms: Resets are observed on low speed links.

  Conditions: The symptom is observed on low speed interfaces over the WAN that produce retransmissions, out of order segments, etc.

  Workaround: There is no workaround.

- CSCtj78210

  Symptoms: One-way audio. Moves from one port to another when the router is rebooted.

  Conditions: The symptom is observed when using multiple “session protocol multicast”, “connection trunk” configurations for LMR, E&M Immediate, and/or other multicast applications, such as the conditions where this was first detected, in a Radio over IP solution. Only affects PVDM3.

  Workaround: Configure conference bridge that is associated with SCCP. The exact numbers to be used to force these ports to be in use will depend on the individual platform.

  For example, configure:

```
voice-card 0 (1... 2... etc...)
dspfarm
dsp service dspfarm

dspfarm profile x conf
max sessions xx << use the maximum
max partic << use the maximum
associate app sccp
no shutdown

dspfarm profile x2 conf
max sessions xx << use the maximum
max partic << use the maximum
associate app sccp
no shutdown
```

```
dspfarm profile x3 conf
max sessions xx << use maximum (if allowed)
max partic << use the maximum (if allowed)
associate app sccp
no shutdown

dspfarm profile x conf
shutdown
no dspfarm profile x conf
```

The idea behind this workaround is to consume all of the upper VOICE DSP channels to disallow them for use by a multicast session.

This workaround will only work if you have enough DSP resources to remove all DSP channels above 16 and still have enough DSP resources for the needed DSP channel/multicast sessions.

- 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.

- CSCtj82292

  Symptoms: EIGRP summary address with AD 255 should not be sent to the peer.

  Conditions: This issue occurs when summary address is advertised as follows:

  ```
  ip summary-address eigrp AS# x.x.x.x y.y.y.y 255
  ```

  Workaround: There is no workaround.

- CSCtj84901

  Symptoms: Cisco routers crash when traffic passes from the MGF port of any module towards the router CPU with a PVDM module present in the router.

  Conditions: This symptom is observed on Cisco 19xx, 2911 and 2921 routers with PVDM modules, as well as any other module that connects to the MGF backplane switch. The modules that currently connect to MGF are

  1. Service Ready Engine modules (ISM and SM SRE)
  2. Etherswitch modules (SM and EHWIC)

  If any traffic from these modules flows over the MGF port towards the router CPU, then the router will crash.

  This symptom is not observed on Cisco 2951, 39XX, or 39XXe routers.

  Workaround: For the EHWIC Etherswitch module with PVDM on the router, there is no workaround.

  For the Etherswitch SM modules and Service Ready Engine modules, as long as the MGF port on these modules is not configured to send traffic to the router, there will be no issue. For traffic between modules over MGF there is no issue. If the MGF port on these modules has to be used, then the PVDM would have to be removed from the router. There is no workaround if both the PVDM and the MGF port on these modules has to be used.

- CSCtj87180

  Symptoms: An LAC router running VPDN may crash when it receives an invalid redirect from the peer with a CDN error message of “SSS Manager Disconnected Session”.

  Conditions: The symptom is observed when the LAC router receives an incorrect “Error code(9):

  ```
  Try another directed and Optional msg: SSS Manager disconnected session <<<< INVALID”
  from the multihop peer.
  ```

  Workaround: There is no workaround.

- CSCtj89941

  Symptoms: IOSd crash when using the command **clear crypto session** on an EzVPN client.

  Conditions: Testbed setup:

  1. RP2+ESP20 worked as the EzVPN simulator, which is configured with over 1000 clients. Then simulator is connected to Cisco ASR 1004-RP1/ESP10 (UUT) with DVTI configured.
  2. Use IXIA to generate 1Gbps traffic.
  3. Wait until all the SAs have been established and traffic is stable.
  4. Use CLI **clear crypto session** on EzVPN simulator.

  Workaround: There is no workaround.

- CSCtj90342

  Symptoms: A Cisco HWIC-2T module installed on a Cisco 2901, 2911 or 2921 router configured with “physical-layer async” (Async mode) delays printing the characters that you type in the terminal window.

  Conditions: This symptom is observed on Cisco 2901, 2911, and 2921 platforms with Cisco HWIC-2T modules installed and running any Cisco IOS 15.X release.

  This symptom is not observed on a Cisco 2951 platform.

  Workaround: There is no workaround.

  Further Problem Description: In a production environment, the first data string may not be transmitted until you enter the second string. For example, reverse telnet to the line using the command prompt of PC. A blank screen is opened where you will type. Now, using hyperterminal software, connect HWIC- 2T to your PC (similar to the console connection). You will see a blank screen on the software. Start typing numbers such as 1,2,3,4, and 5 at the command prompt. “2” will not be displayed until you press “3” at the command prompt, “4” will not show up until you press “5,” and so forth.

- CSCtj91764

  Symptoms: A UC560/UC540 that is running Cisco IOS Release 15.1(2)T1 reloads due to an unexpected exception to CPU.

  Conditions: The crash happens during a complete SNMP MIB walk.

  Workaround: The CISCO-CALL-APPLICATION-MIB can be excluded via configuration.

- CSCtj94617

  Symptoms: Memory leak is seen while issuing the **show running** or the **show ip access-lists** command even though we do not have any named ACL configured on the box.

  Conditions: This symptom is observed when issuing the **show running** command.

  Workaround: There is no workaround.

Further Problem Description: The memory leak is in dynamic list that was created, which is not destroyed properly.

- 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.

- CSCtk02647

  Symptoms: On an LNS configured for L2TP aggregation, it might be that per- user ACLs downloaded via Radius cause PPP negotiation failures (IPCP is blocked).

  Conditions: This symptom is observed when LNS multilink is configured and negotiated for PPP/L2TP sessions and per-user ACL downloaded for PPP users via radius.

  Workaround: There is no workaround.

- CSCtk06548

  Symptoms: Using CCBU CVP solution, SIP calls are disconnected during stress test.

  Conditions: The symptom is observed when using a TCP connection. SIP messages are sporadically corrupted and cannot be framed correctly by SIP stack. It is seen with PI14 image testing.

  Workaround: Use PI12 image.

  Further Problem Description: The fundamental issue involves the selective ack (SACK) feature. An alternative workaround would be to disable the “SACK Permitted” option from the peer.

- CSCtk12608

  Symptoms: Route watch fails to notify client when a RIB resolution loop changes. This causes unresolved routes to stay in the routing table.

  Conditions: The symptoms are observed using Cisco IOS Release 15.0(1)M, 15.1 (2)T and 15.1(01)S and with the following configurations:

  Router 1:

```
interface Ethernet0/0
 ip address 10.0.12.1 255.255.255.0
!

interface Ethernet1/0
 ip address 10.0.120.1 255.255.255.0
!
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 neighbor 172.16.0.1 remote-as 200
 neighbor 172.16.0.1 ebgp-multihop 255
 no auto-summary
!

ip route 0.0.0.0 0.0.0.0 10.10.200.1
ip route 172.16.0.1 255.255.255.255 10.0.12.2
ip route 172.16.0.1 255.255.255.255 10.0.120.2
```

Router 2:

```
interface Loopback200
 ip address 10.10.200.1 255.255.255.0
!
interface Loopback201
 ip address 172.16.0.1 255.255.255.0
!
interface Ethernet0/0
 ip address 10.0.12.2 255.255.255.0
!

interface Ethernet1/0
 ip address 10.0.120.2 255.255.255.0
!
router bgp 200
 no synchronization
 bgp log-neighbor-changes
 network 10.10.200.0
 neighbor 10.0.12.1 remote-as 100
 neighbor 10.0.12.1 update-source Loopback201
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 10.0.12.1
!
```

Workaround: Use static routes tied to a specific interfaces instead of using “floating static routes”.

- CSCtk12681

  Symptoms: Enabling IP SLA trace for VoIP RTP causes a crash.

  Conditions: This symptom is observed when IP SLA TRACE is enabled for VoIP RTP probe.

  Workaround: Disable IP SLA TRACE for VoIP RTP probe.

- CSCtk35953

  Symptoms: The dampening information will not be removed even if dampening is unconfigured in VPNv4 AF.

  Conditions: The symptom is observed only if DUT has eBGP-VPNv4 session with a peer and a same-RD import happens on the DUT for the route learned from VPNv4 peer.

  Workaround: A hard reset of the session will remove the dampening information.

- CSCtk52599

  Symptoms: A Cisco 888E router does not train up with a third-party vendor’s DSLAM.

  Conditions: The symptom is observed when the DSLAM is running the new firmware.

  Workaround: There is no workaround.

- CSCtk53130

  Symptoms: You may be unable to configure pseudowire on a virtual PPP interface. The command is rejected with the following error:

  ```
  Incompatible with ipv6 command on Vp1 - command rejected.
  ```

  Conditions: The symptom occurs when an IPv6 address has already been configured on the virtual PPP interface.

  Workaround: There is no workaround.

- CSCtk53534

  Symptoms: Router crashes.

  Conditions: The symptom is observed with some combination of zone-based firewall and policy configuration and with IPv6 traffic.

  Workaround: Disable global parameter-map.

- CSCtk56570

  Symptoms: When there are some call loads on CUBE, one-way call occurs while call proceeding, after sending SIP CANCEL.

  Conditions: This symptom occurs when media transcoder-high-density is enabled on CUBE.

  Workaround: Disable media transcoder-high-density.

- CSCtk56817

  Symptoms: Router crashes.

  Conditions: The symptom is observed when pinging the dialer interface attached to the ATM interface.

  Workaround: There is no workaround.

- CSCtk62247

  Symptoms: IKEv2 session fails to come up with RSA sign authentication.

  Conditions: The symptom is observed with a hierarchical CA server structure.

  Workaround: Use non-hierarchical CA servers.

- CSCtk66979

  Symptoms: Hold queue on an ATM interface does not work.

  Conditions: This symptom is observed when hold-queue per VC is configured on ATM interfaces (NM-1A-T3/E3) on ISRG2.

  Workaround: There is no direct workaround. It will work only for default hold- queue size or maximum hold queue size under an ATM interface.

- CSCtk67709

  Symptoms: The AnyConnect 3.0 package does not install correctly on the Cisco IOS headend. It fails with the following error:

  ```
  ssl2-uut-3845a(config)#crypto vpn anyconnect flash:anyconnect-win-3.0.0432-
  k9.pkg
  SSLVPN Package SSL-VPN-Client (seq:1): installed %%Error: Invalid Archive
  ```

  Conditions: This symptom is observed with AnyConnect 3.0.

  Workaround: There is no workaround.

- CSCtk74970

  Symptoms: TE autoroute announced tunnel is not installed in the routing table.

  Conditions: The symptom is observed if you configure TE with one hop-LDP and then unconfigure. Then configure TE with one hop with non-LDP. The TE autoroute announced tunnel is not installed in the routing table.

  Workaround: Configure “no ip routing protocol purge interface”.

- CSCtk84116

  Symptoms: A GETVPN ks crash may occur when split-and-merge is happening between the key servers.

  Conditions: This symptom is observed when a split-and-merge occurs between the key servers.

  Workaround: There is no workaround.

- 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 command **dlsw udp-disable**.

  Further Problem Description: This symptom occurs in the following (and later) Cisco IOS 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

- CSCtl04285

  Symptoms: After a BGP flap or provisioning a new session, the BGP route reflector will not advertise new IPv4 MDT routes to PEs.

  Conditions: This symptom is observed with BGP session flap or when provisioning a new session.

  Workaround: Enter the **clear ip bgp *** command.

- CSCtl08014

  Symptoms: Router crashes with memory corruption symptoms.

  Conditions: This symptom occurs when performing switchover or Online Insertion and Removal (OIR), while MLP sessions are initiating.

  Workaround: There is no workaround.

- 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.

- CSCtl21884

  Symptoms: When enabling auto-summary under the BGP process, a BGP withdraw update is not sent even though the static route goes down.

  Conditions: The symptom is observed under the following conditions:

  - Enable auto-summary under the BGP process.

  - Static route is brought into the BGP table via the **network** command.

  Workaround: Use **clear ip bgp *** or disable “auto-summary” under the BGP process.

- CSCtl47666

  Symptom: Intermittent call drops for CME SNR calls that go to voicemail.

  Conditions: This symptom is observed on a Cisco IP phone with SNR configured. When the “no answer” timer is reached, the call will intermittently drop instead of going to voicemail.

  Workaround: There is no workaround.

- CSCtl50815

  Symptoms: Prefixes remain uncontrolled. Additionally, the following message is logged frequently without any actual routing changes:

  ```
  %OER_MC-5-NOTICE: Route changed Prefix <prefix> , BR x.x.x.x, i/f <if>, Reason
  Non-OER, OOP Reason <reason>
  ```

  Conditions: The symptom is observed under the following conditions:

  - Use ECMP.
  - Use **mode monitor passive**.

  Workaround: Remove equal cost routing. For instance, in a situation where you currently use two default static routes, rewrite one of the two with a higher administrative distance and let PfR move traffic to that link as it sees fit. Alternatively, rewrite the two default routes and split them up in 2x /1 statics, one per exit. This achieves initial load balancing and PfR will balance the load correctly as necessary.

  Further Problem Description: In some networks, when you are using equal cost load balancing, several flows that are mapped to a single traffic class/prefix in PfR might exit on more than just a single exit. This can lead to PfR not being able to properly learn the current exit and can cause PfR to be unable to control this traffic.

- CSCtl57055

  Symptoms: A router may unexpectedly reload when the rttMonStatsTotalsEntry MIB is polled by SNMP.

  Conditions: The symptom is observed on a router that is running a Cisco IOS 15.1T release, is configured for SNMP polling, and when the rttMonStatsTotalsEntry is polled with an IP SLA probe configured.

  Workaround 1: Configure NMS to stop polling the rttMonStatsTotalsEntry or create a view and block the MIB on the router.

  Workaround 2: The issue only affects Cisco IOS 15.1T releases, so use a Cisco IOS 15.0(1)M rebuild or earlier.

- CSCtl67195

  Symptoms: The following three BGP debug commands are not allowed to enable:

  debug ip bgp vpnv4 unicast
  debug ip bgp vpnv6 unicast
  debug ip bgp ipv6 unicast

  Conditions: The symptom is observed with the above BGP debug commands.

  Workaround: There is no workaround.

- CSCtl73914

  Symptoms: A Cisco 2921 Gateway that is running Cisco IOS Release 15.1(1)T1 is unable to register with IMS.

  Conditions: The symptom is observed if the P-Associated-URI of the 200 Ok response contains any special characters (!*.!) in Tel URI Parsing.

  Workaround: There is no workaround.

- CSCtl77735

  Symptoms: Saving a configuration to NVRAM may fail.

  Conditions: This symptom may be observed on a Cisco 2900 platform while saving the Cisco IOS configuration.

  Workaround: Erasing the startup configuration and saving again may recover the configuration.

- 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.

- CSCtl88066

  Symptoms: A router reloads (seen with a Cisco ASR 1000 Series Aggregation Services router) or produces a spurious memory access (seen with most other platforms).

  Conditions: The symptom is observed when BGP is configured and you issue one of the following commands:

  show ip bgp all attr nexthop
  show ip bgp all attr nexthop rib-filter

  Workaround: Do not issue either of these commands with the "all" keyword. Instead, issue the address-family specific version of the command for the address family you are interested in.

  For example, the following are safe:

  show ip bgp ipv4 unicast attr nexthop
  show ip bgp attr nexthop
  show ip bgp vpnv4 vrf *vrfname* **attr nexthop**

  Further Problem Description: While the **show ip bgp all attr nexthop** has never done anything that **show ip bgp attr nexthop** did not do, the reload bug was introduced during the development of multi-topology routing. All versions of Cisco IOS which include multi-topology routing or which are derived from versions which included multi-topology routing, and where this fix is not integrated are impacted.

  The fix prevents the issuing of commands beginning with **show ip bgp all attr**.

- CSCtl92014

  Symptoms: After a reprompt element, “enumerate”, using internal variables like _prompt or _dmtf, no longer produces a valid list of options and repeats the last option.

  Conditions: This symptom occurs when running Cisco IOS Release 12.4(15)T and later releases.

  Workaround: There is no workaround.

- CSCtl98270

  Symptoms: Changing the VC hold-queue under the PVC on a WIC-1ADSL card is not reflected correctly in the **show hqf interface** output.

  Conditions: The symptom is observed in Cisco IOS 15.1(2)T2 Release and later releases.

  Workaround: Execute a shut/no shut to fix the issue.

- CSCtn01832

  Symptoms: The following command sequence crashes the router at check syntax mode:

  config check syntax route-map hello match local-preference no match local-preference

  Conditions: The symptom is observed with the commands above.

  Workaround: There is no workaround.

- CSCtn08613

  Symptoms: Cisco router crashes when interfacing with UCCX.

  Conditions: This has been experienced on a UC560 running Cisco IOS Release 15.1(2)T2 when making consult transfer calls.

  Workaround: There is no workaround.

- CSCtn46263

  Symptoms: Memory leaks are seen in ikev2_packet_enqueue and ikev2_hash.

  Conditions: This symptom is observed during retransmissions and window throttling of requests.

  Workaround: There is no workaround.

- CSCtn51740

  Symptoms: Memory leak is seen in EzVPN process.

  Conditions: This symptom is seen when EzVPN connection is configured with split tunnel attributes.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.1(2)T2a

Cisco IOS Release 15.1(2)T2a is a rebuild release for Cisco IOS Release 15.1(2)T. The caveats in this section are resolved in Cisco IOS Release 15.1(2)T2a but may be open in previous Cisco IOS releases.

- CSCtj39558

  Symptoms: Subinterface queue depth cannot be configured.

  Conditions: The symptom is observed when the policy is attached to ethernet subinterfaces.

  Workaround: There is no workaround.

- CSCtj52077

  Symptoms: Policy at subinterface is not accepted with CBWFQ.

  Conditions: This symptom is observed when policy is used in Ethernet subinterface.

  Workaround: There is no workaround.

- CSCtj66235

  Symptoms: A UC540 that is running Cisco IOS Release 15.1(2)T1 reloads due to software-forced crash while experiencing the following error:

  ```
  %SYS-6-STACKLOW: Stack for process voice file acct dump running low, 0/6000
  ```

  Conditions: The crash suggests that the issue is just one of inefficient stack usage.

  Workaround: There is no workaround.

- CSCtj94617

  Symptoms: Memory leak is seen while issuing the **show running** or the **show ip access-lists** command even though we do not have any named ACL configured on the box.

  Conditions: This symptom is observed when issuing the **show running** command.

  Workaround: There is no workaround.

  Further Problem Description: The memory leak is in dynamic list that was created, which is not destroyed properly.

Resolved Caveats—Cisco IOS Release 15.1(2)T2

Cisco IOS Release 15.1(2)T2 is a rebuild release for Cisco IOS Release 15.1(2)T. The caveats in this section are resolved in Cisco IOS Release 15.1(2)T2 but may be open in previous Cisco IOS releases.

- CSCsu95339

  Symptoms: Output from the **show idmgr session** command displays a corrupted service name.

  Conditions: Enter the **show idmgr session** command.

  Workaround: There is no workaround.

- CSCta53372

  Symptoms: A VPN static route is not seen in the RIB after an interface is shut down and brought back up (shut/no shut).

  Conditions: Configure the crypto client and server routers in such a way that the session is up and RRI installs a static route on the server that is pointing to the client IP address. Now shut down the interface on the server router that is facing the client. The RRI static route disappears from the RIB and never reappears.

  Workaround: Reset the RRI session.

- CSCtb55576

  Symptoms: When an HWIC-3G-GSM cellular interface goes up or down [%LINK-3-UPDOWN event log generated], traffic that is traversing the other interfaces is delayed for approximately 160 to 250 ms during the %LINK-3-UPDOWN event.

  Conditions: The symptom is observed on a Cisco 2811 router with an HWIC-3G-GSM. Any time the cellular interface experiences a state change, traffic routed through the Cisco 2811 router is delayed for approximately 160 to 250 ms.

  Workaround: There is no workaround.

- CSCtc33679

  Symptoms: Routes are not being controlled properly when PIRO is used.

Conditions: If more than one exit per BR is configured and PIRO is used to control the routes, the nexthop is not being calculated correctly. As a result, traffic for these traffic classes is not taking the correct route.

Workaround: There is no workaround.

- CSCtc55897

  Symptoms: R2 will not advertise the routes.

  Conditions: The symptom is observed under the following conditions:

  1. R2 has two IBDG neighbors in the same update-group one neighbor with 4BAS and the other with 2BAS capability.

  2. The locally originated routes or routes without any AS_PATH will not be advertised to this kind of group.

  Workaround: Try to make the 2BAS and 4BAS neighbors fall into different update-groups by configuring dummy route-maps.

- CSCtd39579

  Symptoms: A router crashes when we try to remove 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 as well.

  Workaround:

  1. Remove NAT from the interface.

  2. Remove the service policy.

  3. Re-apply NAT.

- CSCte20187

  Symptoms: When bgp next-hop is configured under a VRF, the following error message is seen on the remote PE router:

  ```
  %BGP-3-INVALID_MPLS: Invalid MPLS label (1)
  ```

  The label advertised may be different but it is always a reserved label (0- 15).

  Additionally, the local PE will see No Label as the Outgoing Label in the MPLS forwarding table.

  Conditions: This symptom is observed when bgp next-hop is configured under an interface.

  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.

- CSCte91259

  Symptoms: A Cisco router may unexpectedly reload due to a bus error after displaying an "%IDMGR-3-INVALID_ID" error.

  Conditions: The crash will be seen only if the router is using DHCP Client Dynamic DNS update.

  Workaround: There is no workaround.

- CSCtg53953

  Symptoms: A standby router reloads due to a parser sync issue when applying certain neighbor commands (neighbor <ip-address> disable-connected-check, neighbor <ip-address> peer-group pgrp, and others).

  Conditions: This symptom applies only to situations where <ip-address> is the IP address of a peer that has a dynamically created session (a neighborship that is the result of the "bgp listen range ..." feature).

  Workaround: There is no workaround. Such a configuration should not be applied in the first place.

- CSCtg58786

  Symptoms: When an external interface on the BR is shut down, the BR could be crashed.

  Conditions: If more than one thousand Application Traffic Classes are configured on MC, and if that traffic is traversing through an external interface on a BR, and if the external interface is shut down, this could result in a crash.

  Workaround: There is no workaround.

- CSCtg59956

  Symptoms: Active supervisor crashes when doing an SSO switchover.

  Conditions: The symptom is observed when performing a switchover operation with a lot of L2VPN NLRIs. BGP L2VPN configuration is required.

  Workaround: There is no workaround.

- CSCtg60201

  Symptoms: Unconfiguring the **maximum-path** command does not trigger a backup path calculation.

  Conditions: This symptom is observed if addition-path install is configured along with the **maximum-path** command.

  Workaround: Reconfigure "bgp additional-path install."

- CSCtg84649

  Symptoms: EIGRP is not forming adjacencies over virtual interfaces in a DVTI environment.

  Conditions: This symptom is observed on a Cisco ASR 1000 platform with Cisco IOS Release 12.2(33)XNE or Release 12.2(33)XNF1.

  Workaround: Remove the passive-interface configurations for Virtual-Template and then re-configure the passive-interface designation. For example,

```
Router# show run | b router

router eigrp 100
 network 10.1.0.0 0.0.31.255
 passive-interface default
 no passive-interface Virtual-Template1

Router(config)# router eigrp 100
Router(config-router)# no passive-interface default
Router(config-router)# passive-interface default
Router(config-router)# no passive Virtual-Template 1
```

- CSCtg94250

  Symptoms: Removing **address-family ipv4 vrf <vrf>** (in router BGP) followed by **no ip vrf <vrf>** (where "vrf" is the same) could result in a crash.

Conditions: The symptom is observed in a large VPNv4 scale setup, when applying the following commands to the same VRF back-to-back:

1. **no address-family ipv4 vrf <vrf>**

2. **no ip vrf <vrf>** 3. **ip vrf <vrf>**

The trigger of the BGP crash is a result of a racing condition between event 1 and event 2.

Workaround: Since this is a racing condition, the workarounds are:

1. Not applying (1) before (2).

2. Give sufficient time for (1) to complete before applying (2).

- CSCtg95940

  Symptoms: The DH operation will fail and no further IKEv2 SAs will come up.

  Conditions: This issue can occur with many IKEv2 requests coming at once and when you are using hardware crypto-engine.

  Workaround: There is no workaround.

  Further Problem Description: You can re-start the router and switch to software-crypto engine if needed.

- CSCtg99114

  Symptoms: The following error message with traceback is observed:

  ```
  %IPC-5-REGPORTFAIL: Registering Control Port
  ```

  Conditions: The symptom is observed with ISR routers and with Cisco IOS Release 12.4(24)T or later.

  Workaround: Drop IPC traffic using control-plane policing:

  ```
  class-map match-all ipc
   match access-group name ipc
  policy-map drop-ipc
   class ipc
    drop
  ip access-list extended ipc
   permit udp any any eq 1975
  control-plane
   service-policy input drop-ipc
  ```

- 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-sip

- CSCth11747

  Symptoms: When a switchover occurs with GR enabled, sometimes the NSF states are not preserved and the forwarding entries are lost, leading to packet loss for a few seconds.

Conditions: This symptom is observed only with single sessions with GR configured when the restarting neighbor does a passive open. Chances of hitting this are low since this issue occurs because we receive a new open message before the old tcp session has a chance to reset.

Workaround: Configuring multi-session capability on the neighbor sessions or restricting the restarting neighbors connection to active mode would prevent this issue.

Further Problem Description: When an established session already exists between the GR-enabled routers, and the tcp has not yet notified of reset due to neighbor SSO, if the receiving router gets a new open from the restarting router, as per the RFC it is supposed to tear down the old session and accept the new connection. The old session was being torn down properly but it would take the service reset walker to completely free the session. In case of multi-sessions there was no problem in accepting the new session since multiple sessions are allowed. But in case of a single session that already exists, the new sessions are not allowed until the old session is completely freed. Hence, the new session was getting rejected and notification was sent to the restarting neighbor. The restarting neighbor, upon reception of this notification, would clear the NSF preserve bits and further opens would clear the NSF states on the receiving neighbor and hence the problem. The solution would be to accept the new connections in single session support neighbors when the GR reopen has marked the session for reset and de-linked the topologies. The topologies would be added to the new session and the connection accepted. The old session would be freed when service reset walker is invoked. So, for a transient period of time between the session mark reset and the session free, there would be multiple sessions established on the neighbor even though the neighbor was configured as single session. Dependent DDTS CSCtd99802 and CSCth90239 need to be committed along with this fix to ensure complete working of this functionality.

- CSCth13153

  Symptoms: An incorrect UDLR Reporter exists on a router that is connected to a UDLR link and PIM-SM domain with auto-rp configurable.

  Conditions: This symptom is observed on a Cisco 7200 series router with Cisco IOS Release 15.1(1.16)T0.1.

  Workaround: There is no workaround.

- CSCth15105

  Symptoms: BFD sessions flap after unplanned SSO (test crash).

  Conditions: The symptom is observed on a UUT up with unicast/multicast along with BGP and BFD configurations. For BFD timers of 1*5, 500*8, after doing a test crash (option C followed by 6), we see BFD sessions flap.

  Workaround: There is no workaround.

- CSCth16011

  Symptoms: After a network event is introduced in the network, such as a 3- percent loss, MOS policy will detect the OOP condition. But PfR will let the prefix stay in the OOP condition for some time and then switch over to an alternative exit.

  Conditions: Introduce loss to network.

  Workaround: There is no workaround.

- CSCth18146

  Symptoms: A Cisco SIP gateway may reload unexpectedly due to a release message with no IEs.

  Conditions: This symptom is observed on a SIP gateway with tunneling enabled.

  Workaround: There is no workaround.

- CSCth25634

  Symptoms: The password is prompted for twice for authentication that is falling over to the line password.

  Conditions: This symptom is observed when login authentication has the line password as fallback and RADIUS as primary. For example:

  aaa authentication login default group radius line

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

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

- CSCth31271

  Symptoms: A Cisco ASR router crashes with next-hop recursive.

  Conditions: This symptom is observed after the following tasks are executed:

  1. Configure a route-map with recursive next-hop clause for IP address (for example, 1.2.3.4).

  2. Change the recursive next-hop to IP address (for example, 5.6.7.8).

  3. Apply PBR with this route-map to an interface.

  4. Delete the route-map.

  5. Shut the interface.

  Workaround: There is no workaround.

- CSCth31395

  Symptoms: Frame-relay PVC stays in INACTIVE state.

  Conditions: The symptom is observed with Cisco IOS interim Release 15.0(1) M2.14.

  Workaround: There is no workaround.

- CSCth33949

  Symptoms: An LNS standby crashes when 1000 IPv6 PPPoEoA sessions are cleared from LNS using the **clear ppp all** command.

  Conditions: This symptom is observed when 1000 IPv6 PPPoEoA sessions are cleared from LNS using the **clear ppp all** command.

  Workaround: Use the **cle vpdn tunnel l2tp all** command instead.

- CSCth36740

  Symptoms: A router may experience CRC and Runt errors.

  Conditions: The symptom is observed with Cisco IOS Release 15.0(1)M2 and when the on-board GigabitEthernet interface is hard-coded to 10mb/full duplex. It is seen with the following routers: Cisco 1900 series, Cisco 2900 series, and Cisco 3900 series.

  Workaround: There is no workaround.

- CSCth38699

  Symptoms: Cisco IOS platforms configured for Auto-RP in a multicast environment lose the RP-to-group mappings.

  Conditions: This symptom is observed in Cisco IOS Release 12.2(18)SXF7, Release 12.2(33)SXH4, and Release 12.2(33)SRC4, but it is believed to affect other releases. This symptom occurs when the length of the RP-Discovery packet reaches its limit. If the Mapping Agent receives RP-Announce

packets, increasing the number of multicast groups, and that number makes the limit of the packet size, then an empty RP-Discovery packet is triggered that clears the RP-to-Group mapping tables in all the routers receiving such a packet.

Workaround: Configure static RP-to-Group mappings.

- CSCth42798

  Symptoms: In a very corner case, when BGP is in read-only mode and attributes are deleted before the networks, memory can be corrupted.

  Conditions: The device should be in read-only mode, and attributes should be deleted before networks.

  Workaround: There is no workaround.

- CSCth45413

  Symptoms: The environmental alarm has additional hard disk drive information in the Syslog message.

  Conditions: The symptom is observed when there is one of the following service modules in the system:

  ```
  SM-SRE-900-K9 SM-SRE-700-K9 NME-APPRE-522-K9 NME-APPRE-502-K9 NME-APPRE-302-K9
  NME-WAE-502-K9 NME-NAM-120S NME-NAM-80S NME-NAC-K9 NME-CUE NME-UMG-EC NME-UMG
  ```

  Workaround: There is no workaround.

- CSCth58283

  Symptoms: NAT/CCE interoperability can cause a crash and several other issues.

  Conditions: NAT is enabled.

  Workaround: There is no workaround.

- CSCth62854

  Symptoms: A Cisco router crashes with traceback ospfv3_intfc_ipsec_cmd.

  Conditions: This symptom is observed when the interface is configured with ospfv3, null authentication/encryption, and non-null encryption/authentication.

  Workaround: Remove the ospfv3 area command, then remove the null authentication/encryption.

- CSCth63379

  Symptoms: With two T1 links running ATM with IMA bundling, the proper CEF- attached adjacency for the opposite end of the link does not appear.

  Conditions: This symptom is observed on a Cisco 3800 series device with VWIC- 2MFT-T1.

  Workaround: There is no workaround.

- CSCth65072

  Symptom: A memory leak occurs in the big buffer pool while using the service reflect feature.

  Conditions: This symptom is observed when the service reflection feature is enabled. A packet is generated from service reflection and is blocked by an ACL on the outgoing interface. This will cause the buffer leak.

  Workaround: Remove the ACL on the outgoing interface or permit the packets generated from service reflect on the ACL.

- CSCth67608

  Symptoms: Some groups are missing in the MLD Proxy cache on the Proxy router.

Conditions: This symptom is observed when ipv6 mld host-proxy is applied with existing multicast routes.

Workaround: Clear the multicast routes using clear ipv6 pim topology after applying ipv6 mld host-proxy.

- CSCth69361

  Symptoms: A Cisco 881 router crashes when verifying energywise endpoint using an Orchestrator Agent.

  Conditions: The symptom is observed when “energywise endpoint” is configured on a Cisco 881 and when Orchestrator Agent is running.

  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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-dlsw

- CSCth77531

  Symptoms: A Cisco ASR 1000 Series Aggregation Services router with hundreds of IPv4 and IPv6 BGP neighbors shows high CPU utilization in the BGP-related processes for several hours (more than 2.5).

  Conditions: The symptom is observed with Cisco IOS Release 12.2(33)XNF. The BGP task process uses the most CPU; also, the number of routemap-cache entries should be very high.

```
Router# show ip bgp sum

BGP router identifier 1.1.1.1, local AS number 4739
BGP table version is 1228001, main routing table version 1228001 604000 network
entries using 106304000 bytes of memory
604000 path entries using 31408000 bytes of memory
762/382 BGP path/bestpath attribute entries using 94488 bytes of memory
381 BGP AS-PATH entries using 9144 bytes of memory
382 BGP community entries using 9168 bytes of memory
142685 BGP route-map cache entries using 4565920 bytes of memory
```

  Workaround: Use “no bgp route-map-cache.” This will not cache the route-map cache results, and the issue will not be observed.

- CSCth80893

  Symptoms: POE and Air Connect (AC) on a Cisco 892FW router do not work simultaneously. You cannot connect to the AC console when POE is powered on.

  Conditions: This symptom is observed on a Cisco 892FW router that has both POE and Air Connect with POE powered on.

  Workaround: There is no workaround.

- CSCth82164

  Symptoms: When OCSP is being used as the revocation check method for IKE, only the first connection attempt (after reboot or cache clearing of public RSA keys) undergoes an OCSP check. Subsequent revocation checks are bypassed because the peer's public key appears to be cached indefinitely.

No CRL or other lifetime parameters are involved, OCSP should be consulted for each IKE tunnel setup.

The following messages indicate bypassing the revocation check.

```
*Jul 13 18:43:18.095: ISAKMP:(1002): peer&amp;apos;s pubkey is cached *Jul 13
18:43:18.095: CRYPTO_PKI: Found public key in hash table. Bypassing certificate
validation
```

Conditions: OCSP configured as revocation check method for IKE.

Workaround: There is no workaround.

- CSCth86402

  Symptoms: When flapping a WAN interface, the PIM tunnel disappears.

  Conditions: This happens when flapping a WAN interface after a few hours of working.

  Workaround: Disable multicast routing, then enable it again.

- CSCth87587

  Symptoms: Spurious memory access or a crash is seen upon entering or modifying a prefix-list.

  Conditions: The primary way to see this issue is to have “neighbor <neighbor address> prefix-list out” configured under “address-family nsap” under “router bgp” when configuring/modifying a prefix-list.

  Workaround: There is no workaround.

  Further Problem Description: The issue is only specific to certain scenarios when prefix-lists are used in conjunction with “nsap address-family”.

- CSCth87638

  Symptoms: WIC-based platforms that have a MAC address with a leading 1 does not allow traffic to flow through the card successfully.

  Conditions: The symptom is observed on WIC-based platforms. It was seen originally on an IAD243x using a HWIC-CABLE-D-2.

  Workaround: Manually change the MAC address problem card.

  Further Problem Description: The same card works correctly on a Cisco 1841 router with the default MAC address from the Cisco 1841.

- CSCth91984

  Symptoms: Standby resets continuously.

  Conditions: This symptom is observed when 32 extended communities are configured with the **set extcommunity** command on the active RP.

  Workaround: Unconfigure the **set extcommunity** command.

- CSCth99237

  Symptoms: LNS does not respond to an LCP echo reply when waiting for a response from the AAA server. As a result, the peer may close the session.

  Conditions: The symptom is observed under the following conditions:

  1. If the client starts to send LCP echo requests during the PPP Authentication phase.

  2. If the primary AAA server is unreachable and/or the authentication response is otherwise delayed.

  Workaround: There is no workaround.

- CSCti08336

  Symptoms: PfR moves traffic-class back and forth between primary and fallback links the when PfR Link group feature is used.

  Conditions: The symptoms are most likely to occur when there is one exit in the primary link-group and utilization is one of the criteria. The issue can also occur when there are two links in the primary. A traffic-class is moved from the primary link to the fallback link when the primary link is OOP. After the move, the primary link and the fallback link are “IN” policy. At that time, PfR moves the traffic-class back to primary causing the primary link to go “Out” of policy.

  Workaround: There is no workaround.

- CSCti10016

  Symptoms: After the **format** command is run on a 32-GB or larger disk, the **show** command displays that only 4 GB is free on the device.

  Conditions: The symptom is observed when formatting disk that is larger than 32 GB in capacity.

  Workaround: Use a smaller size disk that has no more capacity than 32 GB.

- 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#*

  or

  2. Upgrade to Cisco IOS Release 15.1(2)T1.

- CSCti13286

  Symptoms: Putting this configuration on a router:

  ```
  router rip
   version 2
   no validate-update-source
   network 10.0.0.0
   no auto-summary
  ```

  ```
  !
  ```

  ```
  address-family ipv4 vrf test
   no validate-update-source
   network 172.16.0.0
   no auto-summary
   version 2
   exit-address-family
  ```

and doing a reload causes the “no validate-update-source” statement to disappear from the VRF configuration (the one under the global RIP configuration remains). This affects functionality, preventing the RIP updates in VRF from being accepted.

Conditions: The symptom has been observed using Cisco IOS Release 15.0(1)M3 and Release 15.1(2)T.

Workaround: There is no workaround.

- CSCti19627

  Symptoms: Extension assigner (EA) application erroneously exits after the first digit of the password is entered.

  Conditions: The symptom is observed when “call-park system application” is configured under telephony-service.

  Workaround: Remove “call-park system application”.

- CSCti22190

  Symptoms: The EIGRP autonomous system command does not NVGEN.

  Conditions:

```
interface Tunnel2
 ip vrf forwarding vpn2
 no ip next-hop-self eigrp 10
```

  Now configure the address-family ipv4 command under legacy mode. For example:

```
router eigrp 10
 no auto-summary
 address-family ipv4 vrf vpn2
 no auto-summary
```

  Now show the running configuration; the autonomous system command is not NVGENed.

  Workaround: Use the “address-family ipv4 vrf vpn2 autonomous 10” command.

- CSCti25280

  Symptoms: An outgoing ISDN call with the module HWIC-2CE1T1-PRI might fail with this error message:

```
**ERROR**: call_setup_ack_proceeding: NO HDLC available b channel 30 call id 0x8007
```

  Conditions: The symptom is observed when there is also a VWIC installed in the chassis (example: VWIC2-2MFT-T1/E1). This issue only happens on an ISR G2 router (Cisco 1900/2900/3900 series routers).

  Workaround: Remove the VWIC.

- CSCti26202

  Symptoms: With a Cisco 3900 series router, Modular Exponent (ModExp) is currently done using software and this leads to bad scalability.

  Conditions: The symptom is observed on a Cisco 3900 series router.

  Workaround: There is no workaround.

- CSCti27128

  Symptoms: A Cisco 2911 router crashes repeatedly when trying to boot up.

  Conditions: This symptom occurs when an IPVS module is installed in the NME slot with an SM-NM adaptor in a Cisco 2911 router. The Cisco 2921 is not affected.

Workaround: There is no workaround if the IPVS module is required. Otherwise, the IPVS module can be removed from the Cisco 2911.

- CSCti34627

  Symptoms: This bug is caused by a problem with the fix for CSCth18982. When a neighbor in multiple topologies is enabled, the open sent for the base topology clears the nonbase topology session for the same neighbor.

  Conditions: A GR-enabled neighbor exists in different topologies, one of them being the base topology.

  Workaround: Disable GR.

- CSCti45042

  Symptoms: When the "reload warm file flash0:<image>" command is issued on a Cisco 3900e router, the router does not boot the specified image due to "System received a Bus Error exception."

  Conditions: This symptom is observed in a Cisco IOS Release 15.1(2.13)T image when the "reload warm file flash0:<image>" command is issued.

  Workaround: There is no workaround.

- CSCti47649

  Symptoms: A router may crash with the message:

  ```
  Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x43563D04
  ```

  Conditions: The symptom is observed when the IOS DHCP server is enabled and DDNS updates are configured on the DHCP server.

  Workaround: There is no workaround.

- 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.

- CSCti55261

  Symptoms: On a phone button that has an overlay with call waiting DNs configured while the first call is connected, there is no audio on the second call and the first call gets disconnected after few seconds. The issue occurs when the second call comes in.

  Conditions: The symptom is observed on a phone button that has an overlay with call waiting DNs and when one DN is at hold state and the other is at connected state. It is seen with a CME that is running Cisco IOS Release 15.1(2)T1.

  Workaround: There is no workaround.

- CSCti69008

  Symptoms: When dampening is configured for many VRFs, doing full vpnv4 radix tree walk and the proposed fix improves convergence by doing subtree walk based on VRF/RD.

  Conditions: Dampening configuration changes for VRFs.

  Workaround: There is no workaround.

- CSCti72836

  Symptoms: The router crashes when removing an ACL.

Conditions: The symptom is observed when the ACL has some IP addresses that index to 127 in the hash table.

Workaround: There is no workaround.

- CSCti86169

  Symptoms: A device that is acting as a DHCP relay or server crashes.

  Conditions: This symptom is observed when the “no service dhcp” command is configured.

  Workaround: There is no workaround.

- CSCti89571

  Symptoms: The WAAS feature cannot be enabled the first time for a new evaluation license.

  Conditions: This symptom occurs when the evaluation license has not been activated.

  Workaround: Enter the waas enable command twice on the interface of the NGWO device.

- 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.

- CSCti93398

  Symptoms: A Cisco 1861 router reloads.

  Conditions: The reload occurs upon booting.

  Workaround: There is no workaround.

- CSCti96028

  Symptoms: A build failure is seen due to the fix committed using CSCti67511 (“Borghetti DSL PHY Firmware upgrade through usb flash”).

  Conditions: When you try to build Cisco 180x platform IOS images.

  Workaround: There is no workaround.

- CSCtj07125

  Symptoms: Cisco IOS WAAS Express uses the burned-in MAC address of the first Ethernet interface as its own local device ID. This device ID is sent as a router identifier to the WAAS Central Manager (WCM) and is communicated to other WAAS peers during autodiscovery.

  On Cisco 1941W platforms, the burned-in MAC address of the first Ethernet interface is 0000.0000.0007, which happens to be the same for all Cisco 1941W routers.

  This will cause the WCM to have two routers that are registered with the same client ID. It might also affect IOS-WAAS operation.

  Conditions: This symptom is observed while registering WAAS on Cisco 1941W platforms with the WCM and enabling WAAS on these platforms.

  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.

- CSCtj25649

  Symptoms: Inline power to ip phone fails on NM-16-ESW and NMD-36-ESW

  Conditions: This symptom is seen on NM-16-ESW and NMD-36-ESW that is using a 15.1(2)T1.1 image.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.1(2)T1

Cisco IOS Release 15.1(2)T1 is a rebuild release for Cisco IOS Release 15.1(2)T. The caveats in this section are resolved in Cisco IOS Release 15.1(2)T1 but may be open in previous Cisco IOS releases.

- CSCtd59027

  Symptoms: The device crashes due to a bus error.

  Conditions: The symptom is observed when crypto is running and configured on the router. There is also a possible connection with EzVPN.

  Workaround: There is no workaround.

- CSCte86038

  Symptoms: High CPU utilization for ATM OAM timer process.

  Conditions: The symptom is observed with a scaled L2 VC configuration.

  Workaround: Increase the AIS RDI timeout with higher number of up and down retries.

- CSCte94301

  None

  Symptoms: IPv6 PBR is not applied to locally-originated ping packets.

  Conditions: This symptom occurs when IPv6 PBR is configured for application to locally-originated ping packets.

  Workaround: There is no workaround.

- CSCtg63096

  Symptoms: The **deny ip any any fragments** command shows a high number of hits for traffic that may not be truly fragmented.

  Conditions: This symptom occurs when “deny ip any any fragments” may be configured at the top of the ACL.

Workaround: There is no workaround.

- 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.

- CSCtg83932

  Symptoms: “Encapsulation aal5auto” may not be enabled under svc mode.

  Conditions: This symptom is observed on a Cisco 7200 router that is running Cisco IOS Release 15.1(2)T.

  Workaround: There is no workaround.

- 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.

- CSCth33500

  Symptoms: NAS port is reported as zero on LNS.

  Conditions: This symptom occurs when “vpdn aaa attribute nas-port vpdn-nas” is configured.

  Workaround: There is no workaround.

- CSCth33804

  Symptoms: Traffic is dropped at CPP with error message “noipv4route” after RP switchover, and traffic on few sessions is dropped.

  Conditions: This symptom occurs when VRF is configured for PPPoE sessions and RP switchover is done with traffic flowing.

  Workaround: Do not configure VRF.

- CSCth35377

  Symptoms: Master router does not reacquire DLSW Circuits after failing over to slave router and back again.

  Conditions: This symptom is observed on a GigabitEthernet interface on a Cisco 2921 master router running DLSW ethernet redundancy and with the following parameters: encapsulation dot1Q xxx ip pim sparse-mode.

  Workaround: Remove “ip pim sparse-mode.”

- CSCth42594

  Symptoms: Remote standby router crashes when you configure and remove “ppp multilink mrru local” under a multilink interface.

Conditions: The symptom is observed with the following conditions:

1. When multilink is bundled with more than one serial interfaces (not seeing this issue with only one serial interface).
2. Seeing this issue from 1500 and above (not seeing this issue when configure and remove “ppp multilink mrru local 1499”).

Workaround: There is no workaround.

- CSCth64589

  Symptoms: The memory allocated at bds_create_link_list & udb_create_ds was leaked. The service policy would not be attached on the interface.

  Conditions: This symptom is seen in Cisco routers loaded with Cisco IOS version of Release 15.1(2.5)T. This happens in corner case configurations where the parent class map has only one filter, which is a nested class.

  Workaround: The following configuration can be modified to make things work.

```
class-map c1
class-map c2
 match class c1

policy-map p1
 class c2

Replace the above configuration as follows:

class-map c1

policy-map p1
 class c1
```

  The results are the same.

- CSCth67811

  Symptoms: Acct-Terminate-Cause is set as “nas-error” in Tunnel stop record when admin clear.

  Conditions: This symptom is seen with admin clear tunnel using the **clear vpdn tunnel l2tp all** command.

  Workaround: There is no workaround.

- CSCth78630

  Symptoms: Call manager or other SAF clients are not able to learn SAF patterns.

  On the forwarder, “show eigrp service-family external-client” displays multiple expired client registrations. The keepalive timer on the stale registrations is 0, and the “Client API Handle” is “0”, however the File Descriptor is still listed in the table. See the following example:

```
abi-4506#sh eigrp service-family external-client
 SAF External Clients
Client Label                 Client API Handle         File Descriptor
ABI_SAF_CLIENT1                     0                         1
```

```
ABI_SAF_CLIENT1                 0                       2
ABI_SAF_CLIENT1                 0                       3
ABI_SAF_CLIENT1                 0                       4
ABI_SAF_CLIENT1                 0                       5
ABI_SAF_CLIENT1                 0                       6
ABI_SAF_CLIENT1                 0                       7
ABI_SAF_CLIENT1                 0                       8
ABI_SAF_CLIENT1                 0                       9
ABI_SAF_CLIENT1                 0                       10
ABI_SAF_CLIENT1                 0                       11
ABI_SAF_CLIENT1                 0                       12
ABI_SAF_CLIENT1                 0                       13
ABI_SAF_CLIENT1                 0                       14
ABI_SAF_CLIENT1                 15                      15
ABI_SAF_CLIENT1                 16                      16
abi-4506#
```

Using the **debug voice saf** command or the **<debug eigrp service-family [external-client {client|messages|protocol}]** command shows the following traceback:

```
%SCHED-3-STUCKMTMR: Sleep with expired managed timer 229C03BC, time 0xF2968
(4d20h ago).
-Process= "SAF-EC FORWARDER", ipl= 4, pid= 235
-Traceback= 11A14818 11A14E3C 11130E54 109A0594 10997584
```

Conditions: This symptom occurs when a SAF client unregisters/re-registers to a SAF forwarder.

Workaround: Reload the router acting as forwarder and ensure there is no unregister/re-register activity on the client (for example, do not restart publishing/subscribing services, etc.).

- CSCth83508

  Symptoms: When performing an SRE install over WSMA, the router crashes and reboots.

  Conditions: The problem is seen when using WSMA to run the **session install** command.

  Workaround: Perform the install manually from a vty session.

- CSCti17190

  Symptoms: A router crashes when we try to do sre install.

  Conditions: This symptom occurs when the TCL file has some missing attributes. The sre install fails and crashes the router.

  Workaround: There is no workaround.

- CSCti18193

  Cisco IOS¬Æ Software Release, 15.1(2)T is affected by a denial of service (DoS) vulnerability during the TCP establishment phase. The vulnerability could cause embryonic TCP connections to remain in a SYNRCVD or SYNSENT state. Enough embryonic TCP connections in these states could consume system resources and prevent an affected device from accepting or initiating new TCP connections, including any TCP-based remote management access to the device.

No authentication is required to exploit this vulnerability. An attacker does not need to complete a three-way handshake to trigger this vulnerability; therefore, this vulnerability can be exploited using spoofed packets. This vulnerability may be triggered by normal network traffic.

Cisco has released Cisco IOS Software Release 15.1(2)T0a to address this vulnerability.

This advisory is posted at
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100812-tcp

- CSCti18745

  Symptoms: If user has configured http port 80 or default http port, then reboots the router, it will produce invalid connection url with port 0. Later the connection from ACS to CPE might fail.

  Conditions: This symptom occurs if user has default http port 80 configured and then reboots the router.

  Workaround: Once router is up and running, again configure some port other than 80, and then reconfigure port 80.

```
Router(config)#ip http port 8000

Rotuer(config)#no ip http port  or ip http port 80
```

- CSCti25063

  Symptoms: Call drops after codec change through midcall INVITE.

  Conditions: This issue occurs when both the codec and direction are changed compared to previous negotiated SDP. This is seen when using Cisco Unified Border Element (CUBE) with Cisco IOS Release 15.1(2)T. See the following topology:

  SIP(1) -- CUBE -- SIP(2)

  Codec G711 is negotiated.

  Next on SIP(2) midcall INVITE is received with updated SDP.

  CUBE detects updated SDP but when sending out INVITE on SIP(1), the SDP still has previous codec G711.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.1(2)T0a

Cisco IOS Release 15.1(2)T0a is a rebuild release for Cisco IOS Release 15.1(2)T. The caveats in this section are resolved in Cisco IOS Release 15.1(2)T0a but may be open in previous Cisco IOS releases.

- CSCti18193

  Cisco IOS Software Release 15.1(2)T is affected by a denial of service (DoS) vulnerability during the TCP establishment phase. The vulnerability could cause embryonic TCP connections to remain in a SYNRCVD or SYNSENT state. Enough embryonic TCP connections in these states could consume system resources and prevent an affected device from accepting or initiating new TCP connections, including any TCP-based remote management access to the device.

No authentication is required to exploit this vulnerability. An attacker does not need to complete a three-way handshake to trigger this vulnerability; therefore, this vulnerability can be exploited using spoofed packets. This vulnerability may be triggered by normal network traffic.

Cisco has released Cisco IOS Software Release 15.1(2)T0a to address this vulnerability.

This advisory is posted at
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100812-tcp

Open Caveats—Cisco IOS Release 15.1(2)T

This section describes possibly unexpected behavior by Cisco IOS Release 15.1(2)T. All the caveats listed in this section are open in Cisco IOS Release 15.1(2)T. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCtb55576

  Symptoms: When a HWIC-3G-GSM cellular interface goes up or down [%LINK-3-UPDOWN event log generated], traffic traversing the other interfaces is delayed for ~160-250ms during the %LINK-3-UPDOWN event.

  Conditions: The symptom is observed on a Cisco 2811 router with an HWIC-3G-GSM. Any time the cellular interface experiences a state change, traffic routed through the Cisco 2811 router is delayed for ~160-250ms.

  Workaround: There is no workaround.

- CSCtb70595

  Symptoms: A Cisco router may experience a crash.

  Conditions: This symptom has been has been observed on a Cisco 2851 running Cisco IOS Release 12.4(25a).

  Workaround: There is no workaround.

- CSCtb79492

  Symptoms: A Cisco AS5400XM is seeing high CPU due to process background load.

  Conditions: This symptom is observed when calls are flowing through this router and the router is trying to access Flash to pull the sound files.

  Workaround: End all voice calls coming to the box, or reload the box.

  Further Problem Description: Steps to Recreate:

  1. Use the **more flash:XXX** command
  2. Observe the CPU utilization increase back to 100%.

- CSCtc06935

  Symptoms: Packet loss occurs between two Cisco Catalyst 3200 MAR routers connected over FESMIC Fast Ethernet ports via wireless radios after upgrading to Cisco IOS Release 12.4(22)T2.

  Conditions: The symptom is observed with the following conditions:

  - After a code upgrade.
  - On Cisco Catalyst 3200s connected via wireless radios.
  - It does not occur on devices directly connected via fiber.

  Workaround: Use Cisco IOS Release 12.4(1a).

- CSCtc52299

  Symptoms: UDP packets broadcast with destination port 53 for 10 minutes. It brings the CPU to 100% and causes router to crash if DNS server is removed.

  Conditions: This symptom is observed With UDP broadcast at port 53 cause the port remain open and CPU hog in 5-10 minutes Router CPU reaches to 100% and does not come down even you stop the broadcast traffic

  Workaround: There is no workaround.

- CSCtd59027

  Symptoms: The device crashes due to a bus error.

  Conditions: The symptom is observed when crypto is running and configured on the router. There is also a possible connection with EzVPN.

  Workaround: There is no workaround.

- CSCtd62885

  Symptoms: IKE renegotiation might fail for minutes while having one peer display:

  ```
  %CRYPTO-6-IKMP_NOT_ENCRYPTED: IKE packet from <ip> was not encrypted and it should
  have been
  ```

  Conditions: This symptom is observed when certificates are used. The signature verification might fail after MM5 or MM6 messages are exchanged preventing the tunnel establishment. The issue seems to affect Cisco IOS Release 12.4(20)T3 and Release 12.4(24)T2 images as well.

  Workaround: Use pre-shared keys.

- CSCtd90030

  Symptoms: A Cisco 2851 router may crash with a bus error.

  Conditions: The symptom is observed when the function calls involve Session Initiation Protocol (SIP) and it is possibly related to an IPCC server. It is seen with Cisco IOS Release 12.4(24)T1 or Release 12.4(24)T2.

  Workaround: There is no workaround.

- CSCte17560

  Symptoms: Offered rate in QoS class shows unusually high values.

  Conditions: The symptom is observed when service-policy is applied on a multilink interface.

  Workaround: There is no workaround.

- CSCte50870

  Symptoms: A Cisco AS5400 crashes due to watchdog timeout. CPU hogs due to the “SERIAL A detect” process are seen before the reload:

  ```
  %SYS-3-CPUHOG: Task is running for (36000)msecs, more than (2000)msecs (36/6),process
  = SERIAL A’detect.
  ```

  After some time the device crashes:

  ```
  %SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = SERIAL A’detect.
  ```

  Conditions: This symptom is observed on a Cisco AS5400 that is running Cisco IOS Release 12.4(24)T2. The serial interfaces of the device are configured with the **autodetect encapsulation xxx** command.

  Workaround: If possible, remove this command to avoid the crashes.

- CSCte89130

  Symptoms: Router experiences a memory leak.

  Conditions: The router is running out of memory due to the CCSIP_SPI_CONTROL process (as shown by the **sh mem alloc total** command).

  Workaround: There is no workaround.

- CSCte93792

  Symptoms: Virtual access bound to an ATM interface does not come up.

  Conditions: The symptom is observed when two ATM interfaces are part of multilink PPP by virtual access in dialer interface. The PVC of one of the ATM interfaces is removed and then re-added. The virtual access of the other ATM interface is affected and does not come up.

  Workaround: There is no workaround.

- CSCte94221

  Symptoms: PPP connection over CDMA link is flapping.

  Conditions: This symptom is observed with Cisco IOS Release 15.0M.

  Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the interface and wait for 2 minutes.

- CSCtf28796

  Symptoms: With async_dialer interface type, PPP fails.

  Conditions: This issue is seen only with async_dialer interface type. There is no issue with async_legacy and async_virtual interface types.

  Workaround: There is no workaround.

- CSCtf41721

  Symptoms: A DMVPNv6 hub might crash when doing a **shutdown** followed by a **no shutdown** on the tunnel interface of the other hub. DMVPNv6 hub crashes at ifs_lookup_prefix_common.

  Conditions: This symptom is observed when DMVPNv6 is configured with 2 hubs and 2 spokes. Hub 2 tunnel is shut and unshut, and hub 1 crashes.

  Workaround: There is no workaround.

- CSCtf50867

  Symptoms: A Cisco router reloads at iprouting_is_hdvrf_idb.

  Conditions: This symptom is observed when configuring pri-group nfas_d with Cisco IOS Release 15.1(01.05)T.

  Workaround: There is no workaround.

- CSCtf94403

  Symptoms: Input buffer drops and throttles are observed on an onboard FastEthernet interface and HWIC ethernet interface of a Cisco 2801 under low traffic conditions.

  Conditions: This symptom appears to be related to the router fragmenting packets, which causes the interface particle pool and then the Normal fallback pool to fill up.

  Workaround: There is no workaround.

- CSCtg06045

  Symptoms: A Cisco IOS router may reload when changing crypto ACL configuration. Crash traceback is seen from the crypto ACL process.

Conditions: This symptom is observed with Cisco IOS Release 12.4(15)T12 with a high CPU stress load.

Workaround: The workaround is to simplify and consolidate the ACE entries in the crypto ACL. Also, reducing the CPU stress level may help.

Further Problem Description: This is very specific to the ACE entries in crypto ACL downloaded from KS. Its pattern of deny alternating host to any and any to host could be part of the root cause.

- CSCtg41606

  Symptoms: With Reverse Route Injection (RRI) configured with the **reverse-route** command, if the crypto map is applied to a multiaccess interface (for example, Ethernet), then egress traffic may fail when the router cannot populate an ARP entry for the crypto peer address.

  Conditions: This symptom is observed when the upstream device does not support proxy arping.

  Workaround: Use the **reverse-route remote-peer next-hop-ip** command instead of the **reverse-route** command.

- CSCtg42271

  Symptoms: A router running Cisco IOS Release 15.0(1)M1 may experience a series of spurious memory access errors and a bus error when configured for IPS:

  ```
  %ALIGN-3-SPURIOUS: Spurious memory access made at 0xXXXXXXXX reading 0xXXX
  %ALIGN-3-TRACE: -Traceback= 0xXXXXXXXX 0xXXXXXXXX 0xXXXXXXXX 0xXXXXXXXX 0xXXXXXXXX
  0xXXXXXXXX

  %ALIGN-1-FATAL: Illegal access to a low address 13:35:23 CDT Tue Apr 20 2010
  addr=0x70, pc=0x251A00CCz , ra=0xFFFF3331z , sp=0x28F88EB0

  %ALIGN-1-FATAL: Illegal access to a low address 13:35:23 CDT Tue Apr 20 2010
  addr=0x70, pc=0x251A00CCz , ra=0xFFFF3331z , sp=0x28F88EB0

  XX:XX:XX XXX XXX XXX XX XXXX: TLB (store) exception, CPU signal 10, PC = 0xXXXXXXXX
  <snip>
  ```

  Conditions: This symptom is observed on devices configured for IPS and running Cisco IOS Release 15.0(1)M1.

  Workaround: There is no workaround.

- CSCtg42904

  Symptoms: After applying the flow monitor to a virtual-template interface, a Cisco router crashes with the following error message:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address
  ```

  Conditions: This symptom is observed on a router configured with EasyVPN.

  Workaround: There is no workaround.

- CSCtg49868

  Symptoms: CUBE does not pass the RTP in both directions between two pbx devices

  Conditions: This symptom is observed with the following topology:

  PbxA (SAP BCM)---SIP--->CUBE---SIP--->PbxB(OCS 2007 R2)

  This problem is specific to the two third-party vendor SIP servers, SAP BCM and OCS 2007 R2. This problem only occurs when making a call from pbxA (SAP BCM) to pbxB(OCS 2007 R2). The call is okay from pbxB(OCS 2007 R2) to pbxA (SAP BCM).

  Workaround: Use E1 loop.

- CSCtg54606

  Symptoms: Ping fails over a serial interface with x25 encapsulation.

Conditions: This symptom is observed on a Cisco router running Cisco IOS Release 15.1(1.10)T.

Workaround: There is no workaround.

- CSCtg55338

  Symptoms: If a router is reloaded with a GRE tunnel interface configured with tunnel protection and a dialer interface as the tunnel source, the crypto socket is not created and IPSec is not triggered.

  Conditions: This symptom is observed after reload. A router crypt socket is missing.

  Workaround: After the reload, remove and reapply the tunnel protection on each tunnel interface.

- CSCtg59158

  Symptoms: Router console is flooded with the following error messages:

  ```
  crypto_engine_ps_vec: DF_BIT_STATUS_OK Check failed
  crypto_engine_ps_vec: DF_BIT_STATUS_OK Check failed
  ```

  Conditions: This symptom is observed when new SAs are installed during rekeys or after clearing existing SAs. This symptom is observed when GETVPN (crypto map) is configured along with WAAS.

  Workaround: Cryptomaps are currently not supported in the current phase of WAAS-Express. Use VTI or unconfigure WAAS-Express.

- CSCtg65423

  Symptoms: SS7 and RUDP backhaul fails to bring up links correctly on Cisco IOS Release 15.1T.

  Conditions: This symptom is observed in Cisco IOS Release 15.1T with interworking with PGW.

  Workaround: Install Cisco IOS Release 12.4T.

- CSCtg66989

  Symptoms: NDR performance is degraded by 10% on GRE with IPSec.

  Conditions: This symptom is observed on GRE with IPSec.

  Workaround: There is no workaround.

- CSCtg67146

  Symptoms: File transfer to the flash fails with a “TF I/O failed in data-in phase” message. The **archive** command fails 100% of the time, whereas a **copy** command is successful sometimes.

  Conditions: This symptom is observed on a Cisco router running Cisco IOS Release 12.4(24)T or above and with an STI flash 7.2.0. The transfer fails with some delay (~50-100msec).

  Workaround:

  - Transfer without a delay is successful.
  - Transfer with Cisco IOS Release 12.4(9)T is successful.
  - Transfer with a newer flash card (tested with Sandisk 8.0.0) is successful.

  Further Problem Description: This symptom is also observed with Cisco IOS Release 12.4(24)T, Release 12.4(24)T1, Release 12.4(24)T2, Release 12.4(24)T3 and Release 15.1(1)T.

- CSCtg68568

  Symptoms: A Cisco 3945 router configured as a GETVPN group member might crash when passing stateful traffic.

  Conditions: This symptom occurs when fragmentation of the IP datagram is required due to an MTU limit of 1500 bytes.

Workaround: Configure hosts to negotiate lower TCP MSS (1360) bytes and avoid fragmentation.

- CSCtg71332

  Symptoms: Using NM-1T3/E3-T3 controller will be down/down on Cisco 3800 ISR routers.

  Conditions: This symptom is observed on a Cisco 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 to Cisco IOS Release 12.4(24)T.
  3. Install one or more PVDM slots.

- CSCtg72455

  Symptoms: Async interface for an internal V.92 modem on a Cisco 1811 router freezes for approximately 5 to 30 minutes, but eventually fixes itself.

  Conditions: This symptom is observed on a Cisco 1811 router that is running Cisco IOS Release 15.0 and above.

  Workaround: Disable the V.44 compression by configuring the Cisco 1800/890 modem to negotiate V.42bis by using the following modemcap:

  ```
  1811 V.92 modemcap:
  modemcap entry V.42bis:MSC=&F\N4%C0+DS=3
  Sample chat-script:
  chat-script dial "" "ATD\T" TIMEOUT 60 CONNECT \p
  ```

  The following is a sample line configuration to apply the above chat-script:

  ```
  line 1
   script dialer dial
   modem InOut
   no exec
   transport input all
   transport output all
   stopbits 1
   speed 115200
   flowcontrol hardware
  ```

- CSCtg75710

  Symptoms: BGP convergence time is about 8% greater than in unaffected releases.

  Conditions: This symptom is observed only when BGP is configured. It is most notable when using VPNv4 with hundreds of VRFs and hundreds of thousands of networks.

  Workaround: Wait a little bit longer for BGP to converge.

- CSCtg78691

  Symptoms: A Cisco SPA525G IP phone communicating via SSL VPN from a remote office is experiencing choppy and poor quality audio.

  Conditions: This symptom is observed on a Cisco SPA525G IP phone running firmware version 7.4.3 on Cisco Unified CME 8.0. The symptom is observed only when the phone is connected via SSL VPN; the audio quality of the same phone connected in the LAN network is clear.

  Workaround: There is no workaround.

Further Problem Description: Choppy audio is heard by the Cisco SPA525G as well as the PSTN party when the Cisco SPA525G connects to the corporate network via SSL VPN. The first 10 seconds of the audio is clear, and then the choppiness starts. The CPU spikes to over 90% due to SSLVPN_PROCESS.

- CSCtg81560

  Symptoms: A Cisco router crashes.

  Conditions: This symptom is observed when Cisco IOS firewall is configured.

  Workaround: There is no workaround.

- CSCtg83804

  Symptoms: A Cisco router crashes when uploading files larger than 1 MB via WebVPN.

  Conditions: This symptom is observed when CEF and the crypto engine are enabled.

  Workaround: Disable the CEF and/or disable the crypto engine.

- CSCtg84222

  Symptoms: The VRF tunnel flaps when attaching the QOS policy in the tunnel. This problem can cause traffic drop on a tunnel over an ATM subinterface when a service policy is installed.

  Conditions: This symptom occurs when a service policy is attached to an ATM sub interface and the router has OSPF or EIRGP routing protocol configured. Both the subinterface and routing protocol need to be in the same VRF.

  Workaround: There is no workaround.

- CSCtg89893

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

  Conditions: This symptom is observed on a Cisco 2811 router that is running Cisco IOS Release 12.4(22)T3.

  Workaround: There is no workaround.

- CSCtg90518

  Symptoms: The output of “sh ip inspect statistics” shows negative or irrelevant value(s). The following log is generated:

  ```
  %FW-4-ALERT_ON: getting aggressive, count (6/2147483647) current 1-min rate:
  4294967295
  ```

  Conditions: This symptom is observed on Cisco IOS Firewall on Cisco IOS Release 15.0(1)M where ip inspect tcp is enabled.

  Workaround: There is no workaround.

- CSCtg92548

  Symptoms: The D-channel in the PRI module loses “receive” from the carrier and the controller goes down. If HWECAN DSP is down or crashed, then the D-Channel “receive” data stream would not be passed from the multiflex trunk (MFT) RX input to the IOS PRI Controller, which matches the symptom that was observed.

  Conditions: This symptom is observed on an MFT equipped with HWECAN. The failure occurs intermittently; this failure occurred 6 months after the last HWECAN failure.

  Workaround: Remove HWECAN from the MFT module.

- CSCth03379

  Symptoms: A Cisco router reloads while booting with DSL configurations.

Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 15.1(1.15)T and configured with a DSL controller.

Workaround: There is no workaround.

- CSCth04187

  Symptoms: FTP (both active and passive) to the Internet fails.

  Conditions: This symptom is observed on a Cisco router with inspect and crypto map configured on public interface, and an access-group on the inside interface. When the crypto map is applied on the public interface, FTP fails. As soon as we remove the crypto map, FTP works.

  Workaround: Remove the crypto map from the public interface.

- CSCth06209

  Symptoms: A Cisco router reloads in a loop.

  Conditions: This symptom is observed when WAAS is enabled in the configuration and traffic is flowing through the box, and the router is then reloaded using a laptop.

  Workaround: Disconnect the laptop from the router and hard reset the router.

- CSCth07336

  Symptoms: Data calls cannot be dialed when using E1 PRI on a Cisco 2911 router with VWIC2-1MFT-T1/E1. The call lasts for 22 seconds and when using PPP, LCP fails to negotiate.

  Conditions: This symptom is observed when using E1 PRI for making data calls; HDLC as well as PPP have the same issue, but data calls can be made with the T1 PRI.

  Workaround: There is no workaround.

- CSCth09876

  Symptoms: Cisco IOS IP Service Level Agreements (SLAs) cannot be auto-discovered if IP SLAs are removed from the responder first.

  Conditions: This symptom is observed on a Cisco device after IP SLAs have been unconfigured. Subsequent attempts to reconfigure the device as an IP SLAs responder fail.

  Workaround: Reload the router and configure the device as an IP SLAs responder.

- CSCth10764

  Symptoms: PPP negotiation is not working correctly between a Cisco 7200 router and a Cisco GSR XR blade.

  Conditions: This symptom is observed when the max-header size is different on both ends; PPP does not negotiate the lower size.

  Workaround: There is no workaround.

- CSCth12935

  Symptoms: Input CoPP alone does not work for MPLS-VPN tagged packets. All packets match the default “class-default” class. However, if output CoPP is configured together with input CoPP, input CoPP works fine for MPLS-VPN tagged packets. Packets match the intended user-configured class and can be dropped.

  Conditions: This symptom is observed in Cisco IOS Release 12.4 since Release 12.4(23) on the Cisco 7200 series router. In Cisco IOS Release 12.4 releases older than Release 12.4(23), input CoPP does not work at all for MPLS-VPN tagged packets, even if output CoPP is also configured together with input CoPP.

  Workaround: There is no workaround.

- CSCth13153

  Symptoms: An incorrect UDLR reporter occurs on a Cisco router that is connected to a UDLR link and PIM-SM domain with auto-RP configurable.

  Conditions: This symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 15.1(1)T1.

  Workaround: There is no workaround.

- CSCth15519

  Symptoms: A Cisco router reloads with **show memory** *address_value* command.

  Conditions: This symptom is observed on a Cisco 1861 router.

  Workaround: There is no workaround.

- CSCth16539

  Symptoms: A Cisco device crashes.

  Conditions: This symptom is observed a few hours after multiple T1s are configured in a multilink PPP bundle.

  Workaround: Do not use HDLC encapsulation or remove outbound service-policy from any HDLC-encapsulated serial interfaces.

  Further Problem Description: The Cisco device has traffic coming in a multilink PPP bundle with multiple T1s. This traffic exits out of an HDLC serial interface with an outbound service-policy applied to that interface, eventually causing a crash.

- CSCth16962

  Symptoms: The primary KS KEK timer will get stuck after a GDOI policy change, resulting in repeated rekeys. This symptom seems to occur even after a failure in the key servers

  Conditions: This symptom is observed with repeated rekeys to GMs.

  Workaround: There is no workaround.

- CSCth18189

  Symptoms: A Cisco router crashes when multiple SVIs are created and deleted using the **interface range** command.

  Conditions: This symptom is observed when a Cisco EHWIC-D-8ESG card is present in the router and a user tries to create and delete multiple SVIs using the **interface range** command.

  Workaround: There is no workaround.

- CSCth19516

  Symptoms: A Cisco router crashes when PFR is configured and there is a changeover from primary to fallback link.

  Conditions: This symptom is observed when PFR is configured with link group.

  Workaround: Remove the PFR link group and use traditional routing instead of PFR.

- CSCth20018

  Symptoms: A Cisco router crashes after configuring and removing the onboard GE subinterface.

  Conditions: This symptom is observed on a Cisco router with a basic configuration.

  Workaround: There is no workaround.

- CSCth20696

  Symptoms: An address Error (load or instruction fetch) exception occurs (CPU signal 10).

  Conditions: This symptom is observed on a Cisco 7204vxr router with an NPE-G1 that is running Cisco IOS Release 12.4(25c).

  Workaround: There is no workaround.

- CSCth23354

  Symptoms: Packets are not reaching the proper queue.

  Conditions: This symptom is observed when class-map is configured with VLAN.

  Workaround: There is no workaround.

- CSCth23908

  Symptoms: QSIG APDU in PRI release message in SIP 603 is not passed to PRI side.

  Conditions: This symptom is observed in SIP 603 in the release message on egress PRI side.

  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.

- CSCth27442

  Symptoms: A Cisco router crashes when flapping ACL with traffic flowing.

  Conditions: This symptom is observed on a Cisco 7200 series router running Cisco IOS Release 15.0(1)M2 with the following configuration:

```
no access-list 12 permit 192.1.1.170
no access-list 112 permit ip host 192.1.1.249 any
ip access-list extended dc-gab
no deny   ip any 192.15.2.0 0.0.0.255
no permit ip any 192.235.0.0 0.0.255.255
ip access-list extended dc-sli
no deny ip any 192.22.1.0 0.0.255.255
no permit ip any 192.222.0.0 0.0.255.255
no ip access-list extended dc-sli
no ip access-list extended dc-gab
access-list 12 permit 192.1.1.170
access-list 112 permit ip host 192.1.1.249 any
ip access-list extended dc-gab
deny   ip any 192.15.2.0 0.0.0.255
permit ip any 192.235.0.0 0.0.255.255
ip access-list extended dc-sli
deny ip any 192.22.1.0 0.0.255.255
permit ip any 192.222.0.0 0.0.255.255
```

  Workaround: Remove the ACL without removing the ACEs first by entering the **no ip access-list extended dc-gab** command. If you flap the ACL configuration in the following way, it is equivalent of the original configuration, but it will NOT crash the router:

```
conf t
no access-list 12 permit 192.1.1.170
no access-list 112 permit ip host 192.1.1.249 any
```

```
no ip access-list extended dc-sli
no ip access-list extended dc-gab
access-list 12 permit 192.1.1.170
access-list 112 permit ip host 192.1.1.249 any
ip access-list extended dc-gab
deny   ip any 192.15.2.0 0.0.0.255
permit ip any 192.235.0.0 0.0.255.255
ip access-list extended dc-sli
deny ip any 192.22.1.0 0.0.255.255
permit ip any 192.222.0.0 0.0.255.255
```

- CSCth28007

  Symptoms: Cisco IP phone users may experience dropped calls, resetting phones, and one-way audio.

  Conditions: These symptoms are observed on a Cisco 3825 router that is running Cisco IOS Release 15.1(1)T and CME 8.0 when there are 4 or more active calls. The symptoms occur with the following topology:

  ```
  Router/ PBX ---pri---- CISCO3825 ----sccp---- ip phone.
  ```

  It is a normal external call: PSTN <-----> IP phone calls.

  Workaround: Install Cisco IOS Release 12.4(15)XZ2 or another release earlier than Release 15.n.

  Further Problem Description: With “term mon” turned on, the following message is displayed and IP phones are deregistered from CME:

  ```
  %C5510-4-NO_RING_DESCRIPTORS: No more ring descriptors available on slot 0 dsp 3.
  %C5510-4-NO_RING_DESCRIPTORS: No more ring descriptors available on slot 0 dsp 3.
  %IPPHONE-6-REG_ALARM: 10: Name=SEP00235EB6BC89 Load= SCCP70.8-5-3S Last=TCP-timeout
  %IPPHONE-6-UNREGISTER_ABNORMAL: ephone-7:SEP00235EB6BC89 IP:10.0.3.130 Socket:5
  DeviceType:Phone has unregistered abnormally.
  ```

  Test calls indicate that the router behaves normally when there are 3 or fewer active calls. As soon as a fourth active call is established, however, users may lose access to the router (no icmp ping respond), or experience one-way audio or phones deregistering from CME.

  When the symptoms occur, the **show process cpu** command indicates that the router CPU utilization has gone above 90%. The problem is resolved as soon one of the active calls is dropped and there are 3 or fewer active calls.

- CSCth30648

  Symptoms: HWIC-1ADSL is not staying connected to the provider.

  Conditions: This symptom is observed on a Cisco 1841 router.

  Workaround: There is no workaround.

- CSCth31395

  Symptoms: A frame-relay PVC stays in INACTIVE state.

  Conditions: This symptom is observed in Cisco IOS Release 15.0(1)M2.14.

  Workaround: There is no workaround.

- CSCth31939

  Symptoms: A Cisco device crashes when policy map and oam-pvc manage are configured.

  Conditions: This symptom is observed when policy map and oam-pvc manage are configured.

  Workaround: There is no workaround.

- CSCth33500

  Symptoms: NAS port is reported as zero

Conditions: This symptom is observed when “vpdn aaa attribute nas-port vpdn-nas” is configured.

Workaround: There is no workaround.

- CSCth36114

  Symptoms: A Cisco device crashes after executing “write memory” via SDM.

  Conditions: This symptom is observed on a Cisco 1841 platform that is running Cisco IOS Release 15.1(1)T.

  Workaround: Install Cisco IOS Release 12.4 or earlier.

- CSCth36740

  Symptoms: A Cisco device may experience CRC and Runt errors when the on-board GigabitEthernet interface is hard coded to 10mb/Full duplex.

  Conditions: This symptom is observed on a Cisco 3925 that is running Cisco IOS Release 15.0(1)M2.

  Workaround: There is no workaround.

- CSCth37092

  Symptoms: A crash is observed in the PKI-HA feature when standby tries to sync up with active router.

  Conditions: This symptom is observed after a PKI server is created on the active router and cloning of this PKI server on the standby box occurs.

  Workaround: There is no workaround.

- CSCth37580

  Symptoms: Dampening route is present even after removing bgp dampening.

  Conditions: This symptom is observed in Cisco IOS Release 15.1(1)T1.

  Workaround: There is no workaround.

- CSCth38964

  Symptoms: Unknown SSH session may cause the router to crash.

  Conditions: Unknown. The symptom is observed during an SSH attack.

  Workaround: Disable SSH or configure an access list to block invalid addresses.

- CSCth39161

  Symptoms: Duplicate NAT mappings may impact the use of IP Telephony devices operating behind NAT.

  Conditions: This symptom is observed on the Cisco IAD881.

  Workaround: There is no workaround.

- CSCth44275

  Symptoms: A Cisco router may reload due to memory corruption when making multiple on-ramp fax calls.

  Conditions: This symptom is observed on Cisco 2900 series platforms.

  Workaround: There is no workaround.

- CSCth45413

  Symptoms: The environmental alarm contains additional hard-disk drive information in the Syslog message.

Conditions: This symptom is observed when one of the following Cisco service modules is in the system:

- SM-SRE-900-K9
- SM-SRE-700-K9
- NME-APPRE-522-K9
- NME-APPRE-502-K9
- NME-APPRE-302-K9
- NME-WAE-502-K9
- NME-NAM-120S
- NME-NAM-80S
- NME-NAC-K9
- NME-CUE
- NME-UMG-EC
- NME-UMG

Workaround: There is no workaround.

- CSCth48457

  Symptoms: A Cisco device may crash at qos_classify_opttype

  Conditions: This symptom is observed when changes are made to the service policy while traffic is running.

  Workaround: Define the policy-map you wish to run before applying it on the interface level.

- CSCth48467

  Symptoms: FAX Passthrough will not up speed from G729 to G711.

  Conditions: This symptom is observed when MGCP is configured. The topology is as follows:

  Modem--{Telco}--[Nortel IWTSPM IP to TDM RTP]--|--[Nortel Cs2K]--|--[IAD2435]==FXS==[FAX]

  Workaround: There is no workaround.

- CSCth50582

  Symptoms: Dialer interfaces are not getting IP addresses from the IPCP pool after the main ATM interface flaps.

  Conditions: This symptom is observed on Cisco routers that are running Cisco IOS Release 15.1(2)T.

  Workaround: There is no workaround.

- CSCth51143

  Symptoms: A Cisco router crashes when trying to free a chunk with a non-zero refcount.

  Conditions: This symptom is observed when browsing the internet through a laptop.

  Workaround: There is no workaround.

- CSCth51168

  Symptoms: An H.323 to H.323 CUBE may incorrectly reuse existing TCP sockets when completing H.323 calls. This leads to call failures with cause values of:

```
18 - No user responding; or
102 - Recovery on timer expiry
```

Conditions: This symptom is observed on a Cisco 7206VXR CUBE handling 100+ calls and running Cisco IOS Release 12.4(22)T5.

Workaround: Disable reuse of TCP sockets with the **voice service voip h323 h225 timeout tcp call-idle value 0 !** command.

- CSCth52485

  Symptoms: A call from the PSTN reaches an AC agent via the AC Route Point, and the call is successfully answers. The AC agent then attempts a blind transfer using the AC to another IP Phone, but after around 8 seconds of silence the call is dropped.

  On the CUBE we see the following (the below messages exclude the communication between the CUCM and the CUBE as it is irrelevant):

```
<- Invite outbound to the PGW
-> 200 OK inbound from the PGW
<- ACK outbound to the PGW
<- UPDATE outbound to the PGW
-> 200 OK inbound from the PGW
<- Invite outbound to the PGW
-> 200 OK inbound from the PGW
<- ACK outbound to the PGW
<- Invite outbound to the PGW
-> 491 Request Pending inbound from the PGW
<- ACK outbound to the PGW
```

  Then the CUBE receives a BYE after 8 seconds from the CUCM and forwards this to the PGW and the call terminates.

  After receiving the 491 Request Pending, the CUBE is not forwarding this to the CUCM, whereas all previous SIP messages are forwarded successfully.

  The CUBE should forward this 491 to the CUCM, and then the CUCM should react by sending the Invite again for which it received the 491 Request Pending.

  Conditions: This symptom is observed in Cisco IOS Release 12.4(24)T.

  Workaround: There is no workaround.

- CSCth52720

  Symptoms: Client-initiated L2TPv2, IPCP packets are not sent when MLP is enabled.

  Conditions: This symptom is seen when ppp multilink is configured with Cisco IOS Release 12.4(24)T3, Release 12.4(11)XJ and Release 15.1(1)T.

  Workaround: Remove ppp multilink configuration or downgrade to Cisco IOS Release 12.3(14)T6.

- CSCth53056

  Symptoms: Alignment errors are seen on Cisco IOS Release 12.4(24)T1.

  Conditions: This symptom is observed on Cisco 2800 but is not platform dependent.

  Workaround: There is no workaround.

- CSCth54832

  Symptoms: Ping fails when the clients in different VLANs communicate with each other with a packet size greater than the configured MTU size on the SVIs.

  Conditions: This symptom occurs when using any MTU size less than 1500 on the SVIs.

  Workaround: Configure the same MTU size in the entire path.

- CSCth55781

  Symptoms: The Cisco AS5400XM gateway is rebooting due to the following error:

  ```
  %SNMP-3-DVR_DUP_REGN_ERR: Attempt for dupe regn with SNMP by driver having ifIndex
  529 and ifDescr

  Serial7/2:23-Signaling
  ```

  Conditions: This symptom is observed on the Cisco AS5400XM gateway.

  Workaround: There is no workaround.

- CSCth56502

  Symptoms: A router that is running Cisco IOS may crash when executing the **show run** or **write mem** commands.

  Conditions: This symptom is observed when the device has "memory record traceback" configured.

  Workaround: There is no workaround.

- CSCth57542

  Symptoms: The "show voice dsp command history 1/1:0" reloads Cisco AS5400XM router if slot1 is having T1 controller.

  Conditions: This symptom is observed in Cisco IOS Release 15.1(2.5)T.

  Workaround: Apply **show voice dsp command history** command only for the slots having PVDM.

- CSCth59156

  Symptoms: In a router that is running Cisco IOS Release 15.0(1)M, it was observed that the memory got fragmented over a period of 5 weeks. The problem was seen in only one router. We are waiting for more show command outputs to investigate why the free blocks are not getting coalesced.

  Conditions: This symptom is seen on a router that is running Cisco IOS Release 15.0(1)M.

  Workaround: There is no workaround.

- CSCth59784

  Symptoms: Process watchdog timeout crashinfo is not written on steelers box.

  Conditions: This symptom occurs when process watchdog timeout crashinfo file is not written into flash for steelers platforms.

  Workaround: There is no workaround.

- CSCth60192

  Symptoms: A router crashes with WAAS-EX.

  Conditions: This symptom occurs when configuring WAAS-EX and starting data traffic.

  Workaround: There is no workaround.

- CSCth61759

  Symptoms: Video call fails with CVTA.

  Conditions: This symptom is observed with end-to-end SIP flow-around call with CVTA.

  Workaround: There is no workaround.

- CSCth61827

  Symptoms: Invalid memory action is followed by traceback when traffic is on.

  Conditions: This symptom occurs on a Cisco 7200 router that is running Cisco IOS Release 15.1(2.5)T.

Workaround: There is no workaround.

- CSCth62136

  Symptoms: ISDN L2 goes to “Layer 2 NOT Activated”.

  Conditions: This symptom is observed when Service-Policy is attached to the Dialer Interface.

  Workaround: Remove Service-Policy from interface.

  Further Problem Description: This is not seen with Cisco IOS Release 12.4(13d) and Release 12.4(15)T12.

  It has been seen with Cisco IOS Releases 12.4(22)T5, 12.4(24)T3, and 15.0(1)M3.

- CSCth62157

  Symptoms: Router crashes when pumping data (HTTP, TELNET, FTP). This traffic is inspected by Cisco IOS firewall, and WAAS is configured.

  Conditions: This symptom is observed while pumping in continuous data traffic for a duration of one hour. This traffic is optimized by WAAS and inspected by Cisco IOS firewall.

  Workaround: Remove Cisco IOS FW Zone membership under WAAS interface.

- CSCth63196

  Symptoms: The sip source interface binding commands disappear after being configured and functional.

  Conditions: This symptom is observed when the T1 subinterface, which is bound, flaps.

  Workaround: Reapply the CLI manually.

- CSCth64468

  Symptoms: V110 call fails after the previous call was terminated with +++ ATH.

  We do not see the BAD-modem issue caused by CSCtg52450 anymore, but we now see NO CARRIER. See the following example:

```
NLAMSB1-LRTR01 line 0/322 DialOUT_Modems

at
OK
atz
OK
at+isp=0
OK
at+ipt=4
OK
atdi222
CARRIER RX: 9600 TX: 9600
PROTOCOL: V110
CONNECT
NLAMSB1-LRTR02>
NLAMSB1-LRTR02>
NLAMSB1-LRTR02>+++ATH
% Bad IP address or host name
% Unknown command or computer name, or unable to find computer address
NLAMSB1-LRTR02>
OK
at
OK
at
OK
atz
OK
at+isp=0
```

```
OK
at+ipt=4
OK
atdi222
NO CARRIER
```

Conditions: This symptom is seen when V110 call fails after the previous call was terminated with +++ ATH.

Workaround: Use Cisco IOS **exit** or **logout** commands.

Further Problem Description: Log when doing the first call and after braking it with +++ ATH:

```
%CALLRECORD-3-V12_TERSE_CALL_REC: DS0
slot/contr/chan=0/0/30, slot/port=0/322, call_id=1, userid=(n/a), ip=0.0.0.0,
calling=221, called=222, std=V110, prot=None, comp=None, init-rx/tx
b-rate=9600/9600, finl-rx/tx b-rate=9600/9600, rx/tx chars=0/0, retx=0,
retx-per-frame=0, local-retrains=0, remote-retrains=0, local-rate-reneg=0,
remote-rate-reneg=0, time=0h 0m 14s, disc(modem)=0 Normal hang-up

%ISDN-6-CONNECT: Interface Serial0/0/0:30 is now
connected to 221 N/A

%ISDN-6-DISCONNECT: Interface Serial0/0/0:30
disconnected from 221 , call lasted 70 seconds
```

- CSCth65072

  Symptoms: A memory leak is experienced in the big buffer pool while using the service reflection feature.

  Conditions: This symptom is unknown other than service reflection is configured.

  Workaround: There is no workaround.

- CSCth66251

  Symptoms: Not able to configure policy-map for the second time in a Cisco 860 router.

  Conditions: This symptom is observed while configuring policy-map for the second time. The Cisco 860 throws internal data base error.

  Workaround: There is no workaround.

- CSCth67608

  Symptoms: Some groups are missing in the MLD proxy cache on the proxy router.

  Conditions: This symptom happens when the “ipv6 mld host-proxy” is applied with existing multicast routes.

  Workaround: Clear the multicast routes using “clear ipv6 pim topology” after applying “ipv6 mld host-proxy”.

- CSCth67788

  Symptoms: SVTI stops forwarding traffic when a local policy is configured on a device.

  Conditions: This symptom is observed on a router that is running Cisco IOS Release 15.0(1)M1.

  Workarounds:

  1. Do not use a local policy.
  2. Configure “no ip route-cache cef” on the tunnel interface.

- CSCth68038

  Symptoms: After a simulated failover of an L2L tunnel, a Cisco 7200 router with VSA will fail to encrypt traffic for a period of time, typically for several minutes. VSA will then begin to encrypt traffic correctly. The problem appears to be triggered when manually failing over a spoke from one hub Cisco 7200 without VSA to a secondary hub Cisco 7200 with VSA.

  Conditions: This symptom is observed on a Cisco 7200 router with VSA.

  Workaround: Use software encryption.

- CSCth69361

  Symptoms: A Cisco 881 router crashes when verifying enerygwise endpoint using Orchestrator Agent.

  Conditions: This symptom is observed when configuring “energywise endpoint” on a Cisco 881 router and have PC that is running with Orchestrator Agent.

  Workaround: There is no workaround.

- CSCth70437

  Symptoms: Crypto sessions drop upon the following error message:

  ```
  000059:%SYS-2-BADSHARE: Bad refcount in datagram_done, ptr=83D91910, count=0,
  -Traceback= 0x80334D4Cz 0x823409A0z 0x8230D830z 0x8039460Cz 0x80397B40z

  000060:%SYS-2-BADSHARE: Bad refcount in datagram_done, ptr=83D91CE4, count=0,
  -Traceback= 0x80334D4Cz 0x823409A0z 0x8230D830z 0x8039460Cz 0x80397B40z

  000061:%SYS-2-BADSHARE: Bad refcount in datagram_done, ptr=83D920B8, count=0,
  -Traceback= 0x80334D4Cz 0x823409A0z 0x8230D830z 0x8039460Cz 0x80397B40z

  000062:%SYS-2-BADSHARE: Bad refcount in datagram_done, ptr=83D82F8C, count=0,
  -Traceback= 0x80334D4Cz 0x823409A0z 0x8230D830z 0x8039460Cz 0x80397B40z
  ```

  Conditions: This symptom is observed on a Cisco 800 series router. In both cases, crypto has been applied to dialer interface.

  Workaround: Issue seen previously in CSCta57268.

- CSCth71648

  Symptoms: G3 fax fails.

  Conditions: This symptom is observed when T38 version 3 is configured on gateway and Cisco fax server.

  Workaround: Configure gateway and fax server with T38 version 0.

- CSCth74497

  Symptoms: Time elapsed after delay OOP event until route change is more than 3 seconds.

  Conditions: This symptom is observed on a router that is loaded with Cisco IOS.

  Workaround: There is no workaround.

- CSCth75103

  Symptoms: H.323 gateway works call preserve a call when it receives DISCONNECT from ISDN.

  Conditions: This symptom is observed when H.323 gateway receives DISCONNECT from ISDN.

  Workaround: There is no workaround.

- CSCth75203

  Symptoms: Spurious memory access is found while interchanging two configurations.

Conditions: This symptom is observed on a router that is running Cisco IOS Release 15.1(2.6)T with the two configurations.

Workaround: There is no workaround.

- CSCth78183

  Symptoms: Traffic is not transmitted over IPSec tunnel due to duplicate ARP entries and incomplete CEF adjacency.

  Conditions: This symptom occurs when running Cisco IOS Release 12.4(15)T9.

  Workaround: Enter a **shutdown** followed by a **no shutdown** on the tunnel interface.

- CSCth80212

  Symptoms: The following topology is seen:

  PSTN | | |(E1) IP Phone---(Sccp)----CUCM(6.1.3)---(Sip trunk)----Gateway ---(Sip trunk)-----Genesys -----Sipclient

  Conditions:

  1. Calls come from the PSTN to the gateway to the genesys cluster, the sip client behind genesys answers it, the call is fine.
  2. Then the call from the PSTN is put on hold and one more call to the IP phone (behind CUCM) is made and that call is also fine.
  3. Then there is a transfer (consultative), of the PSTN call to the IP phone.
  4. The transferred call is fine for about 30 seconds and then the call drops.

  Workaround: There is no workaround.

- CSCth81095

  Symptoms: Output queue size is 1000/1000 in the output of “show interface Multilink X”. Also output drops are incrementing on the interface.

  Conditions: The complete trigger of the problem is not known yet, but it is related to changing “fair-queue” and “tx-queue-limit” on the member link serial interfaces while bidirectional traffic is flowing over the interfaces.

  Workarounds:

  1. Enter **shutdown** followed by **no shutdown** on the multilink interface, or flap it from the remote side router
  2. Reload the router.

- CSCth82164

  Symptoms: When OCSP is being used as the revocation check method for IKE, only the first connection attempt (after reboot or cache clearing of public RSA keys) undergoes an OCSP check. Subsequent revocation checks are bypassed because the peer public key appears to be cached indefinitely.

  No CRL or other lifetime parameters are involved. OCSP should be consulted for each IKE tunnel setup.

  The following messages indicate bypassing the revocation check:

  ```
  ISAKMP:(1002): peer's pubkey is cached
  CRYPTO_PKI: Found public key in hash table. Bypassing certificate validation
  ```

  Conditions: OCSP is configured as revocation check method for IKE.

  Workaround: There is no workaround.

- CSCth82293

  Symptoms: The Cisco 2900 ISR-G2 router crashes due to bus error at PC 0x0 with spurious errors and %ALIGN-1-FATAL: Corrupted program counter message.

  Conditions: This symptom is observed with CNS configurations.

  Workaround: There is no workaround.

- CSCth82323

  Symptoms: CFD feature fails when onboard crypto engine is enabled on Cisco 1841 platform.

  Conditions: This symptom occurs when UUT is running Cisco IOS Release 15.1(2.7.)T.

  Workaround: There is no workaround.

- CSCth82777

  Symptoms: Router crashes while sending AAA STOP records and cleaning up internal database

  Conditions: This symptom may occur when removing a PVC supporting PPP over ATM that is using radius for stop records.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.1(2)T

All the caveats listed in this section are resolved in Cisco IOS Release 15.1(2)T. This section describes only severity 1, severity 2, and select severity 3 caveats.

- 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.

- 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.

  Workaround: We can overcome the reload issue by disabling hardware crypto using the following command in global configuration mode: **no crypto engine accelerator**.

  Further Problem Description: When hardware crypto is turned off, encryption and decryption will be done by software and not by hardware. This can slightly hike CPU utilization, and this should not be an issue as long as we are not hit with pretty huge volume of traffic.

- 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-sip

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://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20100922-bundle

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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090826-cucm

http://www.cisco.com/en/US/products/products_security_advisory09186a0080b4a313.shtml

- CSCsz97091

  Symptoms: Packet drop occurs when **show version**, **show run,** and **write memory** commands are issued.

  Conditions: Packet drop will be observed as input errors accounted as overruns. The rate of packets being dropped will be proportional to the rate of traffic.

  Workaround: There is no workaround.

- 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-sip

  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://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20100922-bundle

  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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090826-cucm

http://www.cisco.com/en/US/products/products_security_advisory09186a0080b4a313.shtml

- CSCta58068

  Symptoms: During BGP convergence, a CPU spike may be seen on the local PE in an MVPN configuration.

  Conditions: The symptom may be observed with the following conditions:

  - Remote PE neighbor switchover.
  - On local PE, do a **clear ip bgp** *bgp nbr*
  - On bring up of local PE
  - Large configurations, such as one with 300 MDT default tunnels.

  The following is an example of an MVPN configuration where this problem can be seen:

  1. OSPF routing protocol is enabled on all the networks in the topology.
  2. Each PE router has 100 mVRFs defined (between vpn_0 to vpn_99).
  3. MDT default is configured on all the mVRFs on the PE routers.
  4. PE routers have an iBGP session, ONLY with the RR (route-reflector).
  5. eBGP session exists between the router and PE1, with router sending 200,010 VPNv4 routes.
  6. OSPF session also exists between router and PE1, with router sending 100 OSPF routes.
  7. In effect, the following states are present in the network:

  On PE and RR routers:

  1. IGP states = 100 OSPF routes.
  2. BGP states = 200,010 VPNv4 routes.

  On PE routers ONLY:

  1. VRF sessions = 100 VRFs (vpn0 to vpn_99).
  2. MDT sessions = 100 SSM sessions.

  Workaround: There is no workaround.

- CSCtb32043

  Symptoms: CPUHOG messages may be displayed or Cisco IOS might crash when executing no ipv6 multicast-routing in a configuration with more than 20,000 IPv6 multicast-enabled interfaces or sub-interfaces.

  Conditions: This symptom is observed only rarely when an alternate software path is taken. It is not known what causes this alternate path to be taken.

  Workaround: There is no workaround.

- CSCtb47647

  Symptoms: Active RP crashes at pim_send_join_prune.

  Conditions: The symptom is observed when performing some PIM-related testing with specific configurations and after carrying out an SSO. When you attempt to debug memory leak issue using a memory traceback recording command, the router crashes while executing the command **show memory traceback exclusive**.

  Workaround: There is no workaround.

- CSCtc42941

  Symptoms: Standby is not coming up.

  Conditions: When a distribute-list is configured, the ACL is created if it does not exist. Then remove the ACL, but the distribute-list configuration that ties to the ACL is not removed. Configure the IPv6 ACL configuration with the same ACL name. Save the configuration and reload it.

  Workarounds:

  1. When a access list is removed, remove corresponding distribute-list configuration as well.
  2. Do not use the same access list name for IPv4 and IPv6.

  Further Problem Description:

```
router bgp 100
distribute-list sample in
exit
no ip access-list standard sample
ipv6 access-list sample
permit any any
write mem
```

- CSCtc45177

  Symptoms: The “text_start” is not showing up in crashinfo.

  Conditions: The symptom is observed with crashinfo data.

  Workaround: There is no workaround.

- CSCtc71408

  Symptoms: Fax transmission fails when CUBE is in the middle.

  Conditions: The symptom is observed when either one of the dial-peers on OGW/TGW/CUBE is configured for fax protocol T38 version 0.

  Workaround: Configure version 3 on all dial-peers.

- 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-h323

  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

- CSCtd30544

  Symptoms: NetFlow is showing Null in the destination interface even though packets are not getting dropped or blocked.

  Conditions: This symptom is seen when connected to the LNS via VPDN and browsing HTTP. Intermittently Null output is seen as the destination interface as the packet being punted between different CEF switching paths due to **ip tcp adjust-mss** *value* configuration that is applied on the destination interface.

  Workaround: Remove **ip tcp adjust-mss** *value* from the destination interface.

- 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-h323

  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://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20100922-bundle

  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

- CSCte07401

  Symptoms: Normal mode GD fails with tracebacks when you execute the **show memory debug leak chunks** command.

  Conditions: This symptom is seen when you check for memory leaks after clearing an L2TP session.

  Workaround: Wait for all sessions to tear down and then check for leaks.

- CSCte18124

  Symptoms: Ping over back-to-back ATM interface fails, if ATM PVC is created with “atm vc-per-vp 1024".

  Conditions: The issue is seen only with HWIC-4SHDSL line cards and only when “atm vc-per-vp 1024” is configured.

  Workaround: Create ATM PVC without “atm vc-per-vp 1024".

- CSCte20187

  Symptoms: When bgp next-hop is configured under a VRF, the following error message is seen on the remote PE router:

  ```
  %BGP-3-INVALID_MPLS: Invalid MPLS label (1)
  ```

  The label advertised may be different but it is always a reserved label (0- 15). Additionally, the local PE will see “No Label” as the Outgoing Label” in the MPLS forwarding table.

Conditions: This symptom is observed when bgp next-hop is configured under an interface.

Workaround: There is no workaround.

- CSCte27828

  Symptoms: Call forward does not work.

  Conditions: Topology: call originally is H323 then to CUCM---(SIP)---CUBE-- (SIP)---SIP Provider.

  IP addresses:
  CUCM 10.10.10.3
  Cube SUD 10.10.10.2
  CUBE North 192.168.101.10
  SBC 192.168.100.5

  "Call forward no answer" scenario does not work, but not systematically: sometimes it works, sometimes not.

  When the "call forward no answer" fails, we see a malformed contact field on 183 forwarded from CUBE to SBC (the same from CUCM to CUBE is correct); SBC doesn't answer due to this.

  Workaround: There is no workaround.

- CSCte52369

  Symptom: On a Cisco ASR1000 router, the RADIUS will send a NACK for the First COA request message, and Radius Authentication will fail.

  Conditions: This symptom is observed when the RADIUS receives "ACCESS-ACCEPT" with 'Unsupported Vendor' attribute.

  Workaround: Send the COA request message again.

- CSCte53097

  Symptoms: When the IP address of the HA is set to the VIP address of HSRP, end-to-end connectivity will be lost. Tunnel keepalives from the mobile node fail and the bindings are deleted from HA.

  Conditions: This is seen in Cisco IOS Release 12.4(23) when using the HA behind a NAT device and the translated (inside) IP of the HA is set to the HSRP VIP address.

  Workaround: Configure a loopback interface (does not have to be routed) with the same outside (public) IP that the mobile node connects to. This is the outside IP defined in the NAT rule on the NAT device.

- 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.

- CSCte76092

  Symptoms: Cisco 880 series router does not write crashinfo.

  Conditions: The symptom is observed with a Cisco 880 series router.

  Workaround: Connect a device to monitor the console.

- CSCte82917

  Symptoms: On a Cisco 7600 series RSP720, the **show proc cpu sort** command displays a CPU utilization of 0, but the per-process CPU utilization is 100% for some processes; no packet loss occurs, however.

  Conditions: This symptom is observed under the following conditions:

  - The router has recently loaded
  - HSRP is enabled in an HA environment
  - A large number of HSRP sessions are established.

  Workaround: Reduce the number of HSRP sessions to only a few. The router does not see any performance or functional impact. This is an issue only with internal CPU accounting.

- CSCte92581

  Symptoms: A VRF becomes stuck during deletion. This is a rarely-occurring timing condition.

  Conditions: This symptom is observed when the **no ip vrf** command is entered.

  Workaround: There is no workaround.

  Further Problem Description: The stuck VRF cannot be reused.

- CSCte95301

  Symptoms: Memory leak in proxy authentication scenario, when authentication fails.

  Conditions: The symptom is observed when HTTP proxy authentication is used.

  Workaround: There is no workaround.

- CSCte98082

  Symptoms: PPPoE session is not coming up on some clients due to a malformed PADO. PPPoE relay sessions are failing to come up on an LAC.

  Conditions: The symptom is observed with a few clients which are unable to process malformed PADO and also when “pppoe relay service” is configured on the LAC.

  Workaround: There is no workaround.

- CSCtf01344

  Symptoms: IOSD core@chunk_diagnose while doing an ISSU on a Cisco ASR 1004 router.

  Conditions: The symptom is observed on a Cisco ASR 1004 when attempting an ISSU upgrade with VRF-aware IPSec features and an uninitialized Webex SPA in the system.

  Workaround: Properly initialize Webex SPA before ISSU.

- 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-nat

  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://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20100922-bundle

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

- CSCtf35006

  Symptoms: If there are two jobs in an SNMP job queue and if you try to destroy the jobs, the console hangs.

  Conditions: The symptom is observed if you prepare multiple license action entries and then let them execute immediately.

  Workaround: There is no workaround.

- CSCtf48094

  Symptoms: UUT crashes for FTP traffic with debugs enabled for IPv6 inspection.

  Conditions: The symptom is observed only with Legacy Firewall for IPv6 inspection.

  Workaround: There is no workaround.

- 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-sip

  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://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20100922-bundle

  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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090826-cucm

  http://www.cisco.com/en/US/products/products_security_advisory09186a0080b4a313.shtml

- 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-nat

  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://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20100922-bundle

  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

- CSCtf98087

  Symptoms: A Cisco router reloads at sipSPIUpdSrtpSession.

  Conditions: This symptom is observed after completion of the basic call with a hold/resume scenario with IPv6 mode.

  Workaround: There is no workaround.

- CSCtg14446

  Symptoms: Packets are dropped in excess of the configured rate for hierarchical policies, with shaper in the parent policy.

  Conditions: The symptom is observed only with HQoS policies (flat policies are not affected).

  Workaround: There is no workaround.

- 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-sslvpn.

  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://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20100922-bundle

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

- CSCtg30795

  Symptoms: Calls are not torn down since SIP INFO with Qsig disconnect tunneled are not honored by the SIP gateway.

  Conditions: This symptom is observed when disconnect is built and sent by Call manager over a Qsig-enabled SIP trunk to the SIP gateway (GW).

  CUCM1----SIP-QSIG-----SIP GW--------T1 QSIG----------MGCPGW--------CUCM2

  In the above setup, when CUCM1 initiates disconnect, it sends out INFO tunneled with Qsig disconnect to the SIP GW in order to achieve 3-way disconnect.

  Workaround: There is no workaround.

  Further Problem Description: The gateway should send a Qsig Disconnect over the T1 link; since that is not happening, the call is not torn down.

- CSCtg31434

  Symptoms: A Cisco router crashes due to an unexpected exception to the CPU.

  Conditions: This symptom occurs when the **privilege interface level 10 ppp authentication** command is entered. This symptom is observed in Cisco IOS Release 12.2(31)SB through Release 12.2(31)SB18, and in Cisco IOS Releases 12.2(33)SB and 12.2(34)SB.

  Workaround: There is no workaround.

- CSCtg35230

  Symptom: VPDN sessions are created when SCCRQ and SCCRP have different IP addresses.

  Conditions: This symptom occurs after the IP address is downloaded from the AAA server and changed on LNS2.

  Workaround: There is no workaround.

- 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.

- CSCtg51476

  Symptoms: Cisco ISR G2 routers reload on their own with a bus error.

  Conditions: This symptom is observed when BFD is configured.

  Workaround: Remove BFD.

- CSCtg56013

  Symptoms: Router crashes when initiating ping through the modem after router bootup.

  Conditions: The symptom is observed when the modem fails to enumerate at bootup.

  Workaround: There is no workaround.

- CSCtg59956

  Symptoms: Active supervisor crashes when doing an SSO switchover.

Conditions: The symptom is observed when performing a switchover operation with a lot of L2VPN NLRIs. BGP L2VPN configuration is required.

Workaround: There is no workaround.

- CSCtg67425

  Symptoms: A Cisco router crashes at fr_vcb_dlci_status_change.

  Conditions: This symptom is observed after removing frame-relay encapsulation in a router that has T3 interfaces.

  Workaround: Remove all the pvcs configured under an interface before changing/removing frame-relay encapsulation.

- CSCtg69202

  Symptoms: CUBE modifies the RTP port number before passing it to the remote end, which causes one-way audio.

  Conditions: This symptom is observed only when the RTP port number is higher than the RTCP port number in the incoming request from the endpoint. Instead of sending the same RTP port number, CUBE decrements the RTP port number by one less than the RTCP port number when it forwards the OLC Ack to the destination side. This causes the destination to send the audio packets to the wrong port on the originating side, causing one-way audio.

  Workaround: There is no workaround.

  Further Problem Description: Under some specific conditions, when CUBE receives the OLC acknowledgement with the media control information from an H323 client, instead of passing the same RTP port number to the remote end, it modifies the RTP port number, causing the one-way audio.

- CSCtg76688

  Symptoms: An active Cisco route processor reloads in a scale scenario (16k - 24k sessions) when the **clear subscriber session all** command is entered.

  Conditions: This symptom is observed only when there are 16k-24k sessions and the **clear subscriber session all** command is entered.

  Workaround: Do not enter the **clear subscriber session all** command when more than 16k sessions are up on the router.

- CSCtg79105

  Symptoms: A UC560 unexpectedly reboots.

  Conditions: The symptom is observed when the **show memory 0** command is executed.

  Workaround: There is no workaround.

- CSCtg83932

  Symptoms: “Encapsulation aal5auto” may not be enabled under svc mode.

  Conditions: This symptom is observed on a Cisco 7200 router running Cisco IOS Release 15.1(01.14)T.

  Workaround: There is no workaround.

- CSCtg86714

  Symptoms: The **show cellular 0** command might not show any output.

  Conditions: The symptom is observed with the **show cellular 0** command.

Workaround: Shut down the cellular 0 interface, write the configuration to memory and reboot, so that the configured interface is shutdown on boot. You then have your original start up configuration, with the cellular 0 shut down, and you still get **show cellular stats**. If you then unshut the cellular after the "MODEM UP" line, you get "LINK UP" and still retain the **show cellular stats**.

- CSCtg87775

  Symptoms: The router may unexpectedly reload.

  Conditions: The symptom is observed under circumstances where a Cisco 7600 series router is configured to handle several hundred or more neighbors, and an administrator issues the command: **clear bgp vpnv4 unicast ***.

  Workaround: Clear individual neighbors separately, limiting yourself to 100 or fewer in any scanner interval.

  Further Problem Description: Issuing other clear commands and forcing a switchover between active and standby at during the interval immediately before and after issuing the **BGP clear** command increases the probability of a reload.

  The number of neighbors where this is documented as happening is 1200, but the exact minimum number of neighbors needed to trigger the problem is not documented.

- 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.

- CSCtg91201

  Symptoms: DHCP-added static routes get removed sometimes and the traffic towards the host gets dropped.

  Conditions: The symptom is observed with IP unnumbered relay and with a third party external DHCP server. (This issue can also occur with an IOS DHCP server, but the probability is quite low.)

  Workaround: There is no workaround.

- CSCtg91336

  Symptoms: A Cisco router may crash during show command **show ip ospf rib**.

  Conditions: This symptom is observed on Cisco IOS releases with enhancement CSCsu29410 when the following sequence of events occurs:

  - A user enters the **show ip ospf rib** command and stops in the middle
  - OSPF local rib is significantly changed; for example, routes are removed
  - A user presses Enter or spacebar to resume output of the **show ip ospf rib** command.

  Workaround: Do not enter the **show ip ospf rib** command. If it is necessary use the command, enter terminal length 0 and print the entire output.

- CSCtg95618

  Symptoms: 1. MSCD_StartStop fail message is observed in usbflash_mscd_scsi_listener 2. USB flash file system is not accessible sometimes.

  Conditions: This symptom is observed on Cisco 892F and C892FW series routers with two USB slots when the USB sticks are removed and swapped. This symptom is not observed when a single USB stick is removed or inserted in a different bus.

  Workaround: There is no workaround.

- CSCtg96518

  Symptoms: Fast memory leak occurs in CCSIP CCB Pool.

  Conditions: This symptom is observed on a Cisco 2951 integrated services router with Cisco IOS Release 15.1(1)T.

  Workaround: Reload the router.

- CSCtg96630

  Symptoms: A Cisco router crashes when the user tries to configure a default policy with rsvp group percentage configuration.

  Conditions: This symptom is observed when the user tries to configure a default policy with rsvp group percentage configuration under a virtual template.

  Workaround: There is no workaround except to avoid this configuration command.

- CSCtg98783

  Symptoms: Cube: call leg 1 receives SDP 101, 0-15; Cube: call leg 2 sends SDP 101, 0-16. This is seen as a different media, and is treated as such.

  Conditions: This symptom is observed when Cube is configured in DO-EO with flow-around.

  Workaround: There is no workaround.

- CSCtg99114

  Symptoms: The following error message with traceback is observed:

  ```
  %IPC-5-REGPORTFAIL: Registering Control Port
  ```

  Conditions: The symptom is observed with ISR routers and with Cisco IOS Release 12.4(24)T or later.

  Workaround: Drop IPC traffic using control-plane policing:

  ```
  class-map match-all ipc match access-group name ipc policy-map drop-ipc class ipc drop
  ip access-list extended ipc permit udp any any eq 1975 control-plane service-policy
  input drop-ipc
  ```

- 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.

- CSCth02725

  Symptoms: There is an interoperability issue between a third-party vendor's routers and Cisco routers with severe IPTV service failure in Prune-Overriding environment.

  Conditions: The symptom is observed in the following scenario:

  1. Router A is Cisco 7609 router (IP address 10.1.1.1) and connects to Router B (third-party vendor's router; IP address 10.1.1.3) and Router C (IP address 10.1.1.2).
  2. If subscriber under Router C disappears, Router A receives “Prune” message from Router C.
  3. Router A does not change “source IP of PruneEcho message (10.1.1.2)” and sends it to Router B.
  4. At this time, Router B should send overriding-join to Router A because Router B still has subscribers. But Router B drops the PruneEcho message because source IP (10.1.1.2) is not from PIM neighbor. Router B cannot send overriding-join to Router A.

5. As a result, multicast traffic (IPTV stream) to Router B stops.

Workaround: Connect C and B to become PIM neighbors avoids the interoperability issue, but cannot always be considered a recommended workaround because of potential high cost and/or other (sometimes third-party) limitations.

- CSCth02789

  Symptoms: System can crash when attempting to schedule an IPv6 icmp-echo operation.

  Conditions: The symptom is observed with IPv6 and icmp-echo.

  Workaround: There is no workaround.

- CSCth04193

  Symptoms: A Cisco router crashes at cce_dp_named_db_http_free_token_info.

  Conditions: This symptom is observed when Zone-based Policy Firewall is configured to inspect HTTP traffic.

  Workaround: Do not use deep packet inspection.

- CSCth04945

  Symptoms: A Cisco router crashes when adding or removing a QoS policy from an interface.

  Conditions: This symptom is observed when the following occur:

  – packets keep hitting the interface from which the policy is being removed
  – the QoS policy is at least a two-level policy -before the policy was removed, the CLI generated an error for some invalid configuration change in that policy; for example,

```
3845-AA2205(config)
#policy-map VOICE-OUT-PARENT 3845-AA2205(config-pmap)
#class class-default 3845-AA2205(config-pmap-c)
#no shape average 100000000
```

  Queueing must be removed from child classes before queueing can be removed from class-default.

  Workaround: Avoid invalid configuration changes in the QoS policy before adding it to or removing it from an interface.

- CSCth07787

  Symptoms: A standby device crashes when attempting to configure login banner on the active device.

  Conditions: The symptom is observed only when configuring the banner manually, but not during bulk sync or any copy operations. In addition, this symptom is observed when using the following delimiters: -Cntrl-v + Cntrl-C; -Shift-6 + Shift-C

  Workaround: Use any delimiters other than the following: -Cntrl-v + Cntrl-C; -Shift-6 + Shift-C.

- CSCth08505

  Symptoms: PPPoE sessions may not sync to the standby-RP.

  Conditions: This symptom is observed after the first attempt at establishing a PPPoE session fails.

  Workaround: Reloading the standby-RP may resolve this issue.

- CSCth15353

  Symptoms: Incorrect result codes are displayed in vpdn sys logging. The CDN message for admin down was reported in the syslog as “Result Code=2, Error Code=6” instead of “Result Code=3, Error Code=6”.

Conditions: This symptom is observed when a session is cleared by a clear command (for example, **clear interface virtual-access 3.1**).

Workaround: There is no workaround.

- CSCth15518

  Symptoms: Ping through ISDN BRI interface fails.

  Conditions: The symptom is observed when attempting a ping after giving a **shut** and **no shut** on the BRI interface.

  Workaround: There is no workaround.

- CSCth16382

  Symptoms: A Cisco device crashes at cce_dp_results_get_class_group_element.

  Conditions: This symptom is observed when Crypto is on and QoS pre-classify is not enabled. The crash occurs when configurations are loaded and traffic is run.

  Workaround: There is no workaround.

- CSCth18146

  Symptoms: A Cisco SIP gateway may reload unexpectedly due to a release message with no IEs.

  Conditions: This symptom is observed on a SIP gateway with tunneling enabled.

  Workaround: There is no workaround.

- CSCth18611

  Symptoms: A Cisco router crashes.

  Conditions: This symptom is observed when configuring dynamic nat under the vrf interface with an existing firewall configuration. This symptom is not observed without the vrf configuration.

  Workaround: There is no workaround.

- CSCth18982

  Symptoms: BGP sessions flap continuously in a multi-session configuration.

  Conditions: This symptom is observed when the same peer under the same address family is configured under different topologies (MTR with GR-enabled setup) with multiple topo-ids.

  Workaround: The sessions do not flap if topologies use the same topo-id for the peers active under different topologies or when GR is not enabled.

- CSCth20704

  Symptoms: A Cisco router crashes when policy-map is unconfigured while traffic is flowing.

  Conditions: This symptom is observed on a Cisco 7200 router running Cisco IOS Release 15.1(1)T1.

  Workaround: There is no workaround.

- CSCth21017

  Symptoms: Traceback is seen when ISIS adjacency state changes.

  Conditions: This symptom is observed on a Cisco 7200 router running Cisco IOS 15.1(1)T1.

  Workaround: There is no workaround.

- CSCth23787

  Symptom: A Cisco router crashes at mcast_aaa_send_stop_acct_event.

Conditions: This symptom is observed while unconfiguring “ipv6 mld join-group FF1E:7777:7777:1” in the client after configuring within 15-20 seconds.

Workaround: Unconfigure, if required, after multicast start record is sent.

- CSCth23814

  Symptoms: When using Flexible NetFlow, a traceback or crash can occur.

  Conditions: This symptom is observed when a monitor is configured with a flow record that has the “BGP next hop” field configured.

  Workaround: Ensure that the “BGP next hop” field is not configured for a flow.

- CSCth25698

  Symptoms: IPv6 packets are not dropped by the firewall.

  Conditions: IPv6 packets are not dropped by the firewall in case of Zone to non-zone.

  Workaround: There is no workaround.

- CSCth28677

  Symptoms: CUD fails to be parsed when it contains 0x00.

  Conditions: This symptom is observed on a Cisco router configured for X25 translation with CUD verification.

  Workaround: There is no workaround.

- CSCth29105

  Symptoms: On Cisco ISR G2 products—only on the Cisco 2901, 2911, and 2921—occasionally the SYSTEM LED will be OFF even when the router is operating normally.

  Conditions: There are no specific conditions that trigger this issue. The problem happens randomly.

  Workaround: There is no workaround. This issue does not affect any of the router functionality.

- CSCth30815

  Symptoms: StopCCN result codes and strings do not match RFC.

  Conditions: This symptom is observed when the session is cleared by command or due to some error condition; the result code is not correct.

  Workaround: There is no workaround.

- CSCth33457

  Symptoms: A Cisco IOS router configured with IPSec (IP Security) may reload when receiving encrypted packets.

  Conditions: This symptom is observed when one or more of the following is configured on an interface configured with IPSec:

  - ip accounting precedence input
  - ip accounting mac-address input
  - WCCP
  - Flexible NetFlow
  - BGP accounting
  - uRPF
  - mpls accounting experimental input

  Workaround: Avoid using IPSec or avoid using all of the above features on the interface.

- CSCth35377

  Symptoms: Master router does not reacquire DLSW Circuits after failing over to slave router and back again.

  Conditions: This symptom is observed on a Gigabit Ethernet interface on a Cisco 2921 master router running DLSW ethernet redundancy and with the following parameters:

  ```
  encapsulation dot1Q xxx ip pim sparse-mode.
  ```

  Workaround: Remove “ip pim sparse-mode.”

- CSCth35620

  Symptoms: Self zone inspection fails for TCP/UDP and ICMP traffic.

  Conditions: The symptom is observed when the interface is part of self zone and router-terminated traffic hits that interface.

  Workaround: There is no workaround.

- CSCth35780

  Symptoms: A Cisco router crashes for the SIP multi-part traffic.

  Conditions: This symptom is observed when SIP multi-part traffic passes through a Cisco 7200 router. NAT SIP Multi-part must be enabled as part of the NAT configuration.

  Workaround: There is no workaround.

- CSCth38711

  Symptoms: The first WAAS connection takes longer than one minute to begin transferring data.

  Conditions: This symptom is observed during AOIM sync, which occurs once per boot or reconfiguration.

  Workaround: There is no workaround.

- CSCth39774

  Symptoms: UUT hangs when an eTCDF file is loaded on the router in the latest t_base_1 code base.

  Conditions: The symptom is observed when an eTCDF file is loaded on the router, the UUT seems to hang. However, the UUT is actually waiting for user input, and if you enter “#” on the CLI, it will print some error messages about invalid commands and return to CLI.

  Workaround: Do not use the eTCDF file to configure the encrypted filter, rather directly enter the commands on the CLI of the router.

- CSCth39877

  Symptoms: No VPDN logging occurs for the L2TP tunnel.

  Conditions: This symptom is observed when the tunnel goes down.

  Workaround: There is no workaround.

- CSCth40090

  Symptoms: A Cisco device crashes when initiating an analog CAMA call.

  Conditions: On initiation of an analog CAMA call, a crash occurs due to memory corruption leading to a breakpoint exception. A crash occurs in scenarios where e911 is enabled or disabled.

  Workaround: There is no workaround.

- CSCth40213

  Symptom: More than one preshared key for address 0.0.0.0 may not be configurable in different keyrings.

Conditions: Multiple preshared keys cannot be configured for address 0.0.0.0 in different keyrings.

Workaround: There is no workaround.

- CSCth40506

  Symptom: A Cisco voice gateway does not have its Gigabit Ethernet link connected to the network, but the call is not cleared from the PRI when the Application Ack Timer expires.

  Conditions: This symptom is observed on a Cisco 2911 voice gateway with Cisco IOS Release 15.0(1)M and a Cisco 2951 voice gateway with Cisco IOS Release 15.0(1)M1.

  Workaround: There is no workaround.

  Further Problem Description: When a voice call is placed, a SIP INVITE is sent:

  ```
  -- Sent: INVITE sip:x@x.x.x.x:5060 SIP/2.0 --
  ```

  Because the Cisco gateway does not have network connectivity, no SIP reply is received from the network. Sixty seconds later, the Application Ack Timer expires:

  ```
  -- .May 4 17:49:29.120 GMT=+1: ISDN Se1/0:15 **ERROR**: CCPCC_TApplnAckExpiry:
  Application Ack Timer expired. b channel 1 cref 0x8021 call_id 0x0045
  ```

  The call, however, is not cleared from the PRI.

- CSCth45623

  Symptoms: A memory leak occurs in cce dp reclass.

  Conditions: This symptom is observed with WAAS Express plus QoS preclassify disabled plus Crypto plus crypto-map.

  Workaround: There is no workaround.

- CSCth50550

  Symptoms: A Cisco device crashes when using PDP filter.

  Conditions: This symptom is observed when PDP filter is applied in a QoS Policy.

  Workaround: There is no workaround.

- CSCth51125

  Symptoms: PCEX-3G-HSPA-R6 is not recognized at bootup:

  ```
  %CISCO800-2-MODEM_NOT_RECOGNIZED: Cellular0 modem not RECOGNIZED. Carrier id not
  available or invalid! Replace it with Cisco supported modem and reload the router.
  %CELL_MSG-1-MODEM_ACK_FAIL: [Cellular0] Modem Ack not received.
  %CELL_MSG-1-MODEM_ACK_FAIL: [Cellular0] Modem Ack not received.
  %CELL_MSG-1-MODEM_ACK_FAIL: [Cellular0] Modem Ack not received.
  ```

  Conditions: The symptom is observed on a Cisco 881G-K9 that is running Cisco IOS Release 15.1(1)T.

  Workaround: There is no workaround.

- CSCth57478

  Symptoms: When configuring SIP digest authentication, user names with more than 25 characters are truncated in the running config and cause the password component to be corrupted. This error is saved through to startup configuration, causing the authentication to be lost on reboot.

  Conditions: This symptom is observed with a normal dial-peer configuration on a POTS dial-peer running Cisco IOS Release 15.1(1)T.

  Workaround: There is no workaround.

- CSCth59217

  Symptoms: Firewall sessions are not seen when ZBFW and gatekeeper are configured on the UUT.

  Conditions: The symptom is observed when ZBFW and gatekeeper are configured on the UUT.

  Workaround: There is no workaround.

- CSCth62854

  Symptoms: A Cisco router crashes with traceback ospfv3_intfc_ipsec_cmd.

  Conditions: This symptom is observed when the interface is configured with ospfv3, null authentication/encryption, and non-null encryption/authentication.

  Workaround: Remove the ospfv3 area command, then remove the null authentication/encryption.

- CSCth63379

  Symptoms: With two T1 links running ATM with IMA bundling, the proper CEF- attached adjacency for the opposite end of the link does not appear.

  Conditions: This symptom is observed on a Cisco 3800 series device with VWIC- 2MFT-T1.

  Workaround: There is no workaround.

- CSCth69243

  Symptoms: Error messages and tracebacks involving the TCP timer process appear on the console.

  Conditions: This symptom is observed with a large volume of traffic over extended periods of time; the exact trigger is unknown.

  Workaround: There is no workaround.

- CSCth79434

  Symptoms: Policies with mixed filters might not work properly.

  Conditions: If a policy has a filter of type dscp/prec/acl in its first class- map, the rest of the policy might not classify properly.

  Workaround: If the policy has non-dscp/prec/acl filters in it, moving that class-map to the top of the policy will alleviate this problem.