Release Notes for Cisco TelePresence System Software Release 1.10

Created: October 4, 2012
Revised: April 10, 2017

Contents

These release notes describe new features and open and closed hardware and software caveats for the Cisco TelePresence System software 1.10 releases.

Note A copy of source code used in this product that is licensed under the General Public License Version 2.0 can be obtained by e-mailing a request to cts-gpl@cisco.com.

Cisco Systems, Inc.
www.cisco.com

What’s New

The following sections contain new features in the CTS 1.10 releases:

New in Release 1.10.16

CTS software release 1.10.16 resolves various OpenSSL vulnerabilities reported by the Cisco Defects & Enhancements Tracking System (CDETS) number CSCvd06162. The TLS protocol version1.2 is enabled in this release. By default, the TLS secure communication starts with TLSv1.2 and is downscaled to TLSv1.1 and then to TLSv1.0 based on the remote endpoint or node’s supported TLS protocol version. For more information, see the “Caveats in Cisco TelePresence System Software Release 1.10.16” section on page 21.

To avoid backward compatibility issues, the TelePresence administration software must be upgraded to the following releases:

- IX 8.2.1
- TX 6.1.13
- CTS 1.10.16

Cisco has performed regression testing to test the OpenSSL vulnerability for TelePresence calls to and from endpoints running the different software versions. Table 1 shows the software versions in which the calls between selected endpoints were verified as secure with the updated releases.

Table 1 TelePresence Software Support for Secure Calls with OpenSSL Fixes

TelePresence Software Release	**IX 8.2.1**	**IX 8.2.0**	**TX 6.1.13**	**CTS 1.10.16**
Releases updated for these OpenSSL fixes:				
IX 8.2.1	Secure	Secure	Secure	Secure
TX 6.1.13	Secure	Secure	Secure	Secure
CTS 1.10.16	Secure	Secure	Secure	Secure
Releases without these OpenSSL fixes:				
IX 8.2.0	Secure	Secure	Secure	Secure
TX6.1.12	Secure	Secure	Secure	Secure
CTS 1.10.15	Secure	Secure	Secure	Secure
CTS 1.9.11	Non-Secure	Non-Secure	Secure	Secure

New in Release 1.10.15

CTS software release 1.10.15 resolves two separate OpenSSL and NTP vulnerabilities when placing calls from the CTS to other immersive TelePresence systems. These vulnerabilities are being tracked by the Cisco Defects & Enhancements Tracking System (CDETS) numbers CSCuy54628 and CSCuz44368. For more information, see the "Caveats in Cisco TelePresence System Software Release 1.10.15" section on page 22.

These vulnerabilities affect TelePresence administration software for CTS 1.10, and TX 6.*x*. The TelePresence administration software must be upgraded to the following releases to address these vulnerabilities:

- IX 8.1.2
- TX 6.1.12
- CTS 1.10.15
- CTS 1.9.11

Note These vulnerabilities are not present in IX Release 8.1.*x* or CTS 1.9.*x*. However, the IX system or CTS 1.9 system must be upgraded for compatibility with the updated TX and CTS 1.10 releases.

Cisco has performed regression testing to test the OpenSSL vulnerability for TelePresence calls to and from endpoints running the different software versions. Table 2 shows the software versions in which the calls between selected endpoints were verified as secure with the updated releases.

Table 2 TelePresence Software Support for Secure Calls with OpenSSL Fixes

TelePresence Software Release	**IX 8.1.2**	**TX 6.1.2**	**CTS 1.10.15**	**CTS 1.9.11**
Releases updated for OpenSSL fixes:				
IX 8.1.2	Secure	Secure	Secure	Always Non-secure
TX 6.1.12	Secure	Secure	Secure	Secure
CTS 1.10.15	Secure	Secure	Secure	Secure
CTS 1.9.11	Always Non-Secure	Secure	Secure	Secure
Releases without OpenSSL fixes:				
IX 8.1.1 and earlier	Possibly Non-Secure	Possibly Non-Secure	Possibly Non-Secure	Non-secure
TX 6.1.11.1 and earlier	Possibly Non-secure	Possibly Non-secure	Possibly Non-secure	Secure[1]
CTS 1.10.14.1 and earlier	Possibly Non-secure	Possibly Non-secure	Possibly Non-secure	Secure[1]
CTS 1.9.10 and earlier	Always Non-secure	Possibly Non-secure	Possibly Non-secure	Secure[1]

[1] May be vulnerable to the LogJam issue for TLS.

Note Beginning with CTS 1.10.11, secure calls using Cisco TelePresence Multipoint Switch (CTMS) are not supported.

New in Release 1.10.14.1

This release resolves system issues and enhances the user experience. There are no new features associated with this release.

See the “Caveats in Cisco TelePresence System Software Release 1.10.14.1” section on page 25 for a complete list of caveats.

New in Release 1.10.14

This release resolves system issues and enhances the user experience. There are no new features associated with this release.

See the “Caveats in Cisco TelePresence System Software Release 1.10.14” section on page 27 for a complete list of caveats.

New in Release 1.10.13

This release resolves system issues and enhances the user experience. There are no new features associated with this release.

See the “Caveats in Cisco TelePresence System Software Release 1.10.13” section on page 28 for a complete list of caveats.

New in Release 1.10.12

This release resolves system issues and enhances the user experience. There are no new features associated with this release.

See the “Caveats in Cisco TelePresence System Software Release 1.10.12” section on page 30 for a complete list of caveats.

New in Release 1.10.11.2

This release enhances video quality in a point-to-point or Cisco TelePresence Multipoint Switch (CTMS) call by fixing issues related to buffer overflow. This condition is tracked by CDETS CSCuu49617.

See the “Caveats in Cisco TelePresence System Software Release 1.10.11.2” section on page 31 for a complete list of caveats.

New in Release 1.10.11.1

This release fixes a problem with sending DTMF tones in a WebEx meeting. This condition is tracked using CDETS CSCuu25109.

See the “Caveats in Cisco TelePresence System Software Release 1.10.11.1” section on page 32 for a complete list of caveats.

New in Release 1.10.11

This release resolves system issues and enhances the user experience. There are no new features associated with this release.

See the “Caveats in Cisco TelePresence System Software Release 1.10.11” section on page 32 for a complete list of caveats.

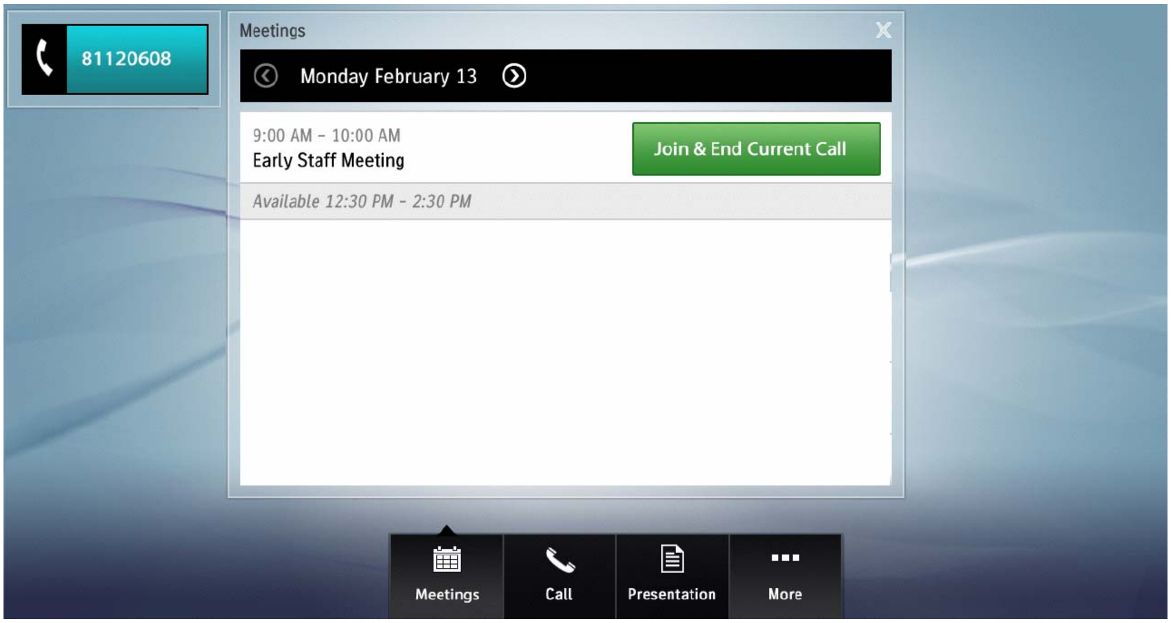
New in Release 1.10.10

New Behavior for Touch 12 Device When Joining Meetings

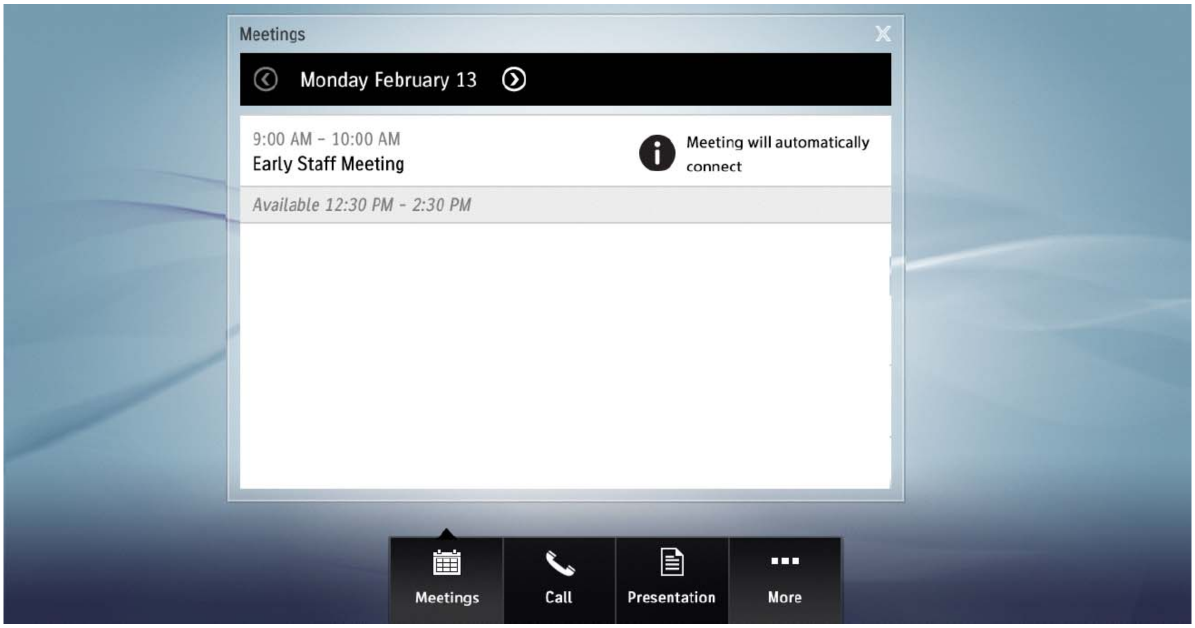
If your network uses Cisco TelePresence Manager (CTS-Manager) for meeting scheduling, some meeting screens have changed.

Note You will not see these screens if your network uses the Cisco TelePresence Management Suite (TMS) for meeting scheduling.

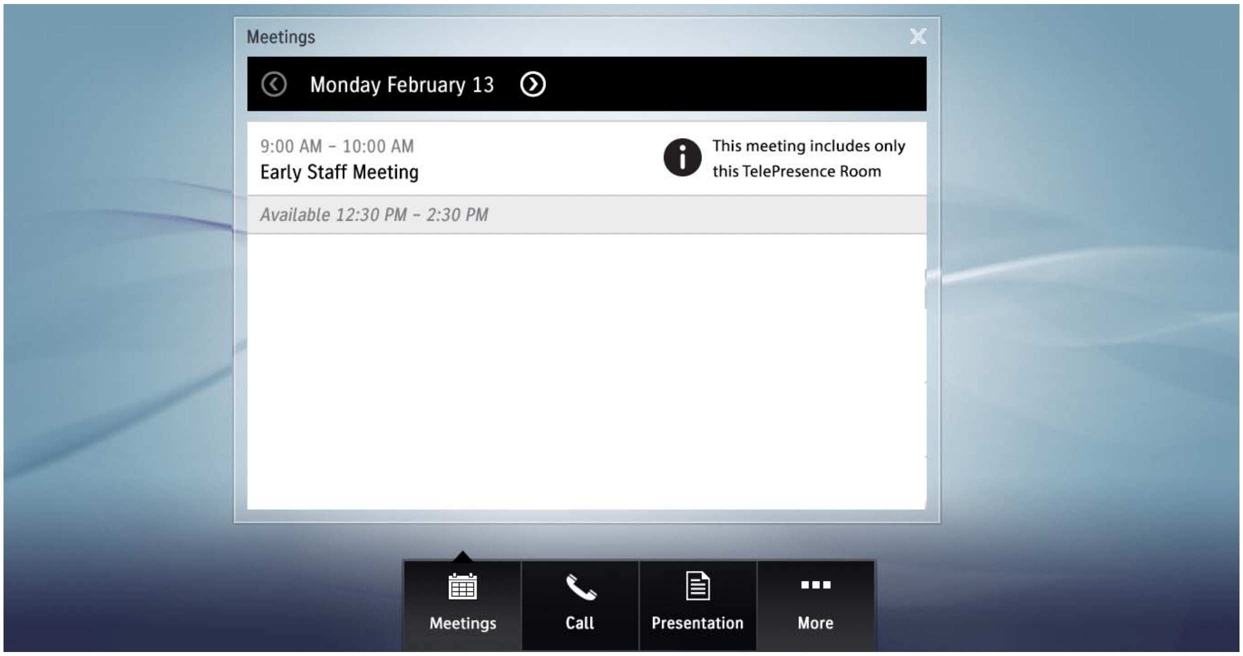
- If you are in a call, and wish to join a scheduled conference, the choice to Join has been replaced with **Join & End Current Call**.



- In an AutoConnect meeting, the choice to join the meeting is disabled, and is replaced by text saying that the meeting will automatically connect.



- If a meeting includes only one TelePresence room, and no WebEx OneTouch (also known as one-button-to-push) number has been defined, the text in the meeting informs you that the meeting only includes the TelePresence room.



Meetings

Monday February 13

9:00 AM - 10:00 AM
Early Staff Meeting

This meeting includes only this TelePresence Room

Available 12:30 PM - 2:30 PM

In addition, this release addresses the Ghost vulnerability in the GNU C library. For more information, see CSCus85759.

New in Release 1.10.9

This release resolves issues and enhances the user experience, and provides security fixes for security issues related to CVE-2013-6438 (Apache HTTP server) and CVE-2013-6420 (OpenSSL).

See the "Caveats in Cisco TelePresence System Software Release 1.10.9" section on page 35 for a complete list of caveats.

New in Release 1.10.8.1

This release fixes the GNU Bash Environment Variable Command Injection Vulnerability (Shellshock). This vulnerability is being tracked by the Cisco Defects & Enhancements Tracking System (CDETS) number CSCur05163.

New in Release 1.10.8

This release resolves system issues and enhances the user experience. There are no new features associated with this release.

See the "Caveats in Cisco TelePresence System Software Release 1.10.8" section on page 36 for a complete list of caveats.

New in Release 1.10.7

This release fixes various OpenSSL issues and upgrades the version of the Apache HTTP server. For additional information, see the “Caveats in Cisco TelePresence System Software Release 1.10.7” section on page 39.

New in Release 1.10.6

This release resolves system issues and enhances the user experience. There are no new features associated with this release.

See the “Caveats in Cisco TelePresence System Software Release 1.10.6” section on page 40 for a complete list of caveats.

New in Release 1.10.5.1

This release fixes the OpenSSL Heartbleed Vulnerability. This vulnerability is being tracked by the Cisco Defects & Enhancements Tracking System (CDETS) number CSCuo20210.

In addition, an enhancement (CSCuo30624) has been added to allow a Locally Significant Certificate (LSC) to be installed and used by the Key Exchange process to establish Datagram Transport Layer Security (DTLS) sessions between endpoints. See the “Caveats in Cisco TelePresence System Software Release 1.10.5.1” section on page 42 for more information.

New in Release 1.10.5

This release resolves system issues and enhances the user experience. There are no new features associated with this release.

See the “Caveats in Cisco TelePresence System Software Release 1.10.5” section on page 43 for a complete list of caveats.

New in Release 1.10.4

This release resolves system issues and enhances the user experience. There are no new features associated with this release.

See the “Caveats in Cisco TelePresence System Software Release 1.10.4” section on page 44 for a complete list of caveats.

Caveat for Microsoft Lync 2013

Because systems running CTS software can decode a maximum of 30 frames per second (fps), and Lync clients intermittently exceed transmission rates of 30 fps, video conferences with a Lync client can have unacceptable quality. For better video quality, use a Cisco TelePresence server between the Lync client and Cisco TelePresence system.

New in Release 1.10.3

This release resolves system issues and enhances the user experience. There are no new features associated with this release.

See the “Caveats in Cisco TelePresence System Software Release 1.10.3” section on page 47 for a complete list of caveats.

New in Release 1.10.2

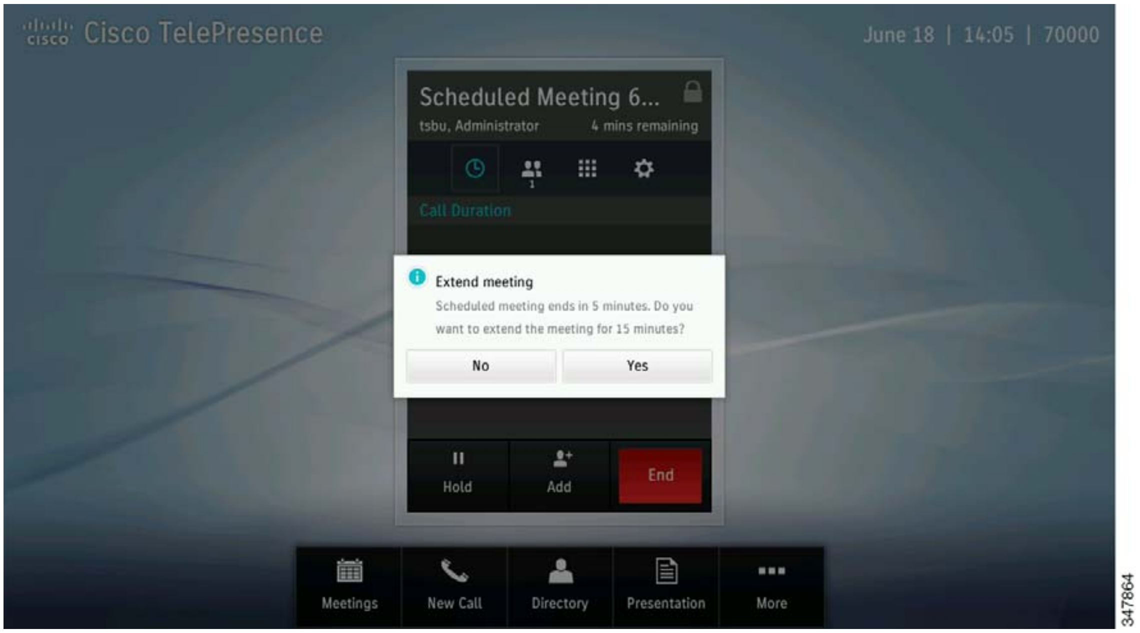
The following feature is new in this release:

TelePresence Management Suite (TMS) Integration

Note This feature requires TMS version 14.3 or later and requires the use of a Touch 12 device as your call control device. Systems that use a Cisco Unified IP Phone for call control cannot use this feature.

This software release enhances the use of TMS as a call scheduling and management platform. If your system uses TMS, some new messages appear on your Touch 12 device. For example, if you are the video conference master (VC master) of your meeting, a prompt appears a few minutes before your meeting ends that gives you the option to extend your meeting. See Figure 1 for an example of this prompt.

Figure 1 *TMS Meeting Extension Prompt to Administrator*

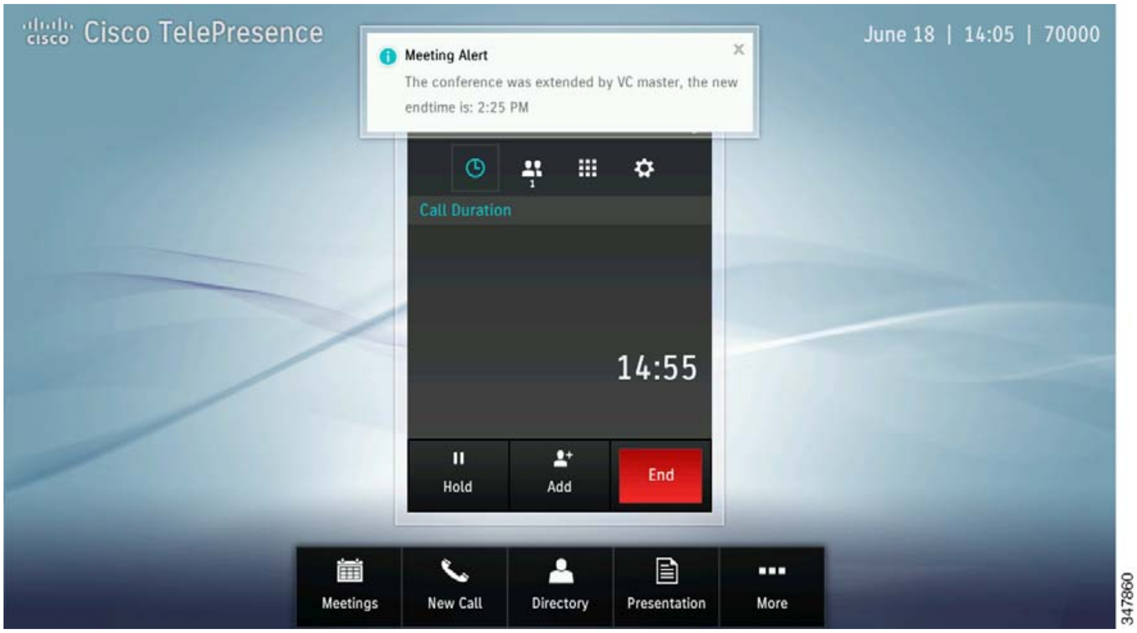


Extend meeting

Scheduled meeting ends in 5 minutes. Do you want to extend the meeting for 15 minutes?

If you tap **Yes**, your meeting length extends, and all call participants see an alert like the one shown in Figure 2.

Figure 2 TMS Meeting Extended Alert



Meeting Alert

The conference was extended by VC master, the new endtime is: 2:25 PM

For more information about the TMS messages that appear on the Touch 12, refer to the System Alerts and Meeting Messages chapter of the *Cisco TelePresence System User Guide, Software Release TX 6.0*. For more information about TMS, refer to the Cisco TMS support documentation.

See the “Caveats in Cisco TelePresence System Software Release 1.10.2” section on page 51 for a complete list of caveats.

New in Release 1.10.1

This release resolves system issues and enhances the user experience; there are no new features.

See the “Caveats in Cisco TelePresence System Software Release 1.10.1” section on page 54 for a complete list of caveats.

New in Release 1.10.0

The following features are new in this release:

- 802.1X Authentication, page 11
- Dialing a URI String, page 11
- Language Versions, page 11
- Screen Dimming, page 11
- TIP Support, page 11

See the “Caveats in Cisco TelePresence System Software Release 1.10.2” section on page 51 for a complete list of caveats.

802.1X Authentication

This software release supports the use of 802.1X authentication for port-based access control. For more information and instructions about configuring this feature, refer to the "802.1X Authentication" section of the *Administration Guide for Cisco TelePresence Software Release 1.10*.

Dialing a URI String

This software release supports using a URI string (for example, user@cisco.com) to place a call. For more information, refer to the "Dialing a URI String" section of the *Cisco TelePresence System User Guide*.

Note The URI Dialing feature for CTS 1.10 endpoints is supported in Cisco Unified CM 9.0 or later.

Language Versions

This software release supports additional languages. These languages change the text that is shown on the Cisco TelePresence Touch 12 device and also affect some on-screen messages. For more information, refer to the "Installing Language Versions" section of the *Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System*.

Note This feature only works with systems that use the Touch 12 device for call control.

Screen Dimming

To save power and extend the life span of the Cisco TelePresence Touch 12 device, the Touch 12 dims during non-business hours, as defined in Unified CM. When dimming is active, the screen is dimmed and the home button is glowing. The system becomes active when the screen or a hard button is touched, and stays on until the system has been idle for one hour.

Note This feature only applies to systems that use the Touch 12 device for call control.

For more information, refer to the "Screen Dimming" section of the *Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System*.

TIP Support

Cisco TelePresence endpoints are designed to work with any device that implements the TelePresence Interoperability Protocol (TIP) and adheres to the interoperability requirements described in Cisco's published TIP Implementation Profiles.

Starting with CTS 1.10, TIP version 8 is supported. TIP version 8 includes support for the following features:

- Video resolution of 640×360 (360p)
- BFCP as an option for presentation sharing

Cisco tests interoperability with TIP devices based on market priority. The Cisco Technical Assistance Center (TAC) accepts calls related to interoperability with third-party endpoints and devices to troubleshoot and identify the root cause of issues. These calls must come from customers with a valid support agreement.

Important Notes for 1.10.x Releases

- **CTS 1.10.x Requires Touch 12**

Cisco TelePresence immersive systems running 1.10.x releases require the Touch 12 device for call control.

Note Using a Cisco IP Phone for call control is supported only in the initial 1.10.0 release.

- **Sharing Video with Motion at 5 fps**

Some legacy Cisco TelePresence immersive systems run video at a maximum of 5 frames per second (fps). In addition, some network conditions can cause your endpoint to downgrade to frame rates as low as 5 fps.

While 5 fps works well for static images such as presentations, videos with motion in them might not be smooth, and could have a jerky appearance. The illusion of motion in recorded or live media begins at 15 to 20 fps. While broadcasting video with 5 fps is acceptable, users can expect to see less realistic motion.

Any network problems (such as jitter or lost packets) can cause additional video problems for presentation content. For example, the presentation can be blurry, or have pixelation, or motion video can jerky.

Note that Long-Term Reference Picture (LTRP) frames are not used for presentation video.

- **Blurred Motion for Moving Objects (Motion Handling)**

Motion handling defines the degree of compression within the encoding algorithm to either enhance or suppress the clarity of the video when motion occurs within the image. High motion handling results in a smooth, clear image even when a lot of motion occurs within the video (people waving their hands, for example). Low motion handling results in a noticeable choppy, blurry, grainy, or pixelized image when people or objects move.

Cisco TelePresence provides you with a way to customize the motion handling. Although the Cisco TelePresence cameras can operate at a resolution of up to 1080p with a maximum frame rate of 60 frames per second (1080p 60), the codec can encode and compress the video into either 1080p or 720p resolutions at three different motion-handling levels per resolution providing you with the flexibility of deciding how much bandwidth is available in your network.

Instead of a sliding scale, Cisco uses the terms Good, Better, and Best. Best motion handling provides the clearest image and uses the most bandwidth. Good motion provides the least-clear image and uses the least bandwidth. For more information, refer to the “Understanding How Endpoints Determine fps and Video Quality” section of the “TX Software Features” chapter of the Administration Guide for Cisco TelePresence Software Release TX 6.

Low motion handling (for example, a hand wave leaving streaks or tracks for a few seconds on the screen) has also been seen under the following circumstances:

  – Under certain lighting conditions (for example, the light from an upper fixture leaving a shadow on a participant). Some lighting conditions cause low motion handling when the codec applies auto-correction to the broadcast image.

  - Using certain wall colors (tan or light brown)
  - Networks with high latency; any latency in your networks can lower the motion handling
  - Networks with a lot of jitter or dropped packets

- **Choppy or Distorted Music or Other Continuous Sound when Sharing Presentation Audio**

Immersive Cisco TelePresence systems use an Acoustic Echo Canceler (AEC) to make human speech sound as clear as possible for the best possible collaboration experience.

Any sound that is continuously played (such as music) as the audio portion of a presentation can sound choppy or distorted during a Cisco TelePresence conference. To remove echo, AEC changes the loudness of the audio coming from the system loudspeaker when it detects sound locally (on the near end). When the loudspeakers are playing presentation audio, this change in loudness may lead to noticeable choppiness or distortion.

Muting the system microphones on both the near and far end can reduce the AEC effects when you share presentation audio; however, any endpoint that is not muted will still experience the same choppiness and distortion.

- **System Behavior During Times of Network Congestion**

Anything that degrades network performance can affect the function of your Cisco TelePresence system. This sources of the network degradation can include, but are not limited to, the following:

  - Administrative tasks such as an internal port scan or security scan
  - Attacks that occur on your network, such as a denial-of-service attack

These network disturbances can affect the voice and/or video quality of a Cisco TelePresence conference, and in some cases, can cause the call to drop. To reduce or eliminate any adverse effects to a TelePresence conference, schedule any administrative network tasks during a time when the Cisco TelePresence system is not being used, or exclude TelePresence systems from the testing.

- **BFCP Backward Compatibility**

BFCP is a protocol for controlling access to the presentation resources in a conference. BFCP is not supported in CTS software releases prior to CTS Release 1.8. BFCP is enabled by default on all CTS endpoints beginning with CTS Release 1.8. Endpoints using CTS software prior to CTS Release 1.8 must either disable BFCP on all new SIP profiles in the Unified CM Administration interface or upgrade all CTS endpoints to CTS Release 1.8 or a later release.

- **Command-Line Interface (CLI) Restrictions**

Avoid using the following commands to collect call status logs while in an active call:

- file tail
- ipsla
- tcpdump

Using these commands during an active CTS call can cause high CPU usage and may bring calls down.

- **Detect and Disconnect Audio Addin Calls**

Occasionally an audio addin call remains listed on the meeting participant Conference List even though the call has dropped. Due to the call preservation feature, the CTS waits for the Unified CM to send a BYE message before dropping an audio addin call. The CTS can enact several mechanisms to detect when the audio addin has dropped, including dropping the call when the phone has been rebooted.

The CTS cannot support two audio addin calls at the same time.

- **Endpoints That Cannot Share or Receive Presentations**

Some telepresence endpoints do not support the ability to share or receive presentations. If you encounter an endpoint that does not support presentations, the CTS displays the following notification on the main screen:

“Remote participant cannot receive presentation”

- **Systems Cannot be Connected to a Router**

Be sure that you connect your TelePresence system to a switch; this device cannot be directly connected to a router.

- **Headset Support**

Headsets are supported on the CTS 500 Series only.

- **MIDlets Not Supported in Most 1.10.x Releases**

MIDlets are supported in CTS 1.10.0 only. They are not supported or tested in subsequent CTS 1.10.x releases.

- **MIDlet File Naming for 1.10.x Releases**

For systems that use the Cisco Unified IP Phone, the MIDlet file names for this release are as follows:

  - TSPM-1.10.0-P1-1S.jad
  - TSPM-1.10.0-P1-1S.jar

Use these exact file names when creating an IP Phone Service. The MIDlet files are included in the COP file that you download from cisco.com.

- **MXP Support on the Cisco TelePresence System**

For information about MXP support for Cisco TelePresence, refer to the document *Cisco TelePresence System Software Version Compatibility - 1.10 Releases*.

- **SCCP and SIP Phone Firmware Upgrades**

For all SCCP and SIP firmware upgrades from firmware release versions earlier than 8.3(3) to version 8.5(3) or a later release, you must first upgrade your firmware to version 8.5(2). Once you have upgraded to version 8.5(2), you can upgrade your Cisco Unified IP Phone to version 8.5(3) or a later release.

See the Installation Notes section of the *Cisco Unified IP Phone Release Notes for Firmware Release 8.5(3) (SCCP and SIP)* for download instructions.

- **SDP and SRTP with CTS Release 1.10.0**

Customers who are deploying their B2B infrastructure with secure trunks to ASR/SBC secured by using TLS/Encryption, may experience call drops unless specific scripts are installed and configured on the ASR/SBC devices. Once the scripts and configuration are in place, certain SDP attributes are manipulated to enable SBC to unblock the SIP messages to and from Unified CM.

The following is an overview of the configuration steps:

1. Upload attached srtp.lua script to your ASR1k.
2. Define two SDP editors, for example to_rtp_avp and to_rtp_savp.
3. Configure a script set, as shown in the following example:

```
script-set 2 lua
    script srtp
      filename bootflash:srtp.lua
      load-order 100
      type full
    complete
   active-script-set 2
```

4. Use the SDP editor on both the inbound and outbound adjacencies:
   - Ask SBC to modify the SDP calling to_rtp_avp before-receive
   - And calling to_rtp_savp after-send

```
editor-type editor
    editor-list before-receive
     editor 1 to_rtp_avp
    editor-list after-send
     editor 1 to_rtp_savp
```

5. Create three editor headers:
   a. tp-to-x-supported
   b. tp-to-supported
   c. tp-add-x-srtp-fb

The first two are used in the inbound side, which will detect if any X-cisco-srtp-fallback tag gets into the supported header and then adds an srtp-fb header that includes the X-cisco-srtp-fallback tag (if present). The third one changes the internal srtp-fb header to the supported header prior to sending on the wire. The following is an example configuration:

```
adjacency sip peer2
    header-editor inbound tp-to-supported
    editor-list before-receive
     editor 1 to_rtp_avp
     editor 2 tp-to-x-supported
 adjacency sip peer1
    header-editor outbound tp-add-x-srtp-fb
```

See the following documents for support:

- Cisco ASR 1000 Series Aggregation Services Routers home page
- Business-to-Business Telepresence Configuration Profile Example

- **Setting the Device Type**

Whenever possible register your device to the Unified CM to configure the correct device type before calibrating the camera. To perform camera calibration if your system is not registered to the Unified CM, use the **set ctstype** command.

- **TIP Endpoint Audio-Only Attendee not Displayed on IP Phone**

When a CTS 3210, CTS 3200, CTS 3010, CTS 3000, CTS 1300-65, CTS 1100, CTS 1000, or CTS 500-37 is in a video call with a TIP endpoint, and an additional TIP endpoint is added to the call as a WebEx audio-only call, the audio-only TIP endpoint is not displayed in the list of users on the CTS IP Phone.

- **Touch 12 Directory Button**

After system software is upgraded and the endpoint reboots, the Touch 12 device Directory button does not show the Directory tab, only the Favorites tab. Wait 10 to 25 minutes for the Directory tab to appear.

- **TMS Messaging Settings (1.10.2 and above)**

If your system is integrated with TMS, see the following notes:

- Some TMS features (such as the setup buffer or meeting extension alert) are disabled by default. These features must be enabled on the TMS administrative interface before they will work with the Cisco TelePresence system. After you configure the features in the TMS administrative interface, TMS updates automatically according to the interval specified in the field **System Force Refresh Interval (in hours)**. Alternately, you can apply your settings immediately by navigating to **Administrative Tools** > **Configuration** > **Network Settings** and scrolling down to the **TMS Services** area. In the field **Enforce Management Settings on Systems**, click **Enforce Now**. If this field is set to Yes, TMS updates your system automatically when you configure features. For more about TMS features, refer to the "New Conference" section of the latest *Cisco TelePresence Management Suite Administrator Guide*.

  – When you configure the setup buffer feature, then schedule a meeting, the meeting start and end times will appear incorrect in TMS or Outlook.

  – Some TMS meeting alerts and prompts may appear even when your system is not in a call. (CSCug52535)

  – When the administrator uses the TMS administrative interface to delete an active meeting, the TelePresence system exits the meeting but still shows the scheduled meeting and the Join button on the Touch 12. (CSCug32505)

- **Viewing Presentations on Laptops**

The VGA cable interface requires a 60 hertz refresh rate, but some laptops receive 60hz but do not send 60hz. For best results when viewing presentation displays on your laptop, try the following:

  – Disable and re-enable sending presentation video. On IBM laptops, perform an **Fn+F7** to disable the presentation first and then use **Fn+F7** to enable the presentation again. This function is not necessary on Mac systems.

  – Set the refresh rate in the monitor settings to something other than 60hz, then set it back to 60hz.

  – Make sure that you have set your laptop resolution to 1024 x 768.

- **Web Browser Support**

The Cisco TelePresence System Administration interface is supported on Internet Explorer (IE) versions 6, 7, 8 and 9, as well as Firefox version 3.6, 5 and 9.

Supported CTS Auxiliary Devices

This section contains auxiliary devices that can be used with the CTS systems:

- Displays, page 16
- Document Cameras, page 18
- Projectors - 1.10, page 18
- Video Signal Splitters, page 18

Displays

This section describes the display choices you have with your Cisco TelePresence System and includes the following topics:

- Qualified Cisco Displays, page 16
- Using Non-Qualified Displays With your Cisco TelePresence System, page 17

Qualified Cisco Displays

The following display is qualified for use with Cisco TelePresence System running CTS or TX software:

55-inch display, part number CTS-MON-55-WW.

Before use, turn off all on-screen display (OSD) capability for the displays. This prevents the display from showing messages after you stop sharing a presentation.

To turn off OSD, complete the following steps.

Tip Perform these steps using the remote control that comes with the system, or use the joystick control on the back of the display.

Step 1 Turn the display on.

Step 2 Press **MENU** on the remote, or press the center of the joystick and move the joystick to select the menu option (the choice on the left), to bring up the menu for the display.

Step 3 Using the up and down arrows, navigate to **System** in the menu panel.

Step 4 Press **Enter** if using a remote, or press the center of the joystick if using the joystick on the display, to select the System choice.

Step 5 Using the up and down arrows, navigate to **General** and press either **Enter** on the remote, or the center of the joystick on the display.

Note This choice does not appear initially. Scroll down to see it.

Step 6 Navigate to **OSD Display** and press **Enter** or the center of the joystick.

Step 7 Set all three OSD choices (Source OSD, No Signal OSD, and MDC OSD) to **Off** (the default is On) to disable OSD messages.

Step 8 Press **EXIT** on the remote, or move the joystick to the previous menu choices, until the menu no longer displays.

Using Non-Qualified Displays With your Cisco TelePresence System

If you decide to use another auxiliary display, Cisco TelePresence systems are designed to work with any Full HD monitor that connects to the system using a standard HDMI or DVI interface. Note that the connector on the TelePresence side is an HDMI connector, so either an HDMI-to-HDMI cable or an HDMI-to-DVI cable is required.

Cisco highly recommends the use of commercial or professional-grade displays with your Immersive TelePresence system. Off-the-shelf consumer displays or TV monitors are not recommended, as they typically have shorter life spans and require a remote control to operate.

When qualifying a display for use with your TelePresence system, consider the following:

- The display should offer native support for 1080p60 over an HDMI or DVI interface.
- The display should become active when a video signal is presented, and should go to sleep when no video signal is presented.
- The display should not require any user interaction (such as a remote control or button press) to become active from standby, sleep or deep sleep modes.

- The ability to switch off On-Screen Display (OSD) messages is highly desirable. No error messages, status messages or splash screens should be visible on the screen when a presentation image is shared or unshared.
- If the display supports multiple inputs, the ability to lock the display to a given input is highly desirable. Otherwise, the time required to show presentation content can be unpredictable. If automatic scanning of ports is supported, the feature should be disabled.
- The Video Electronics Standards Association (VESA) Display Power Management Signaling (DPMS) should be present. Some consumer-grade displays, especially those designed to be used as television displays, do not use DPMS.

Document Cameras

The following WolfVision document cameras have been tested for use with CTS systems:

- VZ-C12 (Ceiling mounted)
- VZ-C32 (Ceiling mounted)
- VZ-C32^3 (Third Generation product line)
- VZ-9plus (Desktop unit)
- VZ-12^3 (All)

Projectors - 1.10

The following projectors are supported:

- Sanyo PLV-Z60—CTS 3000 and CTS 3200 systems.
- Sanyo PLV-Z700—CTS 3000 and CTS 3200 systems.

Note Cisco maintains support for the Sanyo PLV-Z4 and Sanyo PLV-Z5 projector models in older CTS configurations.

Video Signal Splitters

The following video signal splitters have been tested for use with the CTS systems:

- GEFEN EXT-HDMI-144
- EXT-HDMI-144-BLK
- GEFEN EXT-HDMI1.3-144
- GEFEN GTV-HDMI1.3-144

Note **Using External Devices with Your Cisco TelePresence System**—Cisco cannot guarantee the performance of any external device, so Cisco recommends that you choose good quality external devices to optimize CTS performance.

The CTS works best when suitable devices are attached using good quality cables and connectors. Cisco does not supply the cable that connects auxiliary devices to the codec.

Caution In European Union countries, use only devices that are fully compliant with the EMC Directive [2004/108/EC].

For information about managing video signal splitters, see the Routing Power and Signal Cables chapters of the following guides on Cisco.com:

- Cisco TelePresence System 3000 Assembly, Use & Care, and Field-Replaceable Unit Guide
- Cisco TelePresence System 3200 Assembly, Use & Care, and Field-Replaceable Unit Guide

Software Agreements and Licensing

For complete software licensing information, access the Cisco TelePresence Administration Software Licensing Information page on Cisco.com at the following link:

http://www.cisco.com/en/US/products/ps8332/products_licensing_information_listing.html

Exceptions with Other Cisco Devices

- **Dropped Audio-Only Call Between CTS and MCU**

If a non-CTS endpoint using Cisco TelePresence MCU dials out with muted video and audio, then unmutes after CTS enters the call, CTS drops the call. CTS also drops the call if the remote MCU endpoint has an audio codec that is in AAC-LD format (RAW or LATM). (CSCud21801)

- **No Video on CUCI Lync**

After EX60 transfers CUCI Lync call to CTS3000, the CTS 3000 does not send video to CUCI Lync. (CSCug02498)

- **Pixelated Video on EX90 with TC6.1.0**

Main video appears pixelated intermittently during an interop point-to-point call between CTS (1.10.1) and EX90, where EX90 is running software release TC6.1.0. (CSCug52629)

- **Pixelated Jabber Video**

During a call between CTS and Jabber, the incoming Jabber video sometimes appears pixelated. (CSCue49267)

- **Delay When Deleting a Meeting Using TMS Admin Interface**

When the administrator uses the TMS administrative interface to delete an active meeting, the TelePresence system exits the meeting but still shows the scheduled meeting and the Join button on the Touch 12. (CSCug32505)

- **TMS Alerts and Prompts**

Some TMS alerts and prompts appear even while the system is not in a call. (CSCug52535)

Exceptions with Third-Party Endpoints

- **LifeSize Endpoint on Hold After TX9x00 Hold-and-Resume**

During a call between a TX9x00 system and a LifeSize 220 system, the TX9x00 places the call on hold. After the TX9x00 resumes the call, the LifeSize system still appears to be on hold. (CSCub24934)

- **Secure SIP Calls Between CTS and LifeSize Endpoints**

Secure SIP calls between CTS and LifeSize endpoints cannot be established. (CSCtz27432)

Cisco TelePresence Software Compatibility and Device Interoperability

For complete Cisco TelePresence software compatibility and device interoperability information, go to this page:

http://www.cisco.com/en/US/products/ps8332/products_device_support_tables_list.html

Caveats in the CTS 1.10 Releases

This section contains the following caveat information:

Caveats in Cisco TelePresence System Software Release 1.10.16

The following sections show the caveats for this software release:

Unresolved Caveats in Release 1.10.16

There are no unresolved caveats in this release.

Resolved Caveats in Release 1.10.16

CSCvd06162

Symptom Cisco TelePresence 1310 ; Cisco TelePresence System 1000 ; Cisco TelePresence System 1100 ; Cisco TelePresence System 1300 ; Cisco TelePresence System 3000 Series ; Cisco TelePresence System 500-32 ; Cisco TelePresence System 500-37 ; Cisco TelePresence TX 9000 Series includes a version of OpenSSL that is affected by the vulnerability identified by one or more of the following Common Vulnerability and Exposures (CVE) IDs: CVE-2016-2108 CVE-2016-2107 CVE-2016-2105 CVE-2016-2106 CVE-2016-2109 CVE-2016-2176 And disclosed in https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160504-openssl

This bug has been opened to address the potential impact on this product. Cisco has analyzed the vulnerabilities and concluded that this product may be affected by the following vulnerabilities:

- Memory corruption in the ASN.1 encoder CVE-2016-2108
- Padding oracle in AES-NI CBC MAC check CVE-2016-2107
- EVP_EncodeUpdate overflow CVE-2016-2105
- EVP_EncryptUpdate overflow CVE-2016-2106
- ASN.1 BIO excessive memory allocation CVE-2016-2109

This product is not affected by the following vulnerability:

- EBCDIC overread CVE-2016-2176

Conditions Exposure is not configuration dependent.

Workaround None.

CSCvd25945

Symptom Current TLS version in use on CTS is TLSv1.0. It is strongly encouraged to migrate to TLSv1.2 to pick the fixes for various vulnerabilities.

Conditions Not configuration dependent.

Workaround None.

CSCuu72505

Symptom CTS 1300 and a 7945 phone are configured with the same device pool that has the America/Santiago# time zone selected in the date and time group. The phone shows the correct local time in Chile (GMT-3) but the CODEC shows the wrong time (GMT -4) when checking from the CLI. UCM is on 10.5.2.12011-1 and the codec is on 1.10.8.1

Conditions When meetings are scheduled, the phone displays a different start time. There is an off set of 1 hour in the start time and the meeting actually starts an hour early.

Workaround A different time zone in GMT -3 is used for the Date/time group

Caveats in Cisco TelePresence System Software Release 1.10.15

The following sections show the caveats for this software release:

- Unresolved Caveats in Release 1.10.15, page 22
- Resolved Caveats in Release 1.10.15, page 22

Unresolved Caveats in Release 1.10.15

There are no unresolved caveats in this release.

Resolved Caveats in Release 1.10.15

CSCuy54628

Symptom Cisco TelePresence 1310, Cisco TelePresence System 1000, Cisco TelePresence System 1100, Cisco TelePresence System 1300, Cisco TelePresence System 3000 Series, Cisco TelePresence System 500-32, Cisco TelePresence System 500-37, and Cisco TelePresence TX 9000 Series includes a version of OpenSSL that is affected by the vulnerability identified by one or more of the following Common Vulnerability and Exposures (CVE) IDs:

CVE-2016-0800 CVE-2016-0705 CVE-2016-0798 CVE-2016-0797 CVE-2016-0799 CVE-2016-0702 CVE-2016-0703 CVE-2016-0704

And disclosed in https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160302-openssl

This bug has been opened to address the potential impact on this product.

Conditions Exposure is not configuration dependent.

Cisco TelePresence System Software Release 1.10.12 and later releases and Cisco TelePresence System Software TX Release 6.1.9 and later releases are affected by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2016-0797 - BN_hex2bn/BN_dec2bn NULL pointer deref/heap corruption
- CVE-2016-0799 - Fix memory issues in BIO_*printf functions

This product is not affected by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2016-0705 - Double-free in DSA code CVE-2016-0798 - Memory leak in SRP database lookups
- CVE-2016-0702 - Side channel attack on modular exponentiation

All earlier releases of Cisco TelePresence System Software and Cisco TelePresence System Software TX are affected by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2016-0800 - Cross-protocol attack on TLS using SSLv2 (DROWN)
- CVE-2016-0703 - Divide-and-conquer session key recovery in SSLv2 CVE-2016-0704 - Bleichenbacher oracle in SSLv2
- CVE-2016-0797 - BN_hex2bn/BN_dec2bn NULL pointer deref/heap corruption
- CVE-2016-0799 - Fix memory issues in BIO_*printf functions

This product is not affected by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2016-0705 - Double-free in DSA code CVE-2016-0798 - Memory leak in SRP database lookups
- CVE-2016-0702 - Side channel attack on modular exponentiation

Workaround Not available.

Further Problem Description

Additional details about those vulnerabilities can be found at http://cve.mitre.org/cve/cve.html

PSIRT Evaluation

The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base CVSS score as of the time of evaluation is: 4.3

https://tools.cisco.com/security/center/cvssCalculator.x?version=2&vector=AV:N/AC:M/Au:N/C:P/I:N/A:N/E:ND/RL:ND/RC:ND

The Cisco PSIRT has assigned this score based on information obtained from multiple sources. This includes the CVSS score assigned by the third-party vendor when available. The CVSS score assigned may not reflect the actual impact on the Cisco Product. Additional information on Cisco's security vulnerability policy can be found at the following URL:

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

CSCuz44368

Symptom Cisco TelePresence 1310 ; Cisco TelePresence System 1000 ; Cisco TelePresence System 1100 ; Cisco TelePresence System 1300 ; Cisco TelePresence System 3000 Series ; Cisco TelePresence System 500-32 ; Cisco TelePresence System 500-37 ; Cisco TelePresence TX 9000 Series includes a version of ntpd that is affected by the vulnerabilities identified by the Common Vulnerability and Exposures (CVE) IDs:

CVE-2016-1551, CVE-2016-2516, CVE-2016-2517, CVE-2016-2518, CVE-2016-2519, CVE-2015-8138, CVE-2016-1550, CVE-2015-7704, CVE-2016-1547, CVE-2016-1548, CVE-2016-1549

And disclosed in http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160428-ntpd

This product is affected by one or more of the listed CVE ids.

Conditions Device configured with NTP.

Cisco has reviewed and concluded that this product is affected by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2016-2518 - Network Time Protocol Crafted addpeer With hmode > 7 Causes Array Wraparound With MATCH_ASSOC
- CVE-2015-8138 - Network Time Protocol Zero Origin Timestamp Bypass
- CVE-2016-1550 - Network Time Protocol Improve NTP Security Against Buffer Comparison Timing Attacks
- CVE-2015-7704 - Network Time Protocol Original Fix For NTP Bug 2901 Broke Peer Associations
- CVE-2016-1548 - Network Time Protocol Interleave-pivot Denial Of Service Vulnerability
- CVE-2016-1549 - Network Time Protocol Sybil Vulnerability: Ephemeral Association Attack
- CVE-2016-1551: Network Time Protocol Refclock Impersonation Vulnerability
- CVE-2016-2516: Network Time Protocol Duplicate IPs On Unconfig Directives Will Cause An Assertion Botch In ntpd
- CVE-2016-2519 - Network Time Protocol Remote ctl_getitem() Return Value Not Always Checked
- CVE-2016-2517: Network Time Protocol Remote Configuration Trustedkey/Requestkey/Controlkey Values Are Not Properly Validated
- CVE-2016-1547 - Network Time Protocol CRYPTO-NAK Denial Of Service Vulnerability

Workaround Not available.

Further Problem Description

Additional details about those vulnerabilities can be found at http://cve.mitre.org/cve/cve.html

PSIRT Evaluation

The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are: 6.4/5.3.

http://tools.cisco.com/security/center/cvssCalculator.x?version=2&vector=AV:N/AC:L/Au:N/C:N/I:P/A:P/E:F/RL:OF/RC:C/CDP:N/TD:N/CR:L/IR:L/AR:

The Cisco PSIRT has assigned this score based on information obtained from multiple sources. This includes the CVSS score assigned by the third-party vendor when available. The CVSS score assigned may not reflect the actual impact on the Cisco Product.

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

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

Caveats in Cisco TelePresence System Software Release 1.10.14.1

The following sections show the caveats for this software release:

- Unresolved Caveats in Release 1.10.14.1, page 25
- Resolved Caveats in Release 1.10.14.1, page 25

Unresolved Caveats in Release 1.10.14.1

There are no unresolved caveats in this release.

Resolved Caveats in Release 1.10.14.1

CSCum73658

Symptom RTP is no longer encrypted after upgrading the TX9000 to TX.6-1-11-7R-K9.P2 in calls between the TX and another TX or CTS. Signaling remains encrypted.

Conditions TX9000 running TX.6-1-11-7R-K9.P2 and using secure phone profile. Secure profile security mode is set to "Encrypted".

Workaround Downgrade the TX9000 to the previous release.

CSCuy25616

Symptom Call fails due to an encryption mismatch.

Conditions Final DTLS packet is lost when dialling from CTS to the TelePresence Server (or another endpoint).

Workaround Redial the call.

CSCuy72190

Symptom Call becomes non-secure. The TX9000 and IX5000 doesn't have this issue, but it impacts the CTS 3000 endpoint.

Conditions Secure CTS 3000, Secure CUCM 10.5.2 and secure CTMS 1.9.7, CTS3000 endpoint becomes non-secure.

Workaround CTS 3000 1.10.5 works fine.

Caveats in Cisco TelePresence System Software Release 1.10.14

The following sections show the resolved and unresolved caveats for this software release:

- Unresolved Caveats in Release 1.10.14, page 27
- Resolved Caveats in Release 1.10.14, page 27

Unresolved Caveats in Release 1.10.14

There are no unresolved caveats in this release.

Resolved Caveats in Release 1.10.14

CSCuw35927

Symptom DTMF reception problems noted on Cisco immersive endpoints with some third party systems

Conditions Some third party audio or video bridges dropping or not interpreting DTMF digits correctly from CTS release 1.10.13, TX release 6.1.10, and IX release 8.0.6 endpoints

Workaround None.

CSCux20885

Symptom No media on calls into a Cisco TelePresence Server conference that are intercepted by an SBC's (Session Border Controller) IVR (interactive voice response) system until a hold/resume is performed.

Conditions Calls through an SBC/IVR into a TelePresence Server conference while running CTS releases earlier than 1.10.14 and TX releases earlier than 6.1.11

Workaround After connecting to the TelePresence Server conference, perform a hold/resume to re-establish an audio/video connection.

CSCux49232

Symptom Cisco TelePresence System (CTS) includes a version of Partial Hypertext Preprocessor (PHP) library that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs: CVE-2015-6831, CVE-2015-6832 and CVE-2015-6833

Conditions Device with default configuration.

Workaround Not currently available.

CSCuu82518

Symptom This product includes a version of OpenSSL that is affected by the vulnerability identified by the Common Vulnerability and Exposures (CVE) IDs: CVE-2015-4000, CVE-2015-1788, CVE-2015-1789, CVE-2015-1790, CVE-2015-1792, CVE-2015-1791, CVE-2014-8176

Conditions Exposure is not configuration dependent. The following product lines are affected: CTS500-32, CTS1100, CTS1300, CTS3200, and TX9200. Currently latest code runs OpenSSL 1.0.1m. An update to the OpenSSL code is required.

Workaround Not Available

CSCux72873

Symptom For CTS systems using an IP Phone as the interface, TMS scheduled OBTP (one button to push) meetings end up with the "Join" button being active 5 minutes before the meeting start, irrespective of the set up buffer timer specified in TMS.

Conditions CTS systems running releases earlier than 1.10.14 with Cisco 797x phone running the TelePresence IP Phone midlet

Workaround None

Caveats in Cisco TelePresence System Software Release 1.10.13

The following sections show the resolved and unresolved caveats for this software release:

- Unresolved Caveats in Release 1.10.13, page 29
- Resolved Caveats in Release 1.10.13, page 29

Unresolved Caveats in Release 1.10.13

There are no unresolved caveats in this release.

Resolved Caveats in Release 1.10.13

CSCuu97607

Symptom With IX5000 to IX5000 P2P call, when local has audio add-in, remote can't share multi-content.

Conditions Only when local has audio add-in involved.

Workaround There is no workaround.

CSCuu35442

Symptom TX requests .sgn config when CTL file is empty in non-secure UCM cluster.

When an unsecured CUCM cluster sends an empty CTL file to TelePresence Immersive endpoints (CTS, TX, and IX), the endpoint attempts to download a signed config file from the TFTP server. Since the CUCM cluster is nonsecure, only unsigned files are available. This causes the endpoint to not receive any config updates, possibly leading to it not registering with CUCM, in which case calls are not possible.

Conditions When nonsecure CUCM that was previously secure is sending an empty CTL file to the endpoint.

Workaround Delete CTL from CUCM and clear security credentials on the endpoint.

CSCuv81870

Symptom DTMF events have inconsistent event timestamps.

Conditions Each DTMF event should have the same timestamp. When the same event does not, a remote system receives incorrect digits.

Workaround There is no workaround.

Caveats in Cisco TelePresence System Software Release 1.10.12

The following sections show the resolved and unresolved caveats for this software release:

- Unresolved Caveats in Release 1.10.12, page 30
- Resolved Caveats in Release 1.10.12, page 30

Unresolved Caveats in Release 1.10.12

There are no unresolved caveats in this release.

Resolved Caveats in Release 1.10.12

CSCuu20752

Symptom SNMP crashes are experienced on TX endpoints when in a call with an MX800. Note that the SNMP server crash is not experienced between an MX800 with SpeakerTrack and TX systems.

The behavior is independent of software versions.

MX800 -> TX1310 - SNMP server crashes on the TX.

MX800 -> TX9000 - SNMP server crashes on the TX.

MX800 Speakertrack -> TX1310 - SNMP server does not crash on the TX.

MX800 Speakertrack -> TX9000 - SNMP server does not crash on the TX.

Conditions The issue can occur if the remote URI is greater than or equal to 32 characters.

Workaround Use URIs that are 32 characters or less.

CSCuu34838

Symptom Directory entries are not appearing on the Touch 12 device.

Conditions This condition is seen when the “Alternate CUCM for Directory Lookup” field is specified in Unified CM. This field is not being applied correctly.

Workaround There is no workaround.

CSCuu49617

Symptom Intermittent video quality issues are seen in a point-to-point or CTMS call with an IX5000.

Conditions This condition is caused by a buffer overflow.

Workaround There is no workaround.

CSCuu79520

Symptom A switch from a right or left segment to a center segment can cause video quality issues.

Conditions This issue is seen with three-screen immersive Cisco TelePresence systems (CTS, TX, or IX series systems).

Workaround There is no workaround.

Caveats in Cisco TelePresence System Software Release 1.10.11.2

The following sections show the resolved and unresolved caveats for this software release:

- Unresolved Caveats in Release 1.10.11.2, page 31
- Resolved Caveats in Release 1.10.11.2, page 31

Unresolved Caveats in Release 1.10.11.2

There are no unresolved caveats in this release.

Resolved Caveats in Release 1.10.11.2

CSCuu49617

Symptom Intermittent video quality issues are seen in a point-to-point or CTMS call with an IX5000.

Conditions This condition is caused by a buffer overflow.

Workaround There is no workaround.

Caveats in Cisco TelePresence System Software Release 1.10.11.1

The following sections show the resolved and unresolved caveats for this software release:

- Unresolved Caveats in Release 1.10.11.1, page 32
- Resolved Caveats in Release 1.10.11.1, page 32

Unresolved Caveats in Release 1.10.11.1

There are no unresolved caveats in this release.

Resolved Caveats in Release 1.10.11.1

CSCuu25109

Symptom Duplicate DTMF tones are sent during a Cisco WebEx call.

Conditions This caveat is seen under the following conditions:

1. Using a TelePresence endpoint, dial a Cisco WebEx dial-in number.
2. When prompted, enter any digit and do not press the pound sign.

In these conditions, duplicate numbers are sent. For example, pressing the number '1' sends '11111'.

Workaround There is no workaround.

Caveats in Cisco TelePresence System Software Release 1.10.11

The following sections show the resolved and unresolved caveats for this software release:

- Unresolved Caveats in Release 1.10.11, page 32
- Resolved Caveats in Release 1.10.11, page 33

Unresolved Caveats in Release 1.10.11

There are no unresolved caveats in this release.

Resolved Caveats in Release 1.10.11

CSCuq19232

Symptom Error messages, such as the following, for the Auxiliary Control Unit (ACU) are frequently seen in Sysop logs:

Conditions These messages are frequently seen in sysop logs of a CTS endpoint.

Workaround There is no workaround.

CSCur48604

Symptom When Address Resolution Protocol (ARP) requests are sent to Cisco TelePresence immersive systems, the system's internal address (i.e. 192.168.x.1) is being returned, rather than the system's actual network address.

Conditions This is seen only when 802.1x is enabled.

Workaround One likely cause of the problem is an external device on the network segment that is pinging, or sending ARP requests to the 192.168.x.1 address. So, a workaround would be to remove that device.

CSCut10214

Symptom RTP Control Protocol (RTCP) encryption was disabled for presentation sharing.

Conditions This condition was noted when using the Binary Floor Control Protocol (BFCP) for presentation sharing.

Workaround There is no workaround.

CSCut10506

Symptom Conference IDs are not included in the Cisco TelePresence Call MIB. In addition, scheduled calls cannot be exported via SNMP.

Conditions These conditions are noted when using SNMP to include call information

Workaround This CDETS incorporates the following OID in the CISCO-TELEPRESENCE-CALL-MIB.my:

1.3.6.1.4.1.9.9.644.1.4.8.1.18

The object name in the CISCO-TELEPRESENCE-CALL-MIB is

ctpcMeetingId

CSCut58844

Symptom Audio reverberation is heard during a meeting.

Conditions This condition can be seen in multipoint meetings using TelePresence server when a user sends DTMF tones by pressing the keypad on the Touch device.

Workaround There is no workaround.

CSCut77627

Symptom This product includes a version of ntpd that is affected by the vulnerability identified by the Common Vulnerability and Exposures (CVE) IDs:

CVE-2015-1798 and CVE-2015-1799

This bug has been opened to update the version of ntpd used within this product.

Conditions Whilst this product contains a vulnerable version of ntpd it has been concluded that these vulnerabilities are not exploitable on this product.

Workaround Not applicable.

CSCut60802

Symptom The Touch 12 cannot control the document camera.

Conditions This behavior is seen when trying to control the document camera via the Touch device.

Workaround You can control the document camera using the remote control that shipped with it.

Caveats in Cisco TelePresence System Software Release 1.10.10

The following sections show the resolved and unresolved caveats for this software release:

- Unresolved Caveats in Release 1.10.10, page 35
- Resolved Caveats in Release 1.10.10, page 35

Unresolved Caveats in Release 1.10.10

There are no unresolved caveats in this release.

Resolved Caveats in Release 1.10.10

CSCus85759

Symptom On January 27, 2015, a buffer overflow vulnerability in the GNU C library (glibc) was publicly announced. This vulnerability is related to the various gethostbyname functions included in glibc and affect applications that call these functions. This vulnerability may allow an attacker to obtain sensitive information from an exploited system or, in some instances, perform remote code execution with the privileges of the application being exploited. This vulnerability is documented in CVE-2015-0235.

A Cisco Security Advisory has been published to document this vulnerability at:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150128-ghost

This bug has been opened to address the potential impact on this product.

Conditions Exposure is not configuration dependent.

Workaround There is no workaround.

Caveats in Cisco TelePresence System Software Release 1.10.9

The following sections show the resolved and unresolved caveats for this software release:

- Unresolved Caveats in Release 1.10.9, page 35
- Resolved Caveats in Release 1.10.9, page 36

Unresolved Caveats in Release 1.10.9

There are no unresolved caveats in this release.

Resolved Caveats in Release 1.10.9

CSCum61281

Symptom Choppy welcome audio is heard at the beginning of a call.

Conditions This condition is observed on systems running TX or Cisco TelePresence System (CTS) software systems when dialing into a multipoint call using an MCU 5320.

Workaround There is no workaround.

CSCuq76637

Symptom Cisco TelePresence Systems connected to a third party switch experience intermittent crashes where all services on the system are restarted, and the system is unable to connect to its secondary codecs since the /etc/host file is missing.

Conditions This condition is seen with Cisco TelePresence Systems that use the Cisco TelePresence Touch 12 for call control. when connected to a third-party switch.

Workaround Reboot the device.

Caveats in Cisco TelePresence System Software Release 1.10.8

The following sections show the resolved and unresolved caveats for CTS software release 1.10.8:

- Unresolved Caveats in Release 1.10.8, page 36
- Resolved Caveats in Release 1.10.8, page 37

Unresolved Caveats in Release 1.10.8

There are no unresolved caveats in this release.

Resolved Caveats in Release 1.10.8

CSCum75022

Symptom A secure call cannot see the presentation for a multipoint call when dialed into an MCU.

Conditions This condition occurs when there is a mix of secure and non-secure endpoints in a multipoint call.

Workaround There is no workaround.

CSCuo00268

Symptom A “Touch backlight turned on” message occurs repeatedly in the sysop log.

Conditions This message occurs on systems that use the Touch 10 device for call control.

Workaround There is no workaround.

CSCuo98569

Symptom CTS-Touch 12 is stuck at checkbox #5 and the message “Unable to load boot image”.

Conditions The path MTU between the Unified CM TFTP node and the codec is less than 1500 bytes.

Workaround Lower the MTU on the Unified CM to match the path MTU.

CSCup48115

Symptom No main video is seen during a Cisco TelePresence call.

Conditions This condition occurs during a call between a TX1300-65 or TX9xxx system and a Cisco TelePresence system with a C40 codec.

Workaround There is no workaround.

CSCup92876

Symptom CTS core unreregisters when change the bandwidth is changed from Auto to 250KB on DX devices.

Conditions Make a video call from DX device to CTS device. Change video bandwidth from Auto to 250KBPS. CTS device Unregistered from CUCM.

Workaround There is no workaround.

CSCuq49459

Symptom While dialing Live Desk, the system omits the last digit from the URI.

Conditions User dialing Live Desk support from Touch omits the last character.

Workaround Dial the number manually, or remove one character from the URI.

CSCuq90956

Symptom In a secure call between a DX system and a system running CTS software, the video freezes on the DX side when the CTS side shares a presentation.

Conditions Conditions: This condition affects the following Cisco TelePresence Systems:

- Cisco TelePresence System 500-37 (PID: CTS-500)
- Cisco TelePresence System 1000 (PID: CTS-1000)
- Cisco TelePresence System 1100 (PID: CTS-1100)
- Cisco TelePresence System 1300-65 (PID: CTS-1300)
- Cisco TelePresence System 3000 (PID: CTS-3000)
- Cisco TelePresence System 3010 (PID: CTS-3010)
- Cisco TelePresence System 3200 (PID: CTS-3200)
- Cisco TelePresence System 3210 (PID: CTS-3210)

Workaround Perform one of the following steps:

- Issue a hold/resume sequence on the CTS endpoint.
- Set the call to non-secure.

Caveats in Cisco TelePresence System Software Release 1.10.7

The following sections show the resolved and unresolved caveats for CTS software release 1.10.7:

- Unresolved Caveats in Release 1.10.7, page 39
- Resolved Caveats in Release 1.10.7, page 39

Unresolved Caveats in Release 1.10.7

There are no unresolved caveats in this release.

Resolved Caveats in Release 1.10.7

CSCun90394

Symptom CTS point to point calls fail to establish Intermittently, and a "Call ended due to unsupported protocol configuration" error message is seen in the sysop logs.

Conditions In all occurrences, the CTS system involved has been using a 7975 IP Phone as the call control device.

Workaround Rejoin the call.

CSCup22603

Symptom Earlier versions of OpenSSL have vulnerabilities that are being tracked by the Cisco Product Security Incident Response Team (PSIRT). For more information, refer to the PSIRT notice at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140605-openssl (Cisco login required).

Conditions The vulnerable releases by product are:

- TX9000, TX9200, TX1310-65 and CTS500-32: 1.9.x, 6.0.x, 6.1.0, 6.1.2, and 6.1.3
- CTS3000, CTS3010, CTS3200, CTS3210, CTS1000, CTS1100, CTS1300 and CTS500-37: 1.8.x, 1.9.x, 1.10.0, 1.10.1, 1.10.2, 1.10.3, 1.10.4, 1.10.5, and 1.10.6

Workaround There is no workaround.

CSCup32890

Symptom The Cisco TelePresence Administration software uses an Apache server version of 2.2.24, which contains the CVE-2013-1862 vulnerability.

Conditions This condition occurs with Apache server versions earlier than version 2.2.25.

Workaround There is no workaround.

Caveats in Cisco TelePresence System Software Release 1.10.6

The following sections show the resolved and unresolved caveats for CTS software release 1.10.6:

- Unresolved Caveats in Release 1.10.6, page 40
- Resolved Caveats in Release 1.10.6, page 40

Unresolved Caveats in Release 1.10.6

There are no unresolved caveats in this release.

Resolved Caveats in Release 1.10.6

CSCul14243

Symptom During an MCU call, when sharing presentation with 1440x900 or 1280x800 resolutions, the remote endpoints cannot see the presentation.

Conditions This condition only occurs when the resolution is at 1440x900 and 1280x800 pixels.

Workaround Use another resolution to share the presentation.

CSCul18329

Symptom When upgrading to 1.10.4, 802.1X authentication fails in a 802.1X MAC Authentication Bypass (MAB) network configuration and there isn't a way to disable it on the codec.

Conditions The codec is plugged into a port with 802.1X authentication enabled.

Workaround Disable 802.1X on the network port.

CSCun26655

Symptom During a point-to-point or TelePresence server 1080p call, DSP code could reload after a long period of time (several hours or more). The user sees frozen video or video flashes for a couple of seconds. The call does not drop.

Conditions This condition applies to systems running software version between CTS 1.9.3 and CTS 1.10.4.

Workaround There is no workaround.

CSCun68503

Symptom This caveat removes the requirement that the TFTP server have a certificate entry in the Certificate Trust List (CTL) of the codec. However, the signer of the configuration file that is downloaded from the TFTP server must still appear in the CTL of the codec, or the file fails validation.

Conditions This condition affects all systems running software versions earlier than TX 6.1.3 or CTS 1.10.6.

Workaround There is no workaround.

CSCun90394

Symptom CTS point to point calls fail to establish Intermittently, and a `Call ended due to unsupported protocol configuration` error message is seen in the sysop logs.

Conditions This condition applies to systems running software version between CTS 1.9.3 and CTS 1.10.4.

Workaround There is no workaround.

CSCuo19578

Symptom 2-3 times every minute, the TelePresence immersive system sysop logs report the following error: `user 5 root: getServicesUrl exits with 3.`

Conditions The following conditions must be present: 1. the system has a Touch Panel connected. 2. The system has a Cisco Unified IP Phone with MIDlets that do not function.

Workaround There is no workaround.

Caveats in Cisco TelePresence System Software Release 1.10.5.1

The following sections show the resolved and unresolved caveats for software release 1.10.5.1:

- Unresolved Caveats in Release 1.10.5.1, page 42
- Resolved Caveats in Release 1.10.5.1, page 42

Unresolved Caveats in Release 1.10.5.1

There are no unresolved caveats in this release.

Resolved Caveats in Release 1.10.5.1

CSCuo20210

Symptom The following Cisco TelePresence Systems include a version of OpenSSL that is affected by the vulnerability identified by the Common Vulnerability and Exposures (CVE) ID CVE-2014-0160.

- Cisco TelePresence System 500-32
- Cisco TelePresence System 500-37
- Cisco TelePresence System 1000
- Cisco TelePresence System 1100
- Cisco TelePresence System 1300
- Cisco TelePresence 1310
- Cisco TelePresence System 3000 Series
- Cisco TelePresence TX 9000 Series

This CDETS has been opened to address the potential impact on this product.

Conditions The vulnerable releases by product, are:

- TX9000, TX9200, TX1310-65 and CTS500-32: 6.0.*x*, 6.1.0, 6.1.1, and 6.1.2
- CTS3000, CTS3010, CTS3200, CTS3210, CTS1000, CTS1100, CTS1300 and CTS500-37: 1.10.0, 1.10.1, 1.10.2, 1.10.3, 1.10.4 and 1.10.5

Workaround There is no workaround.

CSCuo30624

Symptom A manufacturer-installed certificate (MIC) can only be generated only during manufacturing. Because of OpenSSL Heartbeat Extension Vulnerability, if a MIC has been exposed, the system is susceptible to attacks even after applying the Heartbleed patch. This caveat adds an enhancement to allow a locally significant certificate (LSC) to be used by the Key Exchange process to establish Datagram Transport Layer Security (DTLS) sessions between endpoints.

Conditions This condition might arise for any TelePresence systems that are affected by the Heartbleed vulnerability. See CSCuo20210 for a list of the systems and software. There is also a Cisco security advisory at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140122-cts.

Workaround There is no workaround.

Caveats in Cisco TelePresence System Software Release 1.10.5

The following sections show the resolved and unresolved caveats for software release 1.10.5:

- Unresolved Caveats in Release 1.10.5, page 43
- Resolved Caveats in Release 1.10.5, page 43

Unresolved Caveats in Release 1.10.5

There are no unresolved caveats in this release.

Resolved Caveats in Release 1.10.5

CSCul56741

Symptom When a Cisco Desktop Collaboration Experience DX650 receives a packet loss notification, it sends an Instantaneous Decoder Refresh (IDR) request to a Cisco TelePresence System 500-32, 500-37, or 1000, using a Real-Time Transport Control Protocol (RTCP) Full Intra Request (FIR). However, the Cisco TelePresence System does not send any IDR response to the DX650.

Conditions This condition has been seen in a point-to-point call between a DX650 and CTS-500, or between a DX650 and a CTS-1000. The Cisco Unified Communications Manager version was 10.0.

Workaround There is no workaround.

CSCum86504

Symptom Temperature monitoring from SNMP can fail to work after the system has been monitored for a long period of time (one week or more).

Conditions The left or right displays of multi-display systems can show invalid temperature information after a week of monitoring using SNMP.

Workaround There is no workaround.

CSCun37251

Symptom Cisco TelePresence System (CTS) and TX Series endpoints will experience media service restarts on all three codecs if the legacy encoder bit rate is mistakenly set to anything lower than 704kbps during a call.

Conditions This issue can occur in multipoint calls hosted on Cisco TelePresence Multipoint Switch (CTMS).

Workaround There is no workaround.

CSCun60003

Symptom When a Cisco Jabber endpoint using Cisco Collaboration Edge calls a Cisco TelePresence System (CTS) 500-37, the video on the CTS freezes after the Jabber endpoint shares a presentation.

Conditions This condition only when the Jabber endpoint is connected using Cisco Collaboration Edge architecture.

Workaround There is no workaround.

Caveats in Cisco TelePresence System Software Release 1.10.4

The following sections show the resolved and unresolved caveats for software release 1.10.4:

- Unresolved Caveats in Release 1.10.4, page 44
- Resolved Caveats in Release 1.10.4, page 45

Unresolved Caveats in Release 1.10.4

There are no unresolved caveats in this release.

Resolved Caveats in Release 1.10.4

CSCug90524

Symptom When clicking on the magnifying glass under “System Status” in the Cisco TelePresence Administration GUI, the projector status is shown as **unknown**.

Conditions This condition exists whether you are in or out of a call, or whether or not you are using the projector to share a presentation.

Workaround There is no workaround.

CSCuh01240

Symptom Occasionally, an incorrect error message such as “ERROR Auxiliary Control Unit status is Not Ready(Check Device).” periodically appears in the sysop log.

Conditions This condition occurs on Cisco TelePresence running 1.10.x releases.

Workaround There is no workaround.

CSCui72815

Symptom A Cisco TelePresence System (CTS) 500-32 or CTS 500-37 that uses a Cisco Unified IP Phone for call control receives a call, and the call is muted. If a second call is received and answered by the CTS, the first call is unmuted.

Conditions This condition arises when a CTS 500-32 or CTS 500-37 is muted and receives another incoming call.

Workaround Mute the CTS again.

CSCuj70026

Symptom A Cisco TelePresence System 3000, 3010, 3200, 3101, or TX9000 system intermittently shows as an audio conference, and a blank display is seen on one or two of the three screens.

Conditions This condition is seen when a call is going through an MCU with a Cisco TelePresence System 3000, TX1310-65, and TX9000.

Workaround There is no workaround.

CSCul24865

Symptom Video corruption is seen between a Cisco TelePresence System TX9000 and a Lync 2013 client.

Conditions This condition is seen when in a call between a Cisco TelePresence CTS or TX system and a Lync client.

Workaround Use a Cisco TelePresence Server or a Cisco TelePresence MCU between the Cisco TelePresence system and the Lync client.

CSCul13329

Symptom A Cisco TelePresence Systems (CTS) in a secure call will not hear audio participants after the SIP Session Refresh timer.

Conditions This issue is present in the following circumstances:

- Secured CTS audio only call to an IP Phone.
- Secured CTS to CTS call with an audio add-in participant.

Workaround Complete the following steps:

1. Issue a hold/resume sequence on the CTS endpoint.
2. Set the call to non-secure.

CSCul48364

Symptom Directories do not appear on the Touch device of your TelePresence system.

Conditions This condition occurs only with Cisco Unified Communications Manager (Unified CM) 10.0, and only after an upgrade to TX 6.1.0 or CTS 1.10.3.

Workaround There is no workaround.

CSCum44498

Symptom The Cisco Unified IP phone component of the Cisco TelePresence system loses its registration to Cisco Unified Communications Manager after the system upgrades from a Cisco TelePresence Administration software release before 1.10.0 to a 1.10.x release. In addition, the phone becomes inoperable.

Conditions This condition is seen with systems that use IP Phones for call control only. Systems that use the Touch device for call control are not affected.

Workaround If possible, disable link layer discovery protocol (LLDP) on the Ethernet switchport connecting the Cisco TelePresence system.

Caveats in Cisco TelePresence System Software Release 1.10.3

The following sections show the resolved and unresolved caveats for CTS software release 1.10.3:

- Unresolved Caveats in Release 1.10.3, page 47
- Resolved Caveats in Release 1.10.3, page 48

Unresolved Caveats in Release 1.10.3

CSCul48364 (fixed in Release 1.10.4)

Symptom Directories do not appear on the Touch device of your TelePresence system.

Conditions This condition occurs after an upgrade to TX 6.1.0 or CTS 1.10.3.

Workaround There is no workaround.

Resolved Caveats in Release 1.10.3

CSCuf52211

Symptom The presentation freezes at the remote sites when content is being sent after 2-3 hours on a call using the TelePresence Server. The presentation was frozen on all 1.9.5 endpoints, including CTS 1300, 500-32, 500-37, TX1310, CTS1100, CTS1300, and not frozen on endpoints running 1.9.2. CTS3000 running 1.9.5 is presenting in this case. This condition appears whether the presentation display is a monitor or a projector, or is using an external presentation display.

The same condition is seen on systems using CTMS without the TelePresence Server; however this condition is seen after a longer time (more than 13 hours).

Conditions This condition is seen on CTS endpoints running 1.9.5 and connected to CTMS (1.9.3) and TPS 2.3 (1.57).

Workaround Press **Hold** and **Resume** to resolve this problem.

CSCug80319

Symptom During a conference with another Cisco TelePresence immersive endpoint running Release 1.9, the endpoint running 1.9 software shares a presentation. The endpoint running 1.10 software displays a cropped image of the presentation.

Conditions This condition appears whether the presentation display is a monitor or a projector, or is using an external presentation display.

Workaround No workaround is available.

CSCug80344

Symptom You experience one-way audio during a conference.

Conditions The following conditions cause the issue:

1. You place a call from a TX system to another system that is not a CTS (CTS 1000, 1100, 1300-65, 3000, 3010, 3200, or 3210) or TX (TX1310-65, TX9000, or TX9200) system. This type of call is known as an interop call.
2. You add another CTS or TX system to the call.

Workaround Hold, and then resume, the conference.

You can prevent this issue by calling the CTS or TX system first, then placing the interop call.

CSCuh18153

Symptom When a TX or CTS system joins an MCU call as the first participant, the audio prompt that plays is corrupted slightly.

Conditions This issue occurs when a CTS or TX system enters an MCU call as the first participant.

Workaround There is no workaround.

CSCuh64139

Symptom During a point-to-point call between a TelePresence endpoint and another endpoint that does not use MUX or TIP (known as an interop call), a third endpoint calls the VCS-registered endpoint, and the three endpoints enter a conference (either an MCU or TelePresence conference).

If it is an MCU conference: after entering the conference, the TelePresence endpoint does not see any incoming video, and the shared presentation appears on the center screen. If it is a TelePresence conference: only XGA resolution is supported and all other resolutions are disabled.

Conditions A conflict in BFCP server mode occurs between the TelePresence endpoint and the server (whether MCU or TelePresence server). The conflict disables BFCP server mode.

Workaround Press hold and resume on the TelePresence endpoint.

CSCui33067

Symptom When attempting to perform an audio add-in, the directory appears, but there is no keypad.

Conditions This condition appears during an audio add-in attempt during a TelePresence conference.

Workaround Tap the New Call button to display the keypad.

CSCui65472

Symptom During a multipoint call, a multi-screen immersive system can be appear as a single-screen endpoint because of insufficient system resources (insufficient ports). In this case, the screen will not switch to the active speaker.

Conditions This condition occurs during a multi-point call using a TelePresence Server, and not enough ports were available for all three segments of an immersive system.

Workaround Make sure that you allow the correct amount of resources during a multipoint call.

CSCui65578

Symptom During a call that is using the TelePresence Interoperability Protocol (TIP) to switch a shared presentation, endpoints that are using TIP cannot see the presentation.

Conditions If the bandwidth for your conference is less than 2 Mbps, TIP can fail. In this case, the presentation reverts to switched mode and non-immersive endpoints no longer share the presentation.

Workaround Make sure that your bandwidth is set to more than 2 Mbps.

CSCui77480

Symptom You place a call from a CTS or TX system registered to Unified CM to another Cisco TelePresence system registered to the Video Communication Server (VCS) by way of an H.323 SIP gateway. This type of call is known as an interop call.

The presentation is not seen if the other side is a C90 or an SX20.

Conditions This happens during an interop call between a TX system and a C90 or an SX20.

Workaround Press Hold, then Resume, on the TX system.

CSCuj69311

Symptom Cisco TelePresence systems running CTS software release 1.10.2 are not able to retrieve system temperature information using SNMP.

Conditions This condition occurs when Cisco TelePresence systems are running release 1.10.2.

Workaround There is no workaround.

CSCul47854

Symptom CTS endpoints dialing into a Cisco TelePresence Server meeting set to max quality (1080P video/1080P content) connect at 720P30.

Conditions This symptom occurs under the following conditions:

1. CTS endpoints are running 1.10.1.
2. Call goes to the Cisco TelePresence Conductor.
3. The Conductor sends the call to the TelePresence Server.
4. Max quality is set (1080P video / 1080P content) on the TelePresence Server.

Workaround There is no workaround.

Caveats in Cisco TelePresence System Software Release 1.10.2

The following sections show the resolved and unresolved caveats for CTS software release 1.10.2:

- Unresolved Caveats in CTS Release 1.10.2, page 51
- Resolved Caveats in CTS Release 1.10.2, page 53

Unresolved Caveats in CTS Release 1.10.2

CSCud21804

Symptom After an endpoint enters an MCU conference number, the MCU PIN entry screen appears corrupted. Video corruption may also appear intermittently during the MCU conference.

Conditions Issue occurs intermittently after an endpoint enters an MCU conference number.

Workaround There is no workaround.

CSCue49267

Symptom During a call between CTS and Jabber, the incoming Jabber video sometimes appears pixelated.

Conditions Issue occurs intermittently during a call between CTS and Jabber.

Workaround Press hold and resume.

CSCug32505

Symptom When the administrator uses the TMS administrative interface to delete an active meeting, the TelePresence system exits the meeting but still shows the scheduled meeting and the Join button on the Touch 12.

Conditions Issue occurs when an active meeting is canceled by the administrator using the TMS administrative interface.

Workaround Wait for a few seconds until the meeting information and Join button disappear.

CSCug52535

Symptom Some TMS alerts and prompts appear even while the system is not in a call.

Conditions The TelePresence system is managed by TMS but is not in a call.

Workaround There is no workaround.

CSCug80319

Symptom When a presentation is shared during a call between two CTS endpoints, the remote endpoint may see the presentation image slightly cut off on the left side.

Conditions Issue occurs on the remote endpoint, during a call where both endpoints are running CTS software release 1.9.

Workaround There is no workaround.

CSCuh12678

Symptom During a call, TX9x00 system camera image appears pink or purple, both on the remote endpoint screen and in self view mode.

Conditions Issue occurs on systems running camera firmware 1.9.2 or 1.9.3.

Workaround Reboot the system codec or recalibrate the camera to adjust the white balance.

CSCui65578

Symptom In a low-bandwidth interop call, after CTS shares a BFCP presentation, the remote endpoint loses incoming video. BFCP presentation fails and CTS reverts to switched presentation mode.

Conditions Issue occurs during an interop call (not MUX or TIP), where bandwidth is lower than 2 mbps.

Workaround Raise the bandwidth to a value greater than 2 mbps.

Resolved Caveats in CTS Release 1.10.2

CSCug94889

Symptom Systems running CTS or TX software are dropped during a conference using the Cisco TelePresence Server.

Conditions This condition occurs during an ad-hoc, secure conference using a Cisco TelePresence Server running TS 3.1 with a system running CTS software release 1.10.1 or earlier, or TX software release 6.0.2 or earlier.

Workaround If your Cisco TelePresence server is running release 3.1 or later, upgrade your CTS systems to CTS release 1.10.2 or later, and upgrade your TX systems to TX release 6.0.3 or later.

CSCug28175

Symptom During a point-to-point call between a TX9x00 system and a TX1310 65 system, a shared presentation may appear pixelated intermittently on the remote endpoint.

Conditions This issue occurs during a point-to-point call between a TX9x00 system and a TX1310 65 system, where one system shares a presentation.

Workaround There is no workaround.

CSCuh54966

Symptom During a multipoint call using an MCU, the presentation image appears pixelated on the lower part of the image.

Conditions This condition occurs when the audio and video are sent securely, but the presentation (media) content is non-secure. The presentation media is sent securely in error, which leads to the pixelation of the image.

Workaround There is no workaround.

Caveats in Cisco TelePresence System Software Release 1.10.1

The following sections show the resolved and unresolved caveats for CTS software release 1.10.1:

- Unresolved Caveats in CTS Release 1.10.1, page 54
- Resolved Caveats in CTS Release 1.10.1, page 55

Unresolved Caveats in CTS Release 1.10.1

CSCuf32686

Symptom During a multipoint call where one participant is a Cisco Unified IP Phone connected via audio add-in, an endpoint shares a presentation. When the IP Phone goes on hold, the presentation (on the endpoint that performed the audio add-in) appears green or disappears. Other endpoints can still see the presentation.

Conditions Issue occurs during a multipoint call where one participant is an IP Phone connected via audio add-in and another endpoint shares a presentation. The IP Phone goes on hold.

Workaround Perform one of the following actions:

1. Unshare, then share the presentation by tapping the **UnShare** option on the Touch Panel, then tapping **Share**.
2. Issue a Hold/Resume sequence from the endpoint that added the audio participant into the call.
3. Disconnect and reconnect the presentation source by unplugging the presentation cable, then plugging it back in.

   If you perform this action before the hold/resume action completes, perform it again after the endpoint resumes the call.
4. Have a non-host site that is not sharing the presentation add the audio-only participant into the call.

CSCug52629

Symptom Main video appears pixelated intermittently during an interop point-to-point call between CTS and EX90, where EX90 is running software release TC6.1.0.

Conditions Interop point-to-point call, where EX90 is running software release TC6.1.0.

Workaround Downgrade EX90 to software release TC6.0.0.

Resolved Caveats in CTS Release 1.10.1

CSCub62170

Symptom The Touch 12 device requires the user to enter a full e-mail address (rather than just a user ID) in order to share Cisco TelePresence Recording Server (CTRS) videos. Entering a partial e-mail address causes an error message to appear.

Conditions Issue occurs on the Touch 12 device, when the user attempts to share CTRS videos without a full e-mail address.

Workaround Enter a full e-mail address, including an at (@) sign, in order to share CTRS videos on the Touch 12.

CSCug02498

Symptom After an EX60 system transfers a Cisco Unified Communication Integration Lync (CUCI Lync) call to CTS 3000, the CTS 3000 does not send video to CUCI Lync.

Conditions Issue occurs during a call between CUCI Lync and CTS 3000.

Workaround There is no workaround.

CSCug57683

Symptom During self-view mode, the right side of the screen appears more blue than the left side.

Conditions Issue occurs during self-view mode.

Workaround There is no workaround.

CSCug77610

Symptom A CTS controlled by Cisco TelePresence Management Suite (TMS) appears unresponsive and/or drops an active call.

Conditions The CTS runs out of memory.

Workaround Manually reboot the system.

Caveats in Cisco TelePresence System Software Release 1.10.0

The following sections show the resolved and unresolved caveats for CTS software release 1.10.0:

- Unresolved Caveats in CTS Release 1.10.0, page 56
- Resolved Caveats in CTS Release 1.10.0, page 58

Unresolved Caveats in CTS Release 1.10.0

CSCtu22483

Symptom A remote CTS endpoint auto-answers an incoming call, even when the present CTS endpoint is configured for the OffNet trunk setting.

Conditions A CTS endpoint configured for the OffNet trunk setting calls another CTS endpoint. This other endpoint auto-answers the call, ignoring the OffNet configuration, which should disable auto-answer.

Workaround There is no workaround.

CSCtz78310

Symptom Cisco Unified Communications Manager (Unified CM) shows the incorrect file name in the Active Load ID field.

Conditions This condition is noticed when you log into Unified CM, navigate to **Device > Phone**, and select your Cisco TelePresence system. The Active Load ID field at the top of the screen shows the image in the factory slot, rather than slot 2.

Workaround To see the correct version of software for your system, log in to your Cisco TelePresence System Administration GUI. The Device Information screen, which is the first screen that you log into, shows you the software image that is loaded in slot 1, slot 2, and the factory slot. The software image that has the asterisk next to it is the software that the system loads after a reboot. Usually, this is the software image in slot 2. This software image is known as the Active Load in Unified CM.

CSCud21801

Symptom If an interop endpoint using Cisco TelePresence MCU calls CTS with muted video and audio, then unmutes after CTS enters the call, CTS drops the call. Issue may occur if the remote MCU endpoint has an audio codec that is in AAC-LD format (RAW or LATM).

Conditions Issue occurs during an interop audio-only call from MCU to CTS, if the MCU audio codec is in AAC-LD format (RAW