Caveat List for Cisco IOS Release 12.2(33)SCB

This chapter describes open and resolved severity 1 and 2 caveats and select severity 3 caveats:

- The "Open Caveats" sections list open caveats that apply to the current release and may apply to previous releases. A caveat that is open for a prior release and is still unresolved applies to all future releases until it is resolved.
- The "Resolved Caveats" sections list caveats resolved in a specific release, but open in previous releases.

The bug IDs are sorted alphanumerically.

Note The Caveats section includes the bug ID and a short description of the bug. For details on the symptoms, conditions, and workaround for a specific caveat you must use the Bug Search Tool.

Cisco Bug Search

Cisco Bug Search Tool (BST), the online successor to Bug Toolkit, is designed to improve effectiveness in network risk management and device troubleshooting. You can search for bugs based on product, release, and keyword, and aggregates key data such as bug details, product, and version. For more details on the tool, see the help page located at http://www.cisco.com/web/applicat/cbsshelp/help.html

Open Caveats—Cisco IOS Release 12.2(33)SCB11

Bug ID	Description
CSCsw37209	The **cable ipv6 src-verify** command is not effective when configured on Cisco uBR7200 platform.
CSCsy56666	The **cable primary-sflow-qos11 keep snmp-only** command is not working properly and the primary service flow packet/byte count is not retained after the cable modem reset.
CSCsz36328	Cable modems remain in online (pk) and expired states after cable privacy mandatory command is executed.
CSCsz63011	Cable metering traps are not getting generated for streaming mode.

Bug ID	Description
CSCsz67716	The 'Gate Report State' counter of the **show packetcable cms verbose** command output is not getting incremented for PacketCable MultiMedia (PCMM) policy servers.
CSCtb79237	No syslog or SNMP trap is generated when Common Open Policy Service (COPS) process is used causing PacketCable to fail.
CSCtc65910	A header buffer memory leak may be observed on Cisco CMTS.
CSCte91760	Simulating an intermediate session routing (ISR) watchdog using a busy-loop delay in an ISR, results in an incorrect traceback. Further, an infinite loop in the ISR results in no ISR watchdog functionality at all.
CSCth24131	The show context summary command always reports null crashes when there are crashes on the cable line card.
CSCti19280	The FFT engine is not updated with the CNR threshold values if a change is made either in the CLI or the SNMP interface to the CNR threshold profile for a given upstream.

Resolved Caveats—Cisco IOS Release 12.2(33)SCB11

Bug ID	Description
CSCtd25669	When a secondary rf-channel shutdown/no shutdown is performed on a Cisco uBR-MC8X8 cable interface line card, the wideband CM reports primary-channel QAM failure/recovery.
CSCti71911	When a Cisco IOS release 12.2(33)SCB10 downgrade is performed on the active RP, the standby RP resets the peak-rate TLV.
CSCti81896	When the ingress cancellation feature is enabled, all modems on an upstream may momentarily go offline and then recover within minutes.

Open Caveats—Cisco IOS Release 12.2(33)SCB10

Bug ID	Description
CSCsw37209	The **cable ipv6 src-verify** command is not effective when configured on Cisco uBR7200 platform.
CSCsy56666	The **cable primary-sflow-qos11 keep snmp-only** command is not working properly and the primary service flow packet/byte count is not retained after the cable modem reset.
CSCsz36328	Cable modems remain in online (pk) and expired states after cable privacy mandatory command is executed.
CSCsz63011	Cable metering traps are not getting generated for streaming mode.
CSCsz67716	The 'Gate Report State' counter of the **show packetcable cms verbose** command output is not getting incremented for PacketCable MultiMedia (PCMM) policy servers.

Bug ID	Description
CSCtb79237	No syslog or SNMP trap is generated when Common Open Policy Service (COPS) process is used causing PacketCable to fail.
CSCtc65910	A header buffer memory leak may be observed on Cisco CMTS.
CSCte91760	Simulating an intermediate session routing (ISR) watchdog using a busy-loop delay in an ISR, results in an incorrect traceback. Further, an infinite loop in the ISR results in no ISR watchdog functionality at all.
CSCth24131	The show context summary command always reports null crashes when there are crashes on the cable line card.
CSCti19280	The FFT engine is not updated with the CNR threshold values if a change is made either in the CLI or the SNMP interface to the CNR threshold profile for a given upstream.

Resolved Caveats—Cisco IOS Release 12.2(33)SCB10

Bug ID	Description
CSCsg82766	CMTS may crash due to a bus error during user authentication.
CSCsr40529	Corrupted output is displayed when the standby disk is formatted during an In-Service Software Upgrade (ISSU) of the CMTS router running Cisco IOS Release 12.2(33)SCB4.
CSCsr96042	Router crashes when the VPN Routing and Forwarding (VRF) configuration is changed.
CSCsv06975	Dynamic Message Integrity Check (DMIC) fails TFTP for IPv6 over CMTS bundle subinterface
CSCsv73754	A router crash is observed during VPN Routing and Forwarding (VRF) configuration.
CSCsw73403	CMTS does not warn the user while configuring a bundle subinterface if the primary bundle has any IPv6 enabled.
CSCsx58335	When relaying to multiple servers from an unnumbered interface, the DHCP relay sends packets to all servers, even for packets where the client is in a RENEWING state unicasting to attempt to reach a single server.
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.
CSCtc95495	The **show cable modem service-flow verbose** command incorrectly displays the MAC Rewrite Indices (MRI) that exceed 64 K. Subsequent information displayed by this command is also incorrect because it is dependent on the MRI.
CSCtd20903	The **cable clock dti** command does not work occasionally when one of the two DTCC cards in the CMTS system is unplugged during run time.
CSCtd83463	DOCSIS 3.0 cable modem goes offline after executing **test cable dcc** command.

Bug ID	Description
CSCtd86472	The Cisco IOS Software Network Address Translation functionality contains three denial of service (DoS) vulnerabilities. The first vulnerability is in the translation of Session Initiation Protocol (SIP) packets, the second vulnerability in the translation of H.323 packets and the third vulnerability is in the translation of H.225.0 call signaling for H.323 packets.
CSCte17479	All cable modems under a single upstream unexpectedly move to expire (pt) state on the Cisco CMTS router.
CSCte83897	The output of the MIB object docsDiag is not complete when the number of CMs in error state is greater than 30.
CSCte94013	When the diagnostic log feature is active and cable modems are flapping, some of the cable modem records are not obtained by an SNMP query command such as **snmpwalk docsDiagMib**.
CSCte97922	The hardware version, software version and serial number are not displayed for UBR10-FAN-ASSY, UBR10-PWR-DC and UBR10-PWR-AC modules.
CSCte99323	The secondary RP is reset due to parser return error after the secondary collector associate on the IPDR config is added or deleted.
CSCtf05943	Cable modem subscribers experience one-way RTP traffic.
CSCtf78545	IPv6 does not work on multiple CMTS bundle subinterface.
CSCtg07854	Packets are assigned to wrong queues when the policy-map configuration is modified.
CSCtg21410	The RP crashes when polling SNMP MIB object ciscoFlashMIB.
CSCtg40581	Missing entries when polling the SNMP MIB object ifStackStatus.
CSCtg92199	The Support for IfMIB is added for CMTS bundle IPv6 subinterface.

Open Caveats—Cisco IOS Release 12.2(33)SCB9

Bug ID	Description
CSCsy56666	The **cable primary-sflow-qos11 keep snmp-only** command is not working properly and the primary service flow packet/byte count is not retained after the cable modem reset.
CSCsz63011	Cable metering traps are not getting generated for streaming mode.
CSCsz67716	The 'Gate Report State' counter of the **show packetcable cms verbose** command output is not getting incremented for PacketCable MultiMedia (PCMM) policy servers.
CSCtd83463	DOCSIS 3.0 cable modem goes offline after executing **test cable dcc** command.

Resolved Caveats—Cisco IOS Release 12.2(33)SCB9

Bug ID	Description
CSCtd86472	The Cisco IOS Software Network Address Translation functionality contains three denial of service (DoS) vulnerabilities. The first vulnerability is in the translation of Session Initiation Protocol (SIP) packets, the second vulnerability in the translation of H.323 packets and the third vulnerability is in the translation of H.225.0 call signaling for H.323 packets.

Open Caveats—Cisco IOS Release 12.2(33)SCB8

Bug ID	Description
CSCsy56666	The **cable primary-sflow-qos11 keep snmp-only** command is not working properly and the primary service flow packet/byte count is not retained after the cable modem reset.
CSCsz63011	Cable metering traps are not getting generated for streaming mode.
CSCsz67716	The 'Gate Report State' counter of the **show packetcable cms verbose** command output is not getting incremented for PacketCable MultiMedia (PCMM) policy servers.
CSCtd83463	DOCSIS 3.0 cable modem goes offline after executing **test cable dcc** command.

Resolved Caveats — Cisco IOS Release 12.2(33)SCB8

Bug ID	Description
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.
CSCte14603	A vulnerability in the Internet Group Management Protocol (IGMP) version 3 implementation of Cisco IOS Software and Cisco IOS XE Software allows a remote unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition. Cisco has released free software updates that address this vulnerability.

Open Caveats—Cisco IOS Release 12.2(33)SCB7

- CSCsy56666

  Symptoms: The **cable primary-sflow-qos11 keep snmp-only** command is not working as expected and the primary service flow packet/byte count is not retained after the cable modem is reset.

  Conditions: This issue is seen in DOCSIS 1.1 specific modems after reset.

Workaround: Clear the cable modem counters associated with primary service flows.

- CSCsz63011

  Symptoms: The cable metering traps are not generated as expected for streaming mode.

  Conditions: There are no specific conditions for this issue to occur.

  Workaround: There is no workaround.

- CSCsz67716

  Symptoms: The “Gate Report State” counter in the output of the **show packetcable cms verbose** command does not increment for PacketCable Multimedia (PCMM) policy servers.

  Conditions: This issue is seen for PCMM policy servers.

  Workaround: There is no workaround.

- CSCtd83463

  Symptoms: The DOCIS 3.0 cable modem goes offline after a test cable dynamic channel change (DCC) with ranging technique 1.

  Conditions: There are no specific conditions for this issue to occur.

  Workaround: There is no workaround.

- CSCtf25400

  Symptoms: The Cisco CMTS crashes as freelist corruption.

  Conditions: Conditions are unknown.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(33)SCB7

- CSCsm88000

  Symptoms: export-map route-map changes are not automatically updated in the Border Gateway Protocol (BGP) VPNv4 table.

  Conditions: This issue is seen on the universal broadband router running the Cisco IOS Release 12.2(33)SRB under the following conditions:

  When adding or removing the new route-target values under the route-map configuration, which is being called by the export-map statement under VPN Routing and Forwarding (VRF) configuration.

  Workaround: Perform a manual clear of the VRF routing table for the prefixes to be updated.

- CSCsx33622

  Symptoms: Flapping BGP sessions occur in the network when a Cisco IOS application sends full-length segments with TCP options.

  Conditions: This issue is seen when a Cisco IOS device that is configured to send TCP options sends its initial Maximum Segment Size (MSS) during the three-way handshake. In this case, the router incorrectly accounts for 20 bytes of TCP options when it sends this initial MSS.

  This issue occurs when a "fixed" IOS communicates with a "non-fixed" IOS.

Note The "non-fixed" behavior is to subtract the 20 TCP option bytes when MSS values are initially exchanged.
The "fixed" behavior is to not subtract the 20 TCP option bytes when MSS values are initially exchanged.

Workaround: Set the MSS value on the "non-fixed" router to be the MSS received from the "fixed" router minus the TCP options (20 bytes). Use the global command **ip tcp mss** to adjust the MSS value that the router will use.

- CSCsy31588

  Symptoms: The **show interface x/x/x service flow yy phs** command does not record payload header suppression (PHS) packets for upstream.

  Conditions: This issue is seen when the PHS is enabled.

  Workaround: Use the **show cable modem classifier** command to get the related classifier counter.

- CSCsz13444

  Symptoms: The **show environment all** displays information about numerous fans, even though there is only one fan tray in the Cisco uBR7246VXR router.

  Conditions: This issue is seen on the Cisco uBR7246VXR universal broadband router with the NPE-G2 processor.

  Workaround: The status of the fan tray is displayed by Fan 2.

- CSCsz31339

  Symptoms: The downstream packet source MAC address is corrupted when a cable intercept is configured on the cable interface.

  Conditions: There are no specific conditions for this issue to occur.

  Workaround: There is no workaround.

- CSCsz78872

  Symptoms: A Cisco uBR7246VXR router with NPE G2 processor has wrongly assigned a common MAC address to two ports instead of unique MAC addresses.

  Workaround: There is no workaround.

- CSCta45315

  Symptoms: **ccwbFiberNodeDescrTable** MIB table does not read fiber node 256.

  Conditions: There are no specific conditions for this issue to occur.

  Workaround: Use the **show running-config | begin fiber** command to view description of fiber node 256.

- CSCtb82697

  Symptoms: The **show controller cable** command does not provide information about CPU revision.

  Conditions: There are no specific conditions for this issue to occur.

  Workaround: The **show tech** command provides information about the CPU revision.

- CSCtc43231

  Symptoms: SNMP traps and informs source interface do not work.

Conditions: This issue occurs when the **snmp-server trap-source Loopback0** and **snmp-server source-interface informs Loopback0** commands are configured.

Workaround: There is no workaround.

- CSCtc60776

  Symptoms: Layer 3 traffic cannot be forwarded by a Wideband CM in a non-MTC mode for a certain period of time after the Cisco CMTS has used the downstream channel change (DCC) to change its upstream with the initialization technique 1-4. The Wideband CM stays w-online.

  Conditions: This issue occurs on wideband CMs. However, CMs running in non-MRC mode are not affected.

  Workaround: Use the upstream channel change (UCC) if the wideband supports it.

- CSCtc60950

  Symptoms: The Cisco uBR7225VXR router hangs due to SYS-3-CPUHOG, which is caused by the EnvMon process.

  Conditions: This issue is observed on the Cisco uBR7225VXR universal broadband router.

  Workaround: There is no workaround.

- CSCtc92379

  Symptoms: Modems and service-flow counters update incorrectly.

  Conditions: This issue occurs when the CM instance is marked offline due to errors during the DCC rebuild.

  Workaround: There is no workaround.

- CSCtc93642

  Symptoms: Spurious memory accesses and tracebacks are observed after a ping time out.

  Conditions: The issue is seen on the Cisco IOS Release 12.2(33)SCB5 release.

  Workaround: There is no workaround.

- CSCtc96090

  Symptoms: The polling of the MIB object **IfHCInOctets** or **IfHCOutOctets** wraps at the 32-bit marker rather than at the expected 64-bit marker.

  Conditions: This issue is observed in Cisco IOS Release 12.2(33)SCB4.

  Workaround: There is no workaround.

- CSCtd18368

  Symptoms: When RF-channel 1 on one controller is shut down, RF-channel 1 on another controller also automatically shuts down.

  Conditions: This issue occurs when the wide band resiliency and cross-controller bonding group are configured.

  Workaround: There is no workaround.

- CSCtd33099

  Symptoms: The logical status of RF-channels in **show cable rf-status** command may still be in the DOWN state, after executing the **shut/no shut** commands on those RF-channels.

  Conditions: This issue occurs when the **shut/no shut** commands are executed on RF-channels of a bonding group in the IC controller.

  Workaround: There is no workaround.

- CSCtd35119

  Symptoms: There is two entries for each chassis slot container in the output of SNMP.

  Conditions: This issue occurs on the Cisco uBR7200 series universal broadband routers running the Cisco IOS releases and have the “Get entity” MIB Objects in the SNMP client.

  Workaround: There is no workaround.

- CSCtd53334

  Symptoms: Memory leak is observed on executing the **show cable filter verbose** command.

  Conditions: This issue occurs on the Cisco uBR7200VXR universal broadband router.

  Workaround: Do not execute the **show cable filter verbose** command on Cisco uBR7200VXR universal broadband router.

- CSCtd56821

  Symptoms: The Cisco uBR7225VXR universal broadband router may crash after running the **show packetcable gate summary** command.

  Conditions: This issue was observed with a PacketCable gate created on slot 1/0 on a Cisco uBR7225VXRuniversal broadband router.

  Workaround: There is no workaround.

- CSCtd60182

  Symptoms: Although the secondary wideband interface is down, it can still be selected as a multicast forwarding interface.

  Conditions: This issue is seen on the Cisco uBR7200 universal broadband routers running the Cisco IOS Release 12.2(33)SC.

  Workaround: When configuring a secondary wideband interface as multicast forwarding interface, ensure that the secondary wideband interface is not down.

- CSCtd78225

  Symptoms: High CPU usage seen after adding **privilege interface** commands.

  Conditions: This issue was observed on Cisco CMTS routers running the Cisco IOS Release 12.2(33)SCB5. After adding **privilege interface** commands, the CPU usage peaks. When the configuration is saved, the CPU takes a while to reload.

  Workaround: Do not use **privilege** commands.

- CSCtd87704

  Symptoms: Some Subscriber Account Management Interface Specification (SAMIS)/ IP Detail Record (IPDR) processes are incorrectly killed. This may cause memory leaks on the Route Processor (RP)/Network Processing Engine (NPE).

  Conditions: This issue is seen when there is high CPU usage on the RP/NPE and when SAMIS/IPDR is running.

  Workaround: There's no workaround.

- CSCtd93151

  Symptoms: The network is shut down by the IOS and the voltage from voltage monitor chip is about 10 percent less than normal value.

  Conditions: There are no specific conditions for this issue to occur.

Workaround: Disable the environment monitor feature by executing the **test cable envm off** command.

- CSCte20216

  Symptoms: Some cable modems, such as the DPC2505 cable modem report QAM/FEC lock failure (event type 2) when a secondary RF-channel is down, and report an MDD recovery (event type 4) when the RF-channel is UP, instead of reporting a QAM/FEC recovery.

  This causes QAM/MDD state transition error in the Cisco CMTS.

  Conditions: This issue is seen when a DPC2505 is connected to the Cisco CMTS.

  Workaround: There is no workaround.

- CSCte58329

  Symptoms: Layer 2 VPN configuration with BPI configuration failed on the Cisco CMTS router.

  Conditions: This issue is seen when both Layer 2 VPN and BPI are configured.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 12.2(33)SCB6

- CSCeh33888

  Symptoms: A Cisco uBR7246VXR router may reload with configurations set during the last watchdog reset.

  Conditions: This issue occurs on a Cisco uBR7246VXR router having a Cisco uBR7200-NPE-G1 processor board and is running Cisco IOS Release 12.3(9a)BC.

  Workaround: There is no workaround.

- CSCsi63649

  Symptoms: All routers synchronized to one router show the following error every 10 seconds:

  ```
  Apr 23 13:33:41.929: %SYS-3-TIMERNEG: Cannot start timer (0x7543D68) with negative
  offset (-996736100). -Process= "TTY Background", ipl= 0, pid= 42
  ```

  Conditions: This issue is observed on some Cisco Gigabit Switch Routers (GSR) running Cisco IOS Release 12.0(28)S, Cisco IOS Release 12.0(31)S, Cisco IOS Release 12.0(32)S, and Cisco IOS Release 12.0(32)SY. This issue occurs when a telnet session is initiated on the router, and a new telnet session is initiated simultaneously to a different device from the same telnet session. The error message is displayed every 10 seconds when the **exec-timeout** command does not disconnect the session and the timeout expires.

  Workaround: Use the **show users** command to determine which users are connected via telnet. Then use the **clear line** *x* command to clear the line and disconnect the session to stop the error messages.

- CSCsl50133

  Symptoms: The Cisco uBR7246VXR router reloads with following message:

  ```
  No crashinfo
  No tracebacks
  Last reload reason: Unknown reason
  Last reset from watchdog reset
  ```

  Conditions: This issue was first observed on a Cisco uBR7246VXR (UBR7200-NPE-G1) router running Cisco IOS Release 12.3(17b)BC4.

  Workaround: There is no workaround.

- CSCsy24676

  Symptoms: A false positive is returned when the file system fails. This results in the file operation displayed as successful even though it failed.

  Conditions: This issue occurs when the file system device returns an error and the code follows the path in the file system buffer cache where the error is masked and converts it to a success code. This issue occurs when there is a device error during the write. The device error may be due to bad media or an OIR.

  Workaround: There is no workaround.

- CSCta03480

  Symptoms: The configurations on the NPE-G1 processor and a line card do not synchronize.

  Conditions: This issue occurs when there is an excess load between the line card and the Cisco uBR7200-NPE-G1 processor board. The modem remains in reject(m) state.

  Workaround: Execute the **cable dynamic-secret exclude oui** command.

- CSCta28029

  Symptoms: Flows with excess information rate (EIR) and maximum information rate (MIR) have higher throughput than expected.

  Conditions: This issue occurs when EIR is higher than MIR and there is congestion on the upstream.

  Workaround: Ensure that MIR is greater than EIR.

- CSCta45075

  Symptoms: The **show interface multicast-session** command may show wrong multicast session instances.

  Conditions: This issue occurs after the following steps:

  1. An aggregate type GQC is created.
  2. The igmp join is sent to two sessions.
  3. The igmp leave is sent for session 1 and after seven seconds, to session 2.
  4. Session 2 is rejoined immediately after session 1 is deleted.

  Workaround: There is no workaround.

- CSCta77009

  Symptoms: A Cisco uBR7200 series router may report memory leaks.

  Conditions: This issue occurs when the dual-stack CPE devices are each running the FTP GET and FTP PUT requests.

  Workaround: There is no workaround.

- CSCtb74904

  Symptoms: The service flow counter displays the value 0.

  Conditions: This issue occurs during an RP switchover. However, the right service flow is used to forward the packets; the packets reach the CPEs as well.

  Workaround: There is no workaround.

- CSCtb79237

  Symptoms: No system log or SNMP trap is generated.

Conditions: This issue occurs in a PacketCable environment when the Common Open Policy Server (COPS) process that is used for packetcable fails.

Workaround: There is no workaround.

- CSCtb94400

  Symptoms: During reboot, the multicast service flow for the tunnel is not established.

  Conditions: This issue occurs during reboot if the **cable multicast group-qos default scn** *service-class-name* **aggregate** is not configured.

  Workaround: Configure the **cable multicast group-qos** command with **default scn** *service-class-name* **aggregate**.

- CSCtc09858

  Symptoms: If the tunnel is disabled, the traffic does not stop. However, if the tunnel is disabled when a "service class name" is not defined for the tunnel, the traffic stops, but re-enabling the tunnel does not restart traffic.

  Conditions: This issue is observed when the "service class name" is defined for the tunnel.

  Workaround: Stop and start the traffic; remove and add the tunnel group to the interface.

- CSCtc10231

  Symptoms: Upstream power adjustment indication is seen after a cable modem comes online.

  Conditions: This issue occurs once every hour when the **show cable modem flap** command is used.

  Workaround: There is no workaround.

- CSCtc11757

  Symptoms: The write operation fails when a disk card is removed while being updated, has some bad sectors, or does not respond when the card is being updated.

  Conditions: This issue is observed under the following two conditions:

  1. The disk card is removed while copying to disk or formatting the disk.
     If you then execute the **show file system**, **dir disk**, or **show disk** commands, the system hangs.
  2. During copy to disk operation, it is found that the card has bad sectors or is not responding.
     If you then execute the **show file system**, **dir disk**, or **show disk** commands, the system hangs.

  Workaround: For condition 1, avoid removing the card when the card is being updated.
  For condition 2, replace the bad card with a good card.

- CSCtc16252

  Symptoms: The **show inventory** command does not display the output until 15 minutes after bootup when there is no line card in the system.

  Conditions: This issue is observed on the Cisco uBR7200 series universal broadband router running Cisco IOS Release 12.2SC.

  Workaround: There is no workaround.

- CSCtc22435

  Symptoms: The MIB object **docsQosServiceFlowLogTable** returns a null value.

  Conditions: This issue occurs on the Cisco uBR7200 universal broadband router with “Keep QoS11 CM primary service flows counters” feature, while executing the **cable primary-sflow-qos11 keep all** command.

  Workaround: Unconfigure the feature by executing the **cable primary-sflow-qos11 keep all** command.

- CSCtc29046

  Symptoms: The write operation fails when a disk card is removed while being updated, has some bad sectors, or does not respond when the card is being updated.

  Conditions: This issue is observed under the following two conditions:

  1. The disk card is removed while copying to disk or formatting the disk.
     If you then execute the **show file system**, **dir disk**, or **show disk** commands, the system hangs.
  2. During copy to disk operation, it is found that the card has bad sectors or is not responding.
     If you then execute the **show file system**, **dir disk**, or **show disk** commands, the system hangs.

  Workaround: For condition 1, avoid removing the card when the card is being updated.
  For condition 2, replace the bad card with a good card.

- CSCtc55893

  Symptoms: The **init-tech-ovr** command in the load balancing group (LBG) does not function for the second logical channel.

  Conditions: This issue occurs when the second logical channel is selected as the source channel.

  Workaround: There is no workaround.

- CSCtc60776

  Symptoms: Layer 3 traffic cannot be forwarded by a Wideband CM in a non-MTC mode for a certain period of time after the Cisco CMTS has used the downstream channel change (DCC) to change its upstream with the initialization technique 1-4. The Wideband CM stays w-online.

  Conditions: This issue occurs on wideband CMs. However, CMs running in non-MRC mode are not affected.

  Workaround: Use the upstream channel change (UCC) if the wideband supports it.

- CSCtc60950

  Symptoms: The Cisco uBR7225VXR router hangs due to SYS-3-CPUHOG, which is caused by the EnvMon process.

  Conditions: This issue is observed on the Cisco uBR7225VXR router.

  Workaround: Disable the EnvMon process using the **test c7200 envm off** command.

- CSCtc61466

  Symptoms: The **cable intercept** command on the cable interface is found missing after executing the following commands.

  ```
  hw-module slot <x> stop, hw-module slot <x> start for MC28U card
  ```

  Conditions: This issue is observed on the Cisco uBR7200 router with the Cisco uBR-MC28U line card running Cisco IOS Release 12.2S or Cisco IOS Release 12.3.

  Workaround: There is no workaround.

- CSCtc62324

  Symptoms: A Cisco uBR7200 Series NPE crashes when dual-stack CPEs get the Layer 3 address using DHCP/DHCPv6.

  Conditions: This issue is observed with more than 300 dual-stack CPEs attempting to get both the IPv4 and IPv6 addresses through DHCP.

  Workaround: There is no workaround.

- CSCtc69216

Symptoms: There is an occurrence of a suspicious Any Transport over MPLS (AToM) L2VPN MPLS Peer Name TLV Parsing Logic, which causes the VCID error.

Conditions: This issue occurs when the AToM L2VPN on the CM configuration file is configured and the MPLS Peer Name TLV(37) is followed by VCID TLV(38).

Workaround: There is no workaround.

- CSCtc74969

  Symptoms: Cannot set the MIB object **docsIf3MdCfgMultTxChModeEnabled** to true.

  Conditions: This issue occurs on the Cisco uBR7200 universal broadband router.

  Workaround: Set “cable mtc-mode” using the CLI.

- CSCtc79306

  Symptoms: After configuring the MAC address in the bundle interface, the MAC state of the Cisco DPC3000 cable modem is found to be w-online and not UB w-online.

  Conditions: This issue occurs when the MAC address of the bundle interface is sent to the line card (LC) when configured under the LC cable interface. This causes the security association (SA) of the MAC Domain Descriptor (MDD) message and SYNC message to be different, which causes the Cisco DPC3000 cable modem to be w-online instead of UB w-online.

  Workaround: There is no workaround.

- CSCtc92379

  Symptoms: Modems and service-flow counters update incorrectly.

  Conditions: This issue occurs when the CM instance is marked offline due to errors during the DCC rebuild.

  Workaround: There is no workaround.

- CSCtc96090

  Symptoms: The polling of the MIB object **IfHCInOctets** or **IfHCOutOctets** wraps at the 32-bit marker rather than at the expected 64-bit marker.

  Conditions: This issue is observed in Cisco IOS Release 12.2(33)SCB4.

  Workaround: There is no workaround.

- CSCtd04983

  Symptoms: The Cisco uBR7200 VXR series router crashes at cmts_bundle_find_mcast_mac.

  Conditions: This issue is observed after the CPE clients rapidly join and leave the multicast groups.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(33)SCB6

- CSCsz45567

  A device running Cisco IOS Software, Cisco IOS XE Software, or Cisco IOS XR Software is vulnerable to a remote denial of service condition if it is configured for Multiprotocol Label Switching (MPLS) and has support for Label Distribution Protocol (LDP).

  A crafted LDP UDP packet can cause an affected device running Cisco IOS Software or Cisco IOS XE Software to reload. On devices running affected versions of Cisco IOS XR Software, such packets can cause the device to restart the mpls_ldp process.

A system is vulnerable if configured with either LDP or Tag Distribution Protocol (TDP).

Cisco has released free software updates that address this vulnerability.

Workarounds that mitigate this vulnerability are available.

This advisory is posted at:

http://www.cisco.com/warp/public/707/cisco-sa-20100324-ldp.shtml

- CSCtb13491

  A malformed Internet Key Exchange (IKE) packet may cause a device running Cisco IOS Software to reload. Only Cisco 7200 Series and Cisco 7301 routers running Cisco IOS software with a VPN Acceleration Module 2+ (VAM2+) installed are affected. Cisco has released free software updates that address this vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100324-ipsec.shtml.

- CSCtd81849

  Symptoms: File copy from active PRE2 to standby PRE2 may fail, or MD5 checksum may fail while reading a file on the disk.

  Conditions: This issue is observed on STI 7.4.0 Compact Flash and PCMCIA Flash cards.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 12.2(33)SCB5

- CSCeh33888

  Symptoms: The Cisco uBR7246VXR router reloads with the last reset from the watchdog reset.

  Conditions: The router has a Cisco uBR7200-NPE-G1 processor board and is running Cisco IOS Release 12.3(9a)BC.

  Workaround: There is no workaround.

- CSCsi63649

  Symptoms: All the routers are synchronized to one router and display the following message every 10 seconds:

  ```
  Apr 23 13:33:41.929: %SYS-3-TIMERNEG: Cannot start timer (0x7543D68) with
  negative offset (-996736100).
  -Process= "TTY Background", ipl= 0, pid= 42
  ```

  Conditions: This issue occurs when a telnet session is initiated on the router, and then a new telnet session to a different device is initiated from the telnet session. The exec-timeout does not disconnect the session even if no keystrokes are issued. When the timeout expires, the error message is displayed every 10 seconds.

  This issue is observed on some Cisco gigabit switch routers (GSRs) running Cisco IOS Release 12.0(28)S, Cisco IOS Release 12.0(31)S, Cisco IOS Release 12.0(32)S, and Cisco IOS Release 12.0(32)SY.

  Workaround: Use the **show users** command to determine which users are logged in through telnet. Then use **clear line X** to clear the line, disconnect the users, and stop the error messages.

- CSCsl50133

  Symptoms: The Cisco uBR7246VXR router reloads with following message:

  ```
  No crashinfo
  No tracebacks
  ```

```
Last reload reason: Unknown reason
Last reset from watchdog reset
```

Conditions: This issue is observed on a Cisco uBR7246VXR (UBR7200-NPE-G1) router running Cisco IOS Release 12.3(17b)BC4.

Workaround: There is no workaround.

- CSCsy24676

  Symptoms: A false positive is returned on a file system failure, that is, a file operation is returned as successful even when it has failed.

  Conditions: This issue occurs when the file system device returns an error and the code follows the path in the file system buffer cache where the error is masked and convert it to a success code. This issue occurs when there is a device error during the write. The device error may be due to bad media or an OIR.

  Workaround: There is no workaround.

- CSCta03480

  Symptoms: Configuration synchronization issue is observed between the Cisco uBR7200-NPE-G1 processor and a line card.

  Workaround: Execute the **cable dynamic-secret exclude oui** command.

- CSCta28029

  Symptoms: Flows with excess information rate (EIR) and maximum information rate (MIR) have higher throughput than expected.

  Conditions: This issue occurs when EIR is higher than MIR and there is congestion on the upstream.

  Workaround: Ensure that MIR is greater than EIR.

- CSCta45075

  Symptoms: The **show interface multicast-session** command may show wrong multicast session instances.

  Workaround: There is no workaround.

- CSCta77009

  Symptoms: A Cisco uBR7200 series universal broadband router reports memory leaks when the dual stack CPE devices are each running FTP GET and FTP PUT application.

  Workaround: There is no workaround.

- CSCtb20166

  Symptoms: Temporary packet drops observed on the line cards in the chassis.

  Conditions: This issue occurs due to online insertion and removal (OIR) of a line card in the chassis.

  Workaround: There is no workaround.

- CSCtb74904

  Symptoms: During the RP switchover, the service flow counter displays the value 0.

  Conditions: This issue occurs during an RP switchover. However, the right service flow is used to forward the packets; the packets reach the CPEs as well.

  Workaround: There is no workaround.

- CSCtb79237

Symptoms: No system log or SNMP trap is generated when the Common Open Policy Server (COPS) process that is used for packetcable, fails.

Conditions: This issue occurs in a packetcable environment where the COPS session fails.

Workaround: There is no workaround.

- CSCtb94400

  Symptoms: During reboot, the multicast service flow for the tunnel is not established.

  Conditions: This issue occurs during reboot if the **cable multicast group-qos default scn** *service-class-name* **aggregate** is not configured.

  Workaround: Configure the **cable multicast group-qos** command with *default scn service-class-name* aggregate.

- CSCtc05600

  Symptoms: The Cisco uBR7200 series universal broadband router reloads when a software-forced crash is issued by the SNMP.

  Conditions: This issue is observed on the Cisco uBR7200 series universal broadband router running Cisco IOS Release 12.2(33)SCB3.

  Workaround: Filter out the online insertion and removal (OIR) requests from SNMP requests.

- CSCtc09858

  Symptoms: If the tunnel is disabled, the traffic does not stop. However, if the tunnel is disabled when a “service class name” is not defined for the tunnel, the traffic stops, but reenabling the tunnel does not restart traffic.

  Conditions: This issue is observed when the "service class name" is defined for the tunnel.

  Workaround: Stop and start the traffic and remove and add the tunnel group to the interface.

- CSCtc10117

  Symptoms: There is memory leak with pool manager process.

  Conditions: This issue is observed when QoS is configured.

  Workaround: There is no workaround.

- CSCtc10231

  Symptoms: Upstream power adjustment indication is seen after a cable modem comes online.

  Conditions: This issue occurs once every hour when the **show cable modem flap** command is used.

  Workaround: There is no workaround.

- CSCtc11757

  Symptoms: The write operation fails when a disk card is removed while being updated, has some bad sectors, or does not respond when the card is being updated.

  Conditions: This issue is observed in the following two conditions:

  1. The disk card is removed while copying to disk or formatting the disk.
     If you then execute the **show file system**, **dir disk**, or **show disk** commands, the system hangs.
  2. During copy to disk operation, it is found that the card has bad sectors or is not responding.
     If you then execute the **show file system**, **dir disk**, or **show disk** commands, the system hangs.

  Workaround: For condition 1, avoid removing the card when the card is being updated.
  For condition 2, replace the bad card with a good card.

- CSCtc16252

Symptoms: The **show inventory** command does not display the output until 15 minutes after bootup, if there is no line card on the system.

Conditions: This issue is observed on the Cisco uBR7200 series universal broadband router running on the Cisco IOS Release 12.2SC.

Workaround: There is no workaround.

- CSCtc22435

  Symptoms: The docsQosServiceFlowLogTable returns a NULL value.

  Conditions: This issue occurs on the Cisco uBR7200 universal broadband router with "Keep QoS11 CM primary service flows counters" feature, while executing the **cable primary-sflow-qos11 keep all** command.

  Workaround: Unconfigure the feature by executing the cable primary-sflow-qos11 keep all command.

- CSCtc55893

  Symptoms: The **init-tech-ovr** command in the load-balancing group (LBG) does not function on the second logical channel.

  Conditions: This issue occurs when the second logical channel is selected as the source channel.

  Workaround: There is no workaround.

- CSCtc60776

  Symptoms: Layer 3 traffic cannot be forwarded by a Wideband CM in a non-MTC mode for a certain period of time after the Cisco CMTS has used the downstream channel change (DCC) to change its upstream with the initialization technique 1-4. The Wideband CM stays w-online.

  Conditions: The issue occurs on wideband CMs. However, CMs running in non-MRC mode are not affected.

  Workaround: Use UCC if the wideband support it.

- CSCtc60950

  Symptoms: The Cisco uBR7225VXR router hangs due to SYS-3-CPUHOG, which is caused by the EnvMon process.

  Conditions: This issue is observed on the Cisco uBR7225VXR router.

  Workaround: Disable the EnvMon process using the **test c7200 envm off** command.

- CSCtc61466

  Symptoms: The **cable intercept** command on the cable interface is found missing after executing the following commands.

  ```
  hw-module slot <x> stop, hw-module slot <x> start for MC28U card
  ```

  Conditions: This issue is observed on the Cisco uBR7200 with MC28U card running Cisco IOS Release 12.2S or Cisco IOS Release 12.3.

  Workaround: There is no workaround.

- CSCtc62324

  Symptoms: A Cisco uBR7200 Series NPE crashes when dual-stack CPEs get the Layer 3 address using DHCP/DHCPv6.

  Conditions: This issue is observed with more than 300 dual-stack CPEs attempting to get both IPv4 and IPv6 address through DHCP.

Workaround: There is no workaround.

- CSCtc69216

  Symptoms: There is an occurrence of a suspicious Any Transport over MPLS (AToM) L2VPN MPLS Peer Name TLV Parsing Logic, which causes the VCID error.

  Conditions: This issue occurs when the AToM l2VPN on the CM configuration file is configured and the MPLS Peer Name TLV(37) is followed by VCID TLV(38).

  Workaround: There is no workaround.

- CSCtc74969

  Symptoms: Unable to set the MIB object “docsIf3MdCfgMultTxChModeEnabled” to true.

  Workaround: Use the **cable mtc-mode** command to set the MIB object "docsIf3MdCfgMultTxChModeEnabled" to true.

- CSCtc79306

  Symptoms: After configuring the MAC address in the bundle interface, the MAC state of the Cisco DPC3000 cable modem is found to be w-online and not UB w-online.

  Conditions: This issue occurs when the MAC address of the bundle interface is sent to the line card (LC) when configured under the LC cable interface. This causes the security association (SA) of the MAC Domain Descriptor (MDD) message and SA of the SYNC message to be different, which causes the Cisco DPC3000 cable modem to be w-online instead of UB w-online.

- CSCtc92379

  Symptoms: Modems and service-flow counters update incorrectly.

  Conditions: This issue occurs when the CM instance is marked offline due to errors during the DCC rebuild.

  Workaround: There is no workaround.

- CSCtc96090

  Symptoms: The polling of IfHCInOctets or IfHCOutOctets objects wrap at the 32-bit marker rather than the expected 64-bit marker.

  Conditions: This issue is observed in Cisco IOS Release 12.2(33)SCB4.

  Workaround: There is no workaround.

- CSCtd04983

  Symptoms: The Cisco 7200 VXR series router crashes at cmts_bundle_find_mcast_mac.

  Conditions: This issue is observed after the v4 CPE clients rapidly join and leave the multicast groups.

Resolved Caveats—Cisco IOS Release 12.2(33)SCB5

- CSCin79116

  Symptoms: Issuing **show** commands push the CPU utilization to 100%.

  Conditions: Long running **show** commands, such as **show running-config**, **show voice call summary**, and **show memory summary** affect voice call processing adversely, even if they are periodically suspend.

  Workaround: There is no workaround.

- CSCsm13892

  Symptoms: A traceback occurs when you reset the line cards and the following output is displayed:

  ```
  RTTY ISSU Start Nego failed: rc: -287
  %ISSU-3-NOT_REG_UNDER_ENTITY: msg session(528938704) is not registered under client
  ISSU RTTY Client(2033) and entity(1)
  -Traceback= ...
  Error in rtty_issu_unregister_sessions at 103
  %C7600_PWR-SP-4-DISABLED: power to module in slot 2 set off (Reset)
  ```

  Conditions: This issue occurs after the Online Insertion and Removal (OIR) for the cards in the chassis.

  Workaround: There is no workaround.

- CSCsq71492

  Symptoms: A Cisco IOS device reloads with an address error or has alignment errors and tracebacks such as %ALIGN-3-SPURIOUS or %ALIGN-3-TRACE.

  Conditions: This issue is most likely to occur when the TACACS+ server (ACS) sends an "authentication error" when ACS is configured, or when a request timeout occurs. There may be other AAA or TACACS-related conditions that cause the symptom.

  Workaround: There is no workaround.

- CSCsq75944

  Symptoms: A Cisco Catalyst 6500 Series/7600 Series Wireless Services Module (WiSM) reloads unexpectedly. On the console or in the Route Processor (RP) crashinfo file, the following message is displayed:

  ```
  %SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = Per-Second Jobs
  ```

  Conditions: This issue occurs when the Cisco IOS NetFlow is configured on one of the following:

  - Cisco Catalyst 7600 Series Wireless Services Module (WiSM) running Cisco IOS Release 12.2(33)SRC
  - Cisco Catalyst 6500 Series Wireless Services Module (WiSM) running Cisco IOS Release 12.2SXH.

  Workaround: Disable Cisco IOS NetFlow by using one of the following commands on every subinterface for which Cisco IOS NetFlow is configured:

  ```
  no ip flow ingress
  no ip flow egress
  no ip route-cache flow
  ```

- CSCsw26713

  Symptoms: A Cisco uBR7200 series universal broadband router experiences cable interface line card memory leaks.

  Workaround: There is no workaround.

- CSCsx97071

  Symptoms: Multicast packets are not accounted for.

  Conditions: This issue occurs when sending multicast traffic. The packets are received properly, but they are not accounted for.

  Workaround: There is no workaround.

- CSCsy14105

  Symptoms: The value range of the MIB object “ccmtrCollectionInterval” is not consistent with the command. The valid range for the MIB object is 15 to 1440, but for the command, the valid range is 2 to 1440.

  Conditions: This issue occurs while setting the MIB object “ccmtrCollectionInterval” using the SNMP set operation.

  Workaround: Set the interval using the command.

- CSCsz21732

  Symptoms: A Cisco router reloads when it is configured for SNMP inform notifications.

  Workaround: Disable the SNMP informs with the command **no snmp-server host host-address informs**.

- CSCsz73611

  Symptoms: The Cisco CMTS accepts inconsistent “per-SF L2VPN TLV” in the cable modem configuration file.

  Conditions: This issue occurs when:

  – Upstream service flow (US-SF) or Downstream Confirmation-to-Receive (DS-CFR) vendor-specific TLV is specified.

  – L2VPN VPNID is specified in the vendor-specific TLV.

  – The VPNID does not match any of the top-level L2VPN TLV VPNIDs.

  Workaround: There is no workaround.

- CSCta22034

  Symptoms: A traceback is seen at the cmts_delete_entry function after a toggling the CPEs on and off multiple times.

  Conditions: This issue occurs when the CPEs are configured with dual-stack IP and IPv6-only addresses, and are all configured behind one cable modem.

- CSCta32291

  Symptoms: The NPE of a Cisco uBR7246VXR universal broadband router crashes while running the multicast protocol.

  Conditions: This issue occurs when the router has a Cisco uBR7200-NPE-G1 processor board and is running Cisco IOS Release 12.2(33)SCB.

  Workaround: There is no workaround.

- CSCta89403

  Symptoms: When CPE under legacy cable modems do an IGMP join, and MQoS configuration requires the multicast session encrypted, the Cisco CMTS sends a MAP reject message to cable modems. In this case, multicast traffic cannot be sent to the CPE.

  Conditions: This issue is observed on the Cisco uBR7200 and Cisco uBR10000 series universal broadband routers running the Cisco IOS Release 12.2S.

  Workaround: There is no workaround.

- CSCta89599

  Symptoms: The entAliasMappingTable does not have entries for the upstreams of the first MAC of the Cisco uBR-MC28U line cards (for example, for a Cisco uBR-MC28U line card in Slot 3, upstreams belonging to Cable3/0 are missing).

Conditions: This issue is observed on the Cisco uBR7200 universal broadband routers with Cisco uBR-MC28U line cards running the Cisco IOS Release 12.2(33)SCB.

Workaround: There is no workaround.

- CSCtb20975

  Symptoms: The **cable source_verify** command does not work with the bundle interface after sub bundle test.

  Conditions: This issue is observed on the Cisco uBR7200 universal broadband routers running the Cisco IOS Release 12.2S.

  Workaround: There is no workaround.

- CSCtb28349

  Symptoms: If a cable modem sends a Dynamic Channel Change response (DCC-RSP) to confirm the dcc_req indicating the target channel is exactly the one that the modem gets online and the technique is larger than 0, the line card crashes when it processes this DCC-RSP.

  Conditions: This issue occurs only when the DPC3K modem responds to dcc_rsp to confirm the dcc_req.

  Workaround: Do not use the test command on the DPC3K modem to trigger this issue.

- CSCtb66848

  Symptoms: After upgrade to Cisco IOS Release 12.3(23)BC8, Cisco uBR-MC28U line cards continue to crash.

  Workaround: There is no workaround.

- CSCtb71251

  Symptoms: Attempting to issue a **debug cable dhcp** command after enabling the logging discriminator crashes the active and secondary PREs.

  Conditions: This issue occurs on both the PRE2 and PRE4.

  Workaround: Remove the logging discriminator or do not run the **debug cable dhcp** command.

- CSCtb95119

  Symptoms: Configuring the RCC template using SNMP leads to the wrong receive channel profile (RCP) ID.

  Conditions: This issue occurs when the RCC template is configured using SNMP.

  Workaround: Use CLI to configure the RCC template.

- CSCtc02317

  Symptoms: The DOCS-DIAG-MIB has a timestamp with no timezone information (length is 8).

  Conditions: This issue occurs when DOCS-DIAG-MIB items are populated.

  Workaround: Clear the current timezone setting to UTC timezone. This causes the timezone offset to be 0, which can be safely ignored.

- CSCtc11425

  Symptoms: When the same DSG tunnel is configured in different cable interfaces that are slaves to different bundle interfaces and then the DSG tunnel MAC address is modified, the Cisco uBR10000 and Cisco uBR7200 series universal broadband router stops working.

  Conditions: This issue is observed on the Cisco uBR10000 and Cisco uBR7200 series universal broadband routers running the Cisco IOS Release 12.2(33)SCB.

- CSCtc17575

  Symptoms: The **cable privacy hotlist cm <a.a.a>** command does not block cable modem (CMs) from coming online.

  Conditions: This issue occurs when the CMs do not have the appropriate certificates.

  Workaround: There is no workaround.

- CSCtc22051

  Symptoms: Removing nonexistent multicast group configuration (GC) ID on the interface causes existent multicast GC to be partially lost on the interface; and these existent global multicast GC cannot be removed and display the following error:

  ```
  Error: MQOS Group Config found configured on interface(s),
   remove from interface first
  ```

  Conditions: This issue occurs when you incorrectly type the multicast GC ID you want to remove on interface or if the GC ID you want to remove is larger than any existent GC ID on that interface.

  Workaround: There is no workaround.

- CSCtc22065

  Symptoms: Concurrent IGMP requests populate multicast service flow counter with wrong aggregated MQoS configurations, that is, on CPE side a total 200 Kbps for two multicast sessions, but only shows 100 Kbps on the Cisco CMTS side.

  Conditions: This issue is observed when multiple IGMP join reports arrive on CMTS almost at the same time.

  Workaround: There is no workaround.

- CSCtc42632

  Symptoms: The Cisco uBR7225VXR may hang due to SYS-3-CPUHOG, which is caused by EnvMon process.

  Conditions: This issue is observed on the Cisco uBR7225VXR routers.

  Workaround: Disable the EnvMon process with the following command:

  Router#test c7200 envm off

- CSCtc45156

  Symptoms: The CM is found stuck in the reject(c) state. If you run the **debug cable tlv** and **debug cable mac-address <cm-mac> verb** commands, the log displays the following:

  ```
  ......
  SLOT 4: Oct  8 15:19:59.098 CST:        Service Class Name : us_sc      ^D
  ......
  SLOT 4: Oct  8 15:19:59.098 CST:        Service Class Name : ds_sc      ^D
  ......
  SLOT 4: Oct  8 15:19:59.098 CST:  Can't find service class name.
  SLOT 4: Oct  8 15:19:59.098 CST:  Can't find service class name.
  SLOT 4: Oct  8 15:19:59.098 CST: MDF DISABLE for CM 0019.474e.e0b6
  SLOT 4: Oct  8 15:19:59.098 CST: Registration failed for Cable Modem 0019.474e.e0b6 on
  interface Cable4/0/U5:
  CoS/Sflow/Cfr/PHS failed in REG-REQ
  ```

  Conditions: This issue occurs when the CM configuration file includes the **service class name** command for US/DS service flows.

  Workaround: There is no workaround.

- CSCtc58147

  Symptoms: The CM is found stuck in the reject(c) state. If you run the **debug cable tlv** and **debug cable mac-address <cm-mac> verb** commands, the log displays the following:

```
......
SLOT 4: Oct 15 13:16:23.379: Found Upstream Service Flow TLV
SLOT 4: Oct 15 13:16:23.379:    Service Flow Reference : 1
SLOT 4: Oct 15 13:16:23.379:    Service Class Name String Length 16, Exceeds Limit of
15
SLOT 4: Oct 15 13:16:23.379: PARSER-ERROR: TLV 4 has bad length 16
SLOT 4: Oct 15 13:16:23.379: Primary CoS/Sflow encodings missing. CoSs:0 Sflows[US,
DS]: [1, 0]
SLOT 4: Oct 15 13:16:23.379: Registration failed for Cable Modem 001a.c3ff.d77e on
interface Cable4/0/U1:
CoS/Sflow/Cfr/PHS failed in REG-REQ-MP
```

  Conditions: This issue is observed when the CM configuration file includes **service class name** of 15 bytes for US/DS service flow.s

  Workaround: Change the **service class name** string to less than 15 bytes.

- CSCtc85728

  Symptoms: The Cisco Broadband Troubleshooter (CBT) 3.3 continuous sweep function fails when performed on the Cisco uBR10000 series universal broadband routers with PRE4 line cards.

  Conditions: This issue is observed on the Cisco IOS Release 12.2(33)SCB4. This issue occurs when the CISCO-CABLE-SPECTRUM-MIB::ccsSpectrumRequestTable - ccsSpectrumRequestOperState MIB object returns a value of 10.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 12.2(33)SCB4

- CSCeh33888

  Symptoms: A Cisco uBR7246VXR router may reload with the last reset from watchdog reset.

  Conditions: The router has a Cisco uBR7200-NPE-G1 processor board and is running Cisco IOS release 12.3(9a)BC.

  Workaround: There is no workaround.

- CSCsi43840

  Symptoms: The Cisco uBR7246VXR-MC28U line card resets with no crash file being generated in bootflash.

  Conditions: The problem may occur on some Cisco uBR7246VXR router with multiple MC28U cards.

  Workaround: There is no workaround.

- CSCsl01427

  Symptoms: In syntax check mode, if there is a standby in SSO mode, the **cts dot1x** command does not work.

  Workaround: There is no workaround.

- CSCsu00342

  Symptoms: A drop in multicast streams is seen after changing the IGMP query interval, using the **ip igmp query-interval** command.

Conditions: This issue occurs in Cisco 7600 chassis with Sup720 engine running Cisco IOS release 12.2(33)SRB. The Cisco 7600 is configured with IGMPV3 and running Source Specific Multicast (SSM).The multicast stream(s) restore itself within 40-60 seconds.

Workaround: There is no workaround.

- CSCsu18117

  Symptoms: ToS value on multicast packets are being incorrectly overwritten.

  Conditions: This issue occurs in routers using Cisco IOS release 12.2(33)SCB.

  Workaround: There is no workaround.

- CSCsv41456

  Symptoms: Tracebacks and duplicate ifIndex messages are observed on an MPLS layer interface.

  Conditions: This is observed while adding MPLS configuration to a subinterface when the interface is already configured.

  Workaround: Remove the MPLS configuration on the subinterface prior to deleting it.

- CSCsv41886

  Symptoms: CMTS crashes and the following error message is seen when the **no ip routing** or the **no router bgp xx** command is run.

  ```
  %IPRT-3-IPDB_DEL_ERROR: i_pdb delete error bgp, 4, 210074C8, 20E322E0, 0, 0 -Process=
  "IP RIB Update", ipl= 0, pid= 117, -Traceback= 0x61FD7F58 0x62005498 0x62006D24
  ```

  Conditions: A large number of VRFs are configured and BGP is also configured to support these VRFs.

  Workaround: There is no workaround.

- CSCsw14622

  Symptoms: The last character in the Service Class Name field is dropped in Subscriber Account Management Interface Specification (SAMIS) records as well as in the SNMP MIB docsQosServiceFlowLogServiceClassName.

  Conditions: This occurs due to deleted service flows.

  Workaround: There is no workaround.

- CSCsw26713

  Symptoms: A Cisco uBR7200 series router may experience cable line card memory leaks.

  Workaround: There is no workaround.

- CSCsw37209

  Symptoms: Source verification of IPV6 packets does not happen, although the **cable ipv6 source-verify** command is configured on cable interface of a Cisco uBR7200 router.

  Conditions: This issue occurs when Cisco IOS 12.2S release is running on a Cisco uBR7200 router.

  Workaround: There is no workaround.

- CSCsw49188

  Symptoms: Cable metering fails and enters a “hung” state.

  Conditions: This occurs when the **ip tcp timestamp** command is configured globally.

  Workaround: Do not use the **ip tcp timestamp** command.

- CSCsx20724

  Symptoms: A Cisco uBR7246VXR router may crash when the **cable monitor** command is executed and when a **shut** command is run on the cable interface.

  Conditions: This occurs when the multicast traffic is transmitted using DSG.

  Workaround: Do not execute the **cable monitor** command.

- CSCsx93502

  Symptoms: The multicast traffic rate on one of the cable interfaces is less than the configured QoS rate limit when two or more cable interfaces are bundled together in a layer 3 bundle interface, and multicast traffic is sent on the bundle interface.

  Workaround: There is no workaround.

- CSCsy14105

  Symptoms: The value range of the MIB object “ccmtrCollectionInterval” is not consistent with the command. The valid range for MIB object is from 15 to 1440, but for the command, the range is from 2 to 1440.

  Conditions: This issue occurs while setting the MIB object “ccmtrCollectionInterval” using the SNMP set operation.

  Workaround: Set the interval using the command.

- CSCsy37677

  Symptoms: A crash is observed on the CMTS.

  Conditions: This issue is seen when ETDB show commands are paused and multicast sessions are removed because a CPE leaves or a CM goes offline.

  Workaround: Set the term length to 0 for not pausing while displaying the command.

- CSCsy56666

  Symptoms: The **cable primary-sflow-qos11 keep snmp-only** command is not working as expected and the primary service flow packet/byte count is not retained after the cable modem is reset.

  Conditions: This issue is observed in DOCSIS 1.1 specific modems after reset.

  Workaround: Clear the cable modem counters associated with primary service flows.

- CSCsy78163

  Symptoms: A Cisco uBR7200 series router may experience spurious memory access when the **hw-module slot x stop** and **hw-module slot x start** commands are executed.

  Workaround: There is no workaround.

- CSCsz23477

  Symptoms: A Cisco uBR7200 series router may crash due to igmp timer timeout or igmp leaves when the **show interfaces multicast-session** command is executed.

  Workaround: There is no workaround.

- CSCsz28000

  Symptoms: Multicast sessions are not created for static group when the Group Config parameters are changed.

  Workaround: Remove the static group by running the **ip igmp static-group** command and reapply the configuration.

- CSCsz31339

  Symptoms: The downstream packet source MAC address is corrupted when a cable intercept is configured on the cable interface.

  Workaround: There is no workaround.

- CSCsz37070

  Symptoms: A Cisco uBR7246VXR router may report fan tray failure when the environmental temperature is lesser than 0 degrees C.

  Workaround: There is no workaround.

- CSCsz59845

  Symptoms: A Cisco uBR7246VXR router may report multiple memory leaks when the **show memory debug leak** command is executed.

  Workaround: There is no workaround.

- CSCsz67716

  Symptoms: The "Gate Report State" counter in the output of the **show packetcable cms verbose** command does not increment for PacketCable Multimedia (PCMM) policy servers.

  Conditions: This issue is seen for PCMM policy servers.

  Workaround: There is no workaround.

- CSCsz73611

  Symptoms: CMTS will accept inconsistent "per-SF L2VPN TLV" in the cable modem configuration file.

  Conditions: This is seen in the following conditions:

  - Upstream service flow (US-SF) or Downstream Confirmation-to-Receive (DS-CFR) Vendor Specific TLV is specified.
  - L2VPN vpnid is specified in the Vendor Specific TLV.
  - The Vpnid does not match any of the top-level L2VPN TLV vpnid.

  Workaround: There is no workaround.

- CSCsz75180

  Symptoms: CMTS may crash when an MPLS subinterface is deleted.

  Workaround: Do not delete the subinterface.

- CSCsz78872

  Symptoms: A Cisco uBR7246VXR router with NPE G2 processor has wrongly assigned a common MAC address to two ports instead of unique MAC addresses.

  Workaround: There is no workaround.

- CSCta03480

  Symptoms: Configuration synchronization issue has been observed between the NPE-G1 processor and a line card.

  Workaround: Execute the **cable dynamic-secret exclude oui** command.

- CSCta05721

  Symptoms: A Cisco uBR7200 series router may report very high and unexpected multicast traffic on a default multicast service flow.

Workaround: There is no workaround.

- CSCta07903

  Symptoms: The EPC2100 may reset due to overload of the upstream traffic.

  Symptoms: This issue was observed on a Cisco uBR7200 series router with the Cisco MC5x20H or MC8x8 line cards.

  Workaround: Configure **ingress-noise-cancellation** or disable rate-adapt.

- CSCta21291

  Symptoms: A Cisco uBR7246VXR router wrongly displays the CPE MAC address rather than the MAC address of the cable modem when the **show cable modem** command is run.

  Workaround: There is no workaround.

- CSCta32291

  Symptoms: The NPE of a Cisco uBR7246VXR router may crash while running the multicast protocol.

  Conditions: The router has a Cisco uBR7200-NPE-G1 processor board and is running Cisco IOS release 12.2(33)SCB.

  Workaround: There is no workaround.

- CSCta45075

  Symptoms: The **show interface multicast-session** command may show wrong multicast session instances.

  Workaround: There is no workaround.

- CSCta49190

  Symptoms: CMTS does not add IP address to the relayed DHCP packets.

  Workaround: There is no workaround.

- CSCta77009

  Symptoms: A Cisco uBR7200 series router may report memory leaks when the dual stack CPE devices are each running FTP GET and FTP PUT application.

  Workaround: There is no workaround.

- CSCtb05948

  Symptoms: CMTS watchdog timeout crash is observed at cmts_address_filter or cmts_cm_lookup.

  Workaround: Downgrade the image version to Cisco IOS Release 12.2(33)SCB2.

Resolved Caveats—Cisco IOS Releases 12.2(33)SCB4

- CSCsh11476

  Symptoms: A Cisco uBR7246VXR router may crash after displaying the following watchdog timeout error message:

  ```
  %SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = CMTS METERING EXPORT
  Process.
  ```

  Conditions: This issue is observed when the router crashes during the process of writing a file to the flash disk.

  Workaround: There is no workaround.

- CSCsj45943

  Symptoms: The **no ip dhcp relay info policy removal pad** config command has no effect.

  Workaround:

  1. Copy the running config to the tftp or ftp server and edit it so that this config line is removed.
  2. Copy this edited configuration to nvram:startup-config.
  3. Reload the router.

- CSCsx20927

  Symptoms: The startup configuration information for a standby RP is not displayed.

  Workaround: There is no workaround.

- CSCsx70889

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

  Cisco has released free software updates that address this vulnerability.

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-tunnels.

- CSCsy07555

  Cisco IOS devices that are configured for Internet Key Exchange (IKE) protocol and certificate based authentication are vulnerable to a resource exhaustion attack. Successful exploitation of this vulnerability may result in the allocation of all available Phase 1 security associations (SA) and prevent the establishment of new IPsec sessions.

  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-20090923-ipsec

- CSCsy15227

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

  There are no workarounds that mitigate this vulnerability.

  This advisory is posted at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-auth-proxy

- CSCsy85008

  Symptoms: The ifInOctets reported erroneous CPU usage.

  Conditions: This issue is observed on the Cisco uBR7200 series router.

  Workaround: There is no workaround.

- CSCsz15590

  Symptoms: A Cisco uBR7246VXR router may hang after it is reset with large downstream traffic passing through the Gigabit Ethernet line card.

  Conditions: The issues is observed on a Cisco uBR7200 series that has large traffic passing through the Gigabit Ethernet line card.

  Workaround: Directly load the image by rommon.

- CSCsz25465

  Symptoms: A few cable modems may be stuck at reject(pk) or w-reject(pk) permanently during OIR or hw-module reset.

  Workaround: Power cycle the cable modem so that the state changes to online(pt) or w-online(pt) state.

- CSCsz44822

  Symptoms: A Cisco uBR7200 series router may crash indicating the following error.

  ```
  *Apr 22 22:40:50.363: %SYS-2-CHUNKBADREFCOUNT: Bad chunk reference count, chunk
  92B3A70 data 92BB3C4 refcount FFFFFFFF alloc pc 69AFF4. -Process= "CMTS SID mgmt
  task", ipl= 3, pid= 74
  -Traceback= B5CB14 B5D334 CAB9F0 CABE1C 69BC50 73A850 762C38 641FF4 641C4C 641E80
  646CE0 917318
  chunk_diagnose, code = 3
  chunk name is CMTSPCTYPE
  ```

  Conditions: The **cable helper-address** command is configured to be the same as the bundle IP address.

  Workaround: There is no workaround.

- CSCsz52508

  Symptoms: The **test cable dcc frequency** command moves one modem to target frequency does not work when the upstream channel ID of the modem does not belong to the target downstream channel.

  Conditions: This issue only affects **test cable dcc frequency** command.

  Workaround: Use **test cable dcc frequency** command to move the modem where the upstream channel ID belongs to the target downstream channel.

- CSCsz52617

  Symptoms: The cdxIfUpChannelAvgUtil reports incorrect numbers when rate adapt is enabled on the router.

  Conditions: This is seen when using SNMP to poll cdxIfUpChannelAvgUtil with rate adapt enabled.

  Workaround:

  1) Use CLI to obtain numbers

  2) Disable rate-adapt

- CSCsz60620

  Symptoms: A Cisco uBR7246VXR router may experience a silent reload.

  Workaround: There is no workaround.

- CSCsz66321

  Symptoms: Static routes that are configured may be lost after reloading the Cisco uBR7225VXR router.

  Workaround: Re-configure the **ip route** command after reloading the router.

- CSCsz67961

  Symptoms: The PacketCable Multimedia (PCMM) calls fail as the Gate Set Ack/Err is not received.

  Conditions: This issue is seen in PCMM calls with a small value used for timer T1 (such as 1 second).

  Workaround: Use larger values for the PCMM timer T1 (at least 5 seconds).

- CSCsz74267

  Symptoms: A Cisco uBR7225VXR router may fail to boot up at PCI Error Interrupt.

  Workaround: Boot the system using the Cisco IOS image directly.

- CSCsz76564

  Symptoms: The **cable primary-sflow-qos11 keep snmp-only** command is not working as expected and the primary service flow packet/byte count is not retained after the cable modem is reset.

  Conditions: This issue is observed in DOCSIS 1.1 specific modems after reset.

  Workaround: Clear the cable modem counters associated with primary service flows.

- CSCta16416

  Symptoms: A Cisco MC28U line card crashes with Data Bus Error exception.

  Workaround: There is no workaround.

- CSCta31219

  Symptoms: Dropped or delayed DOCSIS MAC management packets resulted in problems such as call failures.

  Conditions: Combination of Multicast QoS configuration with BPI+ encryption coupled with the blocking of IGMP for those same multicast groups.

  Workaround: Do not configure multicast QoS with BPI+ for groups where IGMP is blocked.

- CSCta39725

  Symptoms: After the CMTS reload, samis-cable metering source-interface configuration is removed from the running configuration.

  Conditions: This issue is observed on a Cisco uBR7200 series router running Cisco IOS Release 12.2(33)SCB.

  Workaround: Re-configure the cable metering source-interface.

- CSCta62911

  Symptoms: The **ip dhcp relay info policy removal pad** command is not ISSU compliant.

  Conditions: ISSU cannot be conducted and the CMTS must be reloaded.

  Workaround: There is no workaround.

- CSCta67001

  Symptoms: CMTS crashes when removing the flash card.

  Workaround: There is no workaround.

- CSCta83557

  Symptoms: The cable modem information is not displayed when executing the **show cable modem** command after using the DCC command.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS Release12.2(33)SCB3

- CSCsz07955

  Symptoms: CMTS crashes when using on a bad PCMCIA flash card.

  Conditions: This issue occurs when accessing a bad PCMCIA flash card using SNMP or dir.

Workaround: Avoid using a bad PCMCIA flash card.

- CSCsi43840

  Symptoms: The Cisco uBR7246VXR-MC28U card resets with no crash file being generated in bootflash memory.

  Conditions: This issue occurs on some Cisco uBR7246VXR routers with multiple Cisco UBR-MC28U cards.

  Workaround: There is no workaround.

- CSCsz25465

  Symptoms: Upon online insertion and removal (OIR) of the line card or executing a **hw-module reset** command, some of the cable modems get stuck at reject (pk) state or w-reject (pk) state permanently.

  Conditions: This issue in seen when Baseline Privacy Interface (BPI) is enabled.

  Workaround: Power cycle the cable modem to bring it to online(pt) or w-online (pt) state.

- CSCsy14105

  Symptoms: The value range of MIB object “ccmtrCollectionInterval” is not consistent with the command range. The valid value range is set at 15-1440 for MIB object and the command value range is set at 2-1440.

  Conditions: This issue is seen while setting the value range of the MIB object “ccmtrCollectionInterval” using the SNMP set operation.

  Workaround: Set the interval using the **cable metering destination** command.

- CSCsy85008

  Symptoms: A The “ifInOctets” counter values closely follows an abnormal roll-over after a normal roll-over.

```
2009-03-24 15:15:39 - 4076758789
2009-03-24 15:20:39 - 524459145          <========== a normal roll-over
2009-03-24 15:25:46 - 726658247
2009-03-24 15:31:08 - 939124784
2009-03-24 15:35:39 - 583325062         <============an abnormal roll-over
2009-03-24 15:41:11 - 801102043
```

  Conditions: This issue is seen when there is a roll-over between the first and second polls on “ifInOctets” list. This is a normal roll-over for a 32-bit counter. However, there is an abnormal roll-over between the fourth and fifth polls.

  Workaround: There is no workaround.

- CSCsv82736

  Symptoms: The modem cannot come online on the upstream. This issue was first detected in Cisco IOS Release 12.3(21a)BC6. The modem reaches the init(r1) or init(r2) state but, fails to proceed further.

  Conditions: This issue appeared at the site in Cisco IOS Release 12.3(21a)BC6. It is a a very rare condition.

  Workaround: Use **shutdown** or **no shutdown** command.

- CSCsy79015

  Symptoms: The Cisco uBR7200 router crashes during IPC processing.

  Conditions: This issue is seen when one or more debug commands are enabled that can cause a large number of messages are printed.

Workaround: Disable the debug commands.

- CSCsw26713

  Symptoms: A memory leak is observed.

  Conditions: This issue occurs when:

  - Creating tlv_encode_fragm and no CMs exist
  - Creating a init_npe_packet_system
  - Changing the upstream DOCSIS mode to ATDMA first and then changing it to another mode (like tdma): cmts_mac_sched_build_ugs_lookup_tables
  - Configuring crypto on NPE and enabling BPI to make CMs online(pt): crypto_process_root_cert_s and crypto_certc_get_name_der_from_cert_internal

  Workaround: There is no workaround.

- CSCsw37209

  Symptoms: Source verification of IPv6 packets does not occur even when the **cable ipv6 source-verify** command is configured on the cable interface of the Cisco uBR7200 router.

  Conditions: This issue occurs when Cisco IOS Release 12.2S is running on the Cisco uBR7200 router.

  Workaround: There is no workaround.

- CSCsz31339

  Symptoms: The downstream packet source MAC address is corrupted. The expected source address should be the MAC address of the bundle interface.

  Conditions: This issue occurs in when any cable intercept is configured on the cable interface.

  Workaround: There is no workaround.

- CSCso71883

  Symptoms: The string command fails to run in the Cisco IOS Tcl shell.

  Conditions: This issue occurs while running string commands in the Cisco IOS Tcl shell.

  Workaround: There is no workaround.

- CSCsy78163

  Symptoms: A spurious memory access is observed on the CMTS after issuing **hw-module slot x stop** and **hw-module slot x start** commands.

  Conditions: This issue is seen after issuing **hw-module slot x stop** and **hw-module slot x start** commands.

- CSCsy56666

  Symptoms: The primary service flow packet and byte count is not retained once after the cable modem is reset.

  Conditions: This issue is seen in DOCSIS 1.1 provisioned modems.

  Workaround: Remove DOCSIS 1.0 from the cable modem and ensure that the service flow flag for DOCSIS 1.1 (cmts_qos11_primary_sf_keep) is not set. Clear the cable modem counters associated with primary service flows.

- CSCsu18117

  Symptoms: The ToS value on multicast packets are incorrectly overwritten.

Conditions: This issue occurs in routers using Cisco IOS Release 12.2(33)SCB.

Workaround: There is no workaround.

- CSCsz72547

  Symptoms: The Cisco uBR7200 router reboots automatically.

  Conditions: This issue was first seen on the Cisco uBR7246VXR (Cisco uBR7200-NPE-G1) router running Cisco IOS Release12.3(21a)BC4.

  Workaround: There is no workaround.

- CSCsz59845

  Symptoms: Multiple memory leaks are observed on issuing **show memory debug leak** command on the Cisco uBR7246VXR line card.

  Conditions: This issue occurs when issuing the **show memory debug leak** command on the Cisco uBR7246VXR line card.

  Workaround: There is no workaround.

- CSCsy37677

  Symptoms: A crash is observed on the CMTS.

  Conditions: This issue is seen in cases ETDB show commands are paused and multicast sessions removed because a Customer Premises Equipment (CPE) issue a leave request or CM goes offline.

  Workaround: Set the term length to “0” to prevent the pause while displaying the command.

- CSCsz73611

  Symptoms: CMTS will accept inconsistent “per-SF L2VPN TLV” in the cable modem configuration file.

  Conditions: This is when the:

  - Upstream service flow (US-SF) or Downstream Confirmation-to Receive (DS-CFR) vendor-specific TLV is specified
  - L2VPN vpnid is specified in the vendor-specific TLV
  - Vpnid does not match any of the top level L2VPN TLV vpnid.

  Workaround: There is no workaround.

- CSCsz28000

  Symptoms: When modifying the group configuration for multicast QoS, the static-group session does not reevaluate when a multicast session requires to be populated.

  Conditions: This issue is seen while modifying the group configuration.

  Workaround: Unconfigure the **ip igmp static-group** command and re-apply.

- CSCsx93502

  Symptoms: When two or more cable interfaces are bundled together in the Layer3 interface and multicast traffic with Qos configured is sent on this interface, the multicast traffic rate on one of the cable interfaces is found to be lesser than the configured QoS rate limit.

  Conditions: This issue is seen when multicast QoS is configured and two or more cable interfaces are bundled together.

  Workaround: There is no workaround.

- CSCsz23477

  Symptoms: While displaying the multicast session entries using the **show interface multicast-session** command, one or more sessions could be disrupt due to igmp timer timeout or igmp leaves. This may lead to a CMTS crash while the **show interfaces multicast-session** command displays the corresponding session details.

  Conditions: This issue is seen while displaying the multicast session entries.

  Workaround: There is no workaround.

- CSCsz67716

  Symptoms: The "Gate Report State" counter in the output of the **show packetcable cms verbose** command does not increment for Packetcable Multimedia (PCMM) policy servers.

  Conditions: This issue is seen in PCMM policy servers.

  Workaround: There is no workaround.

- CSCsz67961

  Symptoms: The PacketCable Multimedia (PCMM) calls fail when Gate Set Ack/Err is not received.

  Conditions: This issue is seen in PCMM calls with smaller values used for the timer T1 (such as 1 second).

  Workaround: Use larger values for the PCMM timer T1 (at least 5 seconds).

- CSCsz15590

  Symptoms: When large traffic passes through the Gigabit Ethernet interface, takes a long time to load the bootimage(kboot).

  Conditions: This issue is seen when large traffic passes through the Gigabit Ethernet interface (>200kbps).

  Workaround: Directly load the image using ROMmon.

- CSCsz66321

  Symptoms: Static routes configured may be lost after reloading the Cisco uBR7225VXR router, even when the "ip route.." information is present in the running configuration.

  Conditions: This issue is seen only on the Cisco uBR7225 router.

  Workaround: Reconfigure the "ip route.." after reloading the Cisco uBR7225VXR router.

- CSCsu00342

  Symptoms: Multicast streams drop, after changing the "ip igmp query-interval". The following sample shows the output before and after the change:

  Before the change:

```
Router#show ip mroute
<<..skipped..>>
(, ), 01:09:04/00:02:52, flags: sTI
Incoming interface: TenGigabitEthernet1/1, RPF nbr 10.x.x.x, RPF-MFD
Outgoing interface list:
Vlan50, Forward/Sparse, 00:48:45/00:02:52, H <<====
```

  After the change:

```
Router#show ip mroute
<<..skipped..>>
(, ), 01:28:19/00:02:36, flags: sPT
Incoming interface: TenGigabitEthernet1/1, RPF nbr 10.x.x.x, RPF-MFD
Outgoing interface list: Null <<====
```

Conditions: This issue is was first seen in a Cisco 7600 chassis with Supervisor 720 engine running Cisco IOS Release 12.2(33)SRB.

Workaround: There is no workaround.

- CSCeh33888

  Symptoms: A Cisco uBR7246VXR router may reload with the last reset from watchdog reset.

  Conditions: This issue is seen on a router having a Cisco uBR7200-NPE-G1 processor board and is running Cisco IOS Release 12.3(9a)BC.

  Workaround: There is no workaround.

- CSCsw49188

  Symptoms: Cable metering fails and enters a “hung” state.

  Conditions: The issue occurs when the “ip tcp timestamp” option is configured globally.
  Workaround: Do not use the “ip tcp timestamp” option.

- CSCsz31811

  Symptoms: The CMTS causes a high CPU utilization on the IP Detail Record (IPDR) and Subscriber Account Management Interface Specification (SAMIS) collector by sending multiple records for a flow with the same creation time.

  Conditions: The service flow export and service flow deletion occur at the same time.

  Workaround: There is no workaround.

- CSCsw14622

  Symptoms: For deleted service flows associated with PCMM calls the last character in the Service Class Name field is dropped in the SAMIS records and in the SNMP MIB object “docsQosServiceFlowLogServiceClassName”.

  Conditions: This issue is seen when the dynamic service flows associated with PCMM calls are deleted. The last character is found missing from the service class name in the MIB object “docsQosServiceFlowLogServiceClassName” and SAMIS records.

- CSCsx20724

  Symptoms: When multicast traffic is run using the DOCSIS Set-top Gateway (DSG) and the **cable monitor** command is configured, the pool manager process causes a huge memory leak. When a **shutdown** command is issued on the cable interface, the Cisco uBR7246VXR router crashes.

  Conditions: The issue occurs because **service-policy output** command is configured on the FastEthernet interface which sends the DOCSIS packets out of the Cisco uBR7246VXR router using cable monitor.

  Workaround: Do not configure the **service-policy output** command on the FastEthernet interface if the interface is used by cable monitor.

Resolved Caveats—Cisco IOS Release 12.2(33)SCB3

- CSCsy79541

  Symptoms: The Cisco uBR7200 router hangs when enabling the **cable monitor** command.

  Conditions: This issue is seen when the **cable monitor** is configured on the CMTS for an unknown MAC address.

  Workaround: Use the **cable intercept** command on the Cisco uBR7200 router.

- CSCsw52539

  Symptoms: The cable metering collection enters the “write-error” state and does not recover.

  Conditions: This issue occurs when cable metering is configured with the default TCP parameters.

  Workaround: Enabling the **ip tcp path-mtu-discovery command** may help prevent occurrences of the issue. Running the **test cable metering abort** command clears the “hung” state and allows the next iteration of cable metering to occur.

- CSCsz63000

  Symptoms: The CMTS fails to send SAMIS data to the IPDR collector, though the TCP connection is up.The **show ipdr session** command reports unacknowledged data, and the **show process event** command of IPDR process reports the process is in “sleep”.

  Conditions: This issue occurs when IPDR and cable metering collectors are enabled.

  Workaround: Disable and re-enable IPDR.

- CSCsz22819

  Symptoms: When using a wideband-SIP, the total count for the SPA in slot 1/1/0 is a sum of both SPAs, rather than the sum of itself. This can be seen using the **show hw-module bay all counters rf-channel** command.

  Conditions: This issue is seen in the wideband-SIP when more than one SPAs are inserted in one SIP.

  Workaround: There is no workaround.

- CSCsy81766

  Symptoms: The Enhanced Interior Gateway Routing Protocol (EIGRP) reports bad checksum.

  Conditions: This issue is seen when EIGRP adjacency is configured over a Generic Routing Encapsulation (GRE) tunnel.

  Workaround: Disable PXF on the Cisco CMTS router.

- CSCsy22359

  Symptoms: Tracebacks are seen with the following error after reloading the CMTS, during the initialization of downstream parameters:

  ```
  *Mar 5 18:56:18.583 PST: %CR10K_CLNT-3-CR10K_CLNT_ASSERT_FAILED:
  Assert failed at line 185 from func cr10k_docsis_get_ses_info in file
  ../src-cmts/cr10k/client-docsis/cr10k_docsis.c for client 0
  ```

  Conditions: The value of “code mc_idx” can range from 0 to 119. However, a value of 120 was observed on a Cisco uBR7200 router, and the unblocked IPC insertion from the RP to line card failed by producing traces.

  Workaround: Use the reg_add function to send RP to the line card IPC.

- CSCsx79863

  Symptoms: The calculated channel utilization percent is inaccurate. The short term utilization seen via the output of the command s**how interface cable X/Y/Z mac-scheduler**, shows “Avg upstream channel utilization” value much larger than the actual channel usage. The longer term utilization used by the load-balancing module may also be much larger than the actual channel usage.

  Conditions: This issue is seen when “rate-adapt” is configured for a particular upstream channel, under certain configured conditions. The MAC scheduler for that upstream allocates additional data grants to one or more cable modems in a given MAP message. When the data grants go unused by cable modems, the scheduler makes skewed utilization calculations.

  Workaround: There is no workaround.

- CSCsz53800

  Symptoms: Multiple memory leaks are observed while issuing the **show memory debug leak** command on the line card.

  Conditions: The condition is unknown.

  Workaround: There is no workaround.

- CSCsx20894

  Symptoms: The Cisco uBR7246VXR router incorrectly reports “docsIfDocsisBaseCapability” of “4”, that is, the DOCSIS 3.0 support.

  Conditions: This issue occurs in Cisco uBR7246VXR routers running the Cisco IOS Release 12.2(33)SCB.

  Workaround: There is no workaround.

- CSCsx70840

  Symptoms: The modems end up in reject (m) state and the log contains the following error on a Cisco uBR7200 series router, after reloading it with Cisco IOS Release12.2(33)SCB,

```
*Dec 26 17:42:09.948: %UBR7200-4-REG_REJ_AUTH_FAIL_CMTS_MIC_INVALID:
<133>CMTS[DOCSIS]:<73000500>
Registration rejected authentication failure: CMTS MIC invalid
. CM Mac Addr <0019.5e38.96ca>
```

  Conditions: This issue is seen when the **cable shared-secret** command is configured on the interface.

  Workaround: One of the following workarounds may be used:

  1. Reconfigure the shared secret command, after bootup; the devices may go offline after an unexpected reload, but the security is maintained.
  2. Configure the **cable dynamic-secret** command if it is practical in the present network design, and remove the **cable shared-secret** command; This utilizes other code paths and maintains security.
  3. Remove the **cable shared-secret** command from the running configuration, write to memory, and then replace the **cable shared-secret** command; this creates a “resilient” fault though it less secure. The system recovers automatically and all modems go into the online(pt) state, but there theft of service may occur. The devices that come online after an unexpected reload are not as secure and slightly harder to manage.

- CSCsv16701

  Symptoms: Power supply is not displayed in the output of the **show inventory** command on the Cisco uBR7246VXR platform.

  Conditions: This issue occurs on Cisco uBR7246VXR routers.

  Workaround: Use the **show environment** command to see the power supply.

- CSCsx16152

  Symptoms: Erroneous routing prefixes may be added to the routing table.

  Conditions: This issue is seen when the DHCPv6 relay feature is enabled and a router receives a normal DHCPv6 relay reply packet, which leads to an erroneous route being added to the routing table.

  Workaround: There is no workaround.

- CSCsz12821

  Symptoms: The CMTS ignores IGMPv3 join message.

  Conditions: This issue occurs when IGMPv3 is configured on the bundle interface and SSM-mapping is configured on CMTS. The ignored IGMPv3 join is *,G join with group address in the SSM range.

  Workaround: Use either S,G IGMPv3 join or use *,G IGMPv2 join message.

- CSCsy48561

  Symptoms: After configuring a multicast group configuration (GC) and then assigning the GC to the cable interface, a **hw-module slot x stop** command triggers the CMTS to crash.

  Conditions: The issue is seen when the **hw-module slot x stop** command is executed.

- CSCsz21661

  Symptoms: The Gigabit Ethernet output for a 24 downstream wideband and narrowband SPA can get isolated from the port after repeated online insertion and removal (OIR) of the SPA within a short duration of time.

  Conditions: This issue is seen with repeated OIR of the SPA within a short duration of time and with repeated line protocol off/on within a short duration of time.

  Workaround: Reload the SPA using the **hw-module bay reload** command.

- CSCsz05250

  Symptoms: When setting a CA certificate to 'untrusted', any CM that uses an issuer of the same name is rejected, including legitimate modems.

  Conditions: This issue is caused due to a newly created software “Haxorware”, which generates CA certificates that conflict with existing CA certificates.

  Workaround: The recommended method is to disallow self-signed certificates on the CMTS and explicitly set specific self-signed certificates to “trusted”. This is the 'opt-in' model, rather than a 'opt-out' model.

- CSCsv64884

  Symptoms: The SNMP v3 walk with authentication does not complete against a virtual switch system (VSS).

  Conditions: This issue occurs on a SNMP v3 walk with authentication on a VSS.

- CSCsw14433

  Symptoms: On the Cisco CMTS router, during RP module runversion of the ISSU upgrade process, the IPC connection between RP and cable line cards may take additional seconds to come up.

  Conditions: This issue occurs during RP module runversion.

  Workaround: There is no workaround.

- CSCsx77978

  Symptoms: The downstream load is not balanced when the downstream load balancing group (DS LB) is configured with **us-across-ds** policy.

  Conditions: This issue is seen when **us-across-ds** policy is configured on the DS LB group.

  Workaround: Do not configure **us-across-ds** policy on the DS LB group.

- CSCsy28426

  Symptoms: When a wideband interface with w-online modems on it and a primary channels is shut down, an error is seen in the load-balancing modem counter when these modems go offline. This issue has an affect on the load balancing.

  Conditions: The issue occurs when a wideband interface with w-online modems and a primary channel is shut down.

  Workaround: Configure the primary channel of the modem to be excluded from the channels in wideband interface.

- CSCsw24542

  Symptoms: A crash occurs due to a bus error after displaying the following error messages:

  ```
  %DATACORRUPTION-1-DATAINCONSISTENCY: copy error,
  %ALIGN-1-FATAL: Illegal access to a low address < isdn function decoded>
  ```

  Conditions: This crash occurs on a Cisco 3825 router running Cisco IOS Release12.4(22)T with active ISDN connections. The Cisco 3825 router crashed while being monitored using an **SNMP Get** program and reloaded after some time.

  Workaround: There is no workaround.

- CSCsw35917

  Symptoms: The SNMP route processor (RP) agent does not send logged SP syslog messages as SNMP trap messages.

  Conditions: This issue occurs in routers running Cisco IOS Release 12.2(18)SXF.

  Workaround: There is no workaround.

- CSCsu64215

  Symptoms: The **ip tcp adjust-mss** command results in packet loss for non-TCP traffic.

  Conditions: This issue is seen when using the **ip tcp adjust-mss** command.

  Workaround: Disable the **ip tcp adjust-mss** command on all interfaces in the device. This may cause higher CPU utilization due to fragmentation and reassembly in certain tunnel environments where the command is intended to be used.

- CSCsu31549

  Symptoms: When a router (with a large-scaled configuration) is provisioned to perform an RP module failover, a PXF crash occurs (for example, switchover pxf restart 1 0), which results in missed IPC keepalives and a large crash information file is being written causing unexpected behavior, including line card reloads.

  Conditions: This issue is seen in a router with a large configuration that is configured with redundancy, mode switchover, main-cpu, and switchover pxf restart 1 0.

- CSCsy73726

  Symptoms: The cable metering options “flow-aggregate” and “cpe-list-suppress” disappear from the cable metering configuration if **cable metering data-per-session x timer y** command is configured.

  Conditions: This issue is seen in the **cable metering** command.

  Workaround: Reconfigure the metering options “flow-aggregate” and “cpe-list-suppress” in the command.

- CSCsv87997

  Symptoms: The DHCPv6 relay process crashes on the active RP.

Conditions: The condition is unknown.

Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 12.2(33)SCB2

- CSCeh33888

  Symptoms: A Cisco uBR7246VXR router may reload with the last reset from watchdog reset.

  Conditions: This issue occurs if the router has a Cisco uBR7200-NPE-G1 processor board and is running Cisco IOS Release 12.3(9a)BC.

  Workaround: There is no workaround.

- CSCsi43840

  Symptoms: The Cisco uBR7246VXR-MC28U line card resets with no crash file being generated in bootflash.

  Conditions: The issue may occur on some Cisco uBR7246VXR routers with multiple Cisco uBR-MC28U cards.

  Workaround: There is no workaround.

- CSCsu00342

  Symptoms: A drop in multicast streams is seen after changing the IGMP query interval, using the **ip igmp query-interval** command.

  Conditions: This issue occurs in the following conditions:

  – Cisco 7600 chassis with Sup720 engine is running Cisco IOS Release 12.2(33)SRB
  – Cisco 7600 is configured with IGMPV3 and is running Source Specific Multicast (SSM).
  – Multicast stream(s) restore themselves within 40-60 seconds.

  Workaround: There is no workaround.

- CSCsu18117

  Symptoms: The ToS values on multicast packets are incorrectly overwritten.

  Conditions: This issue occurs in routers using Cisco IOS Release 12.2(33)SCB.

  Workaround: There is no workaround.

- CSCsv16701

  Symptoms: Power supply is not displayed in the output of the **show inventory** command on the Cisco uBR7246 VXR platform.

  Conditions: This issue occurs on Cisco uBR7246VXR routers.

  Workaround: Use the **show environment** command to see the power supply.

- CSCsv82736

  Symptoms: The cable modem cannot come online on the upstream. This issue was first detected in Cisco IOS Release 12.3(21a)BC6. The modem reaches the init(r1) or init(r2) but, fails to proceed further.

  Conditions: This issue was seen at the customer site for Cisco IOS Release 12.3(21a)BC6. It is a rare condition.

  Workaround: Use the **shut/no shut** command.

- CSCsw14622

  Symptoms: The last character in the Service Class Name field is dropped in Subscriber Account Management Interface Specification (SAMIS) records as well as in the SNMP MIB docsQosServiceFlowLogServiceClassName.

  Conditions: This occurs for deleted service flows.

  Workaround: There is no workaround.

- CSCsw37209

  Symptoms: Source verification of IPv6 packets does not occur even when the c**able ipv6 source-verify** command is configured on the cable interface of the Cisco uBR7200 router.

  Conditions: This issue occurs when Cisco IOS Release12.2S is running on the Cisco uBR7200 router.

  Workaround: There is no workaround.

- CSCsw49188

  Symptoms: Cable metering fails and enters a “hung” state.

  Conditions: This occurs when the **ip tcp timestamp** command is configured globally on the Cisco uBR7200 router.

  Workaround: Do not use the **ip tcp timestamp** command in global configuration mode.

- CSCsw35917

  Symptoms: SP syslog messages are logged on the RP console but are not sent as SNMP trap messages by the route processor’s (RP) SNMP agent.

  Conditions: This issue occurs on routers running Cisco IOS Release 12.2(18)SXF.

  Workaround: There is no workaround.

- CSCsw52539

  Symptoms: Cable metering collection enters the “write-error” state and does not recover.

  Conditions: This issue occurs when cable metering is configured with the default TCP parameters.

  Workaround: Enabling the **ip tcp path-mtu-discovery command** may help prevent occurrences of the issue; Running the **test cable metering abort** command clears the “hung” state and allows the next iteration of cable metering to occur.

- CSCsw79768

  Symptoms: SNMP GetNext requests for docsQosServiceFlowPrimary (also known as 1.3.6.1.2.1.10.127.7.1.3.1.8 or docsQosServiceFlowEntry.8) are rejected. However, if a certain docsQosServiceFlowPrimary entry is polled with SNMP GetNext directly (after some additional calculations are performed to determine the index value), the value is returned as expected.

  Conditions: This issue occurs in Cisco uBR7114E routers running Cisco IOS Release 12.3(21a)BC3.

  Workaround: Poll the individual values following the steps of the procedure suggested in SR 610144513.

- CSCsx20894

  Symptoms: The Cisco uBR7246VXR router incorrectly reports docsIfDocsisBaseCapability of “4” that is, the DOCSIS 3.0 support.

  Conditions: This issue occurs in Cisco uBR7246VXR routers running the Cisco IOS release12.2(33)SCB.

Workaround: There is no workaround.

- CSCsx38826

  Symptoms: The DOCSIS 2.0-compliant cable modems are stuck in reject (NA) state on the cable modem termination system (CMTS) running Cisco IOS Release 12.2(33)SCB.

  Conditions: This issue is seen in modems that register using service class names instead of service flow definitions.

  Workaround: Do not use service class names during modem configuration; Check if the modem firmware ignores the unknown service flow Type Length Values (TLV), instead of rejecting it.

  Workaround: Use **shut/no shutdown** command.

Resolved Caveats—Cisco IOS Release12.2(33)SCB2

- CSCso90058

  Symptoms: The Multilayer Switch Feature Card (MSFC) crashes with RedZone memory corruption.

  Conditions: This issue occurs when an auto-RP packet is being processed and Network Address Translation (NAT) is enabled.

  Workaround: There is no workaround.

- CSCsv90106

  Symptoms: A router may write a crashinfo that lacks the normal command logs, crash traceback, crash context, or memory dumps.

  Conditions: This issue may be seen in a memory corruption crash depending on precisely how the memory was corrupted.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 12.2(33)SCB1

- CSCeh33888

  Symptoms: A Cisco uBR7246VXR router may reload with the last reset from watchdog reset.

  Conditions: The router has a Cisco uBR7200-NPE-G1 processor board and is running Cisco IOS release 12.3(9a)BC.

  Workaround: There is no workaround.

- CSCsi43840

  Symptoms: The Cisco uBR7246VXR-MC28U line card resets with no crash file being generated in bootflash.

  Conditions: The problem may occur on some Cisco uBR7246VXR router with multiple MC28U cards.

  Workaround: There is no workaround.

- CSCsu00342

  Symptoms: A drop in multicast streams is seen after changing the IGMP query interval, using the **ip igmp query-interval** command.

Conditions: This issue occurs in Cisco 7600 chassis with Sup720 engine running Cisco IOS release 12.2(33)SRB. The Cisco 7600 is configured with IGMPV3 and running Source Specific Multicast (SSM).The multicast stream(s) restore itself within 40-60 seconds.

Workaround: There is no workaround.

- CSCsu18117

  Symptoms: ToS value on multicast packets are being incorrectly overwritten.

  Conditions: This issue occurs in routers using Cisco IOS release 12.2(33)SCB.

  Workaround: There is no workaround.

- CSCsv16701

  Symptoms: Power supply is not displayed in the output of **show inventory** command on Cisco uBR7246 VXR platform.

  Conditions: This issue occurs on Cisco uBR7246VXR routers.

  Workaround: Use the **show environment** command to see the power supply.

- CSCsv82736

  Symptoms: Modem cannot come online on the upstream. This issue was first detected in Cisco IOS Release 12.3(21a)BC6. The modem reaches the init(r1) or init(r2) but, fails to proceed further.

  Conditions: The issue appeared at customer site in Cisco IOS release 12.3(21a)BC6. It is a a very rare condition.

  Workaround: Use **shut/no shutdown** command.

- CSCsw14622

  Symptoms: The last character in the Service Class Name field is dropped in Subscriber Account Management Interface Specification (SAMIS) records as well as in the SNMP MIB docsQosServiceFlowLogServiceClassName.

  Conditions: This occurs fro deleted service flows.

  Workaround: There is no workaround.

- CSCsw35917

  Symptoms: SP syslog messages are logged on the RP console but are not sent as SNMP trap messages by route processor's (RP) SNMP agent.

  Conditions: This issue occurs in routers running Cisco IOS release 12.2(18)SXF.

  Workaround: There is no workaround.

- CSCsw37209

  Symptoms: Source verification of IPV6 packets does not happen, although the **cable ipv6 source-verify** command is configured on cable interface of a Cisco uBR7200 router.

  Conditions: This issue occurs when Cisco IOS 12.2S release is running on a Cisco uBR7200 router.

  Workaround: There is no workaround.

- CSCsw49188

  Symptoms: Cable metering fails and enters a "hung" state.

  Conditions: This occurs when the **ip tcp timestamp** command is configured globally.

  Workaround: Do not use the **ip tcp timestamp** command.

- CSCsw52539

  Symptoms: Cable metering collection enters the “write-error” state and does not recover.

  Conditions: This issue occurs when cable metering is configured with default TCP parameters.

  Workaround: Enabling the **ip tcp path-mtu-discovery command** may help prevent occurrences of the issue; Running the **test cable metering abort** command clears the “hung” state and allows the next iteration of cable metering to occur.

- CSCsw79768

  Symptoms: SNMP GetNext requests for docsQosServiceFlowPrimary (also known as 1.3.6.1.2.1.10.127.7.1.3.1.8 or docsQosServiceFlowEntry.8) are rejected. And, if a certain docsQosServiceFlowPrimary entry is polled with SNMP Get directly (after some additional calculations are performed to determine the index value), the value is returned as expected.

  Conditions: This issue occurs in Cisco uBR7114E routers running Cisco IOS release 12.3(21a)BC3.

  Workaround: Poll the individual values following the steps of the procedure suggested in SR 610144513.

- CSCsx20894

  Symptoms: Cisco uBR7246VXR router incorrectly reports docsIfDocsisBaseCapability of “4”,that is the DOCSIS 3.0 support.

  Conditions: This issue occurs in Cisco uBR7246VXR routers running the Cisco IOS release12.2(33)SCB.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(33)SCB1

- CSCsv04836

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

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

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

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090908-tcp24.

- CSCsv38166

  The server side of the Secure Copy (SCP) implementation in Cisco IOS software contains a vulnerability that could allow authenticated users with an attached command-line interface (CLI) view to transfer files to and from a Cisco IOS device that is configured to be an SCP server, regardless of what users are authorized to do, per the CLI view configuration. This vulnerability

could allow valid users to retrieve or write to any file on the device's file system, including the device's saved configuration and Cisco IOS image files, even if the CLI view attached to the user does not allow it. This configuration file may include passwords or other sensitive information.

The Cisco IOS SCP server is an optional service that is disabled by default. CLI views are a fundamental component of the Cisco IOS Role-Based CLI Access feature, which is also disabled by default. Devices that are not specifically configured to enable the Cisco IOS SCP server, or that are configured to use it but do not use role-based CLI access, are not affected by this vulnerability.

This vulnerability does not apply to the Cisco IOS SCP client feature.

Cisco has released free software updates that address this vulnerability.

Workaround: There are no workarounds available for this vulnerability apart from disabling either the SCP server or the CLI view feature if these services are not required by administrators.

This advisory is posted at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-scp.

- CSCsr29468

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

  Cisco has released free software updates that address this vulnerability.

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

  This advisory is posted at
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-tcp

- CSCsj19540

  Symptoms: Ping request to a /31 loopback interface in VRF fails.

  Conditions: This issue occurs when the loopback has a /31 address configured in a VRF.

  Workaround: There is no workaround.

- CSCso55151

  Symptoms: A memory leak is observed on the router for ARP packets.

  Conditions: This issue occurs on routers with CEF switching.

  Workaround: There is no workaround.

- CSCsr72301

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

  Conditions: The Cisco Security Response is posted at the following link:
  http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20090114-http

  See “Additional Information” section in the posted response for further details.

  Workaround: See “Workaround” section in the posted response for further details.

- CSCsv11927

  Symptoms: The Cisco uBR7200 router might hang when an unknown MAC address is used while running the **cable monitor** command.

  Conditions: This occurs when an unknown MAC address (not present in the CMTS database) is used while executing the cable monitor command.

Workaround: Use a known MAC address.

- CSCsv42988

  Symptoms: When the routers are booted sequentially, by bringing up the standby router after the active router is booted up, the routers fall into route processor redundancy (RPR) mode instead of stateful switchover (SSO) mode.

  Conditions: This issue occurs in network analysis module (NAM) running Cisco IOS SRC2 image.

  Workaround: There is no workaround.

- CSCsv58913

  Symptoms: Address resolution fails for downstream packet when running **cable source-verify dhcp command.**

  Conditions: This issue occurs when a Cisco uBR Series router configured to verify a CPE device's IP address to MAC address resolution, through the use of DHCP LEASEQUERY messages instead of using ARP.

  Workaround: Temporarily allow downstream ARP resolution using cable bundle interface commands **cable arp** and **cable proxy-arp.**

- CSCsv73509

  Symptoms: User authentication is possible through a local server, although Terminal Access Controller Access Control System (TACACS) is configured.

  Conditions: This issue occurs for the exec users under vty configuration.

  Workaround: There is no workaround.

- CSCsw48328

  Symptoms: Service type ID-based cable modem redirection may not work.

  Conditions: This issue occurs in routers running Cisco IOS release 12.2(33)SCB1.

  Workaround: There is no workaround.

- CSCsx38826

  Symptoms: DOCSIS 2.0-compliant cable modems are stuck in reject(na) state on a CMTS running Cisco IOS release 12.2(33)SCB.

  Conditions: This issue is seen in modems that register using service class names instead of service flow definitions.

  Workaround: Do not use service class names during modem configuration or else check if the modem firmware ignores the unknown service flow Type Length Values (TLV), instead of being rejected.

- CSCsx43002

  Symptoms: The output of **show tech-support** command contains snmp community string passwords.

  Conditions: This issue occurs in the output of the **show tech-support** command.

  Workaround: These passwords must be removed. Replace the show tech-support snmp community string **show cable modem remote-query 30 mypassword** and with **show cable modem remote-query 30**.

- CSCsx51619

  Symptoms: The MAC destination address based classifier acts like a default catch-all classifier on the Cisco uBR 7200 router. This issue occurs when this classifier is checked (after the ones with higher rule priority), thus causing it to match all the packets.

  Conditions: This problem exists since Cisco IOS Release 12.3(23)BC6 release on uBR7225 router and uBR7100 platforms.

  Workaround: There is no workaround except avoiding using the MAC classifier on Cisco uBR7200 router.

  If a MAC destination address based classifier is configured, the classifiers with lower rule priority and the default classifier will not see any matches.

- CSCsy13636

  Symptoms: A silent reload occurred on the Cisco uBR-MC28X line card and no crash information was written on the boot flash.

  Conditions: This issue occurred on the Cisco uBR-MC28X line card.

  Workaround: Remove the load balancing configuration on the affected line card.

Open Caveats —Cisco IOS Release 12.2(33)SCB

- CSCsv82736

  Symptoms: Modem cannot come online on the upstream. This issue was first detected in Cisco IOS Release 12.3(21a)BC6. The modem reaches the init(r1) or init(r2) but, fails to proceed further.

  Conditions: The issue appeared at customer site in Cisco IOS release 12.3(21a)BC6. It is a a very rare condition.

  Workaround: Use **shut/no shutdown** command.

- CSCsv11927

  Symptoms: When using the **cable monitor** command and inserting as an argument an unknown MAC address (not in CMTS database) the ubr7200 might hang.

  Conditions: Using the **cable monitor** command with a mac address not known in the CMTS database.

  Workaround: Use the correct mac address.

- CSCeh33888

  Symptoms: A Cisco uBR7246VXR may reload with Last reset from watchdog reset.

  Conditions: The router has a UBR7200-NPE-G1 processor board and is running IOS version 12.3(9a)BC.

  Workaround: None.

- CSCsi43840

  Symptoms: The Cisco uBR7246vxr-MC28U Card resets with no crash file being generated in bootflash.

  Conditions: The problem may happen on some Cisco uBR7246vxr with multiple MC28U cards.

  Workaround: There is no workaround.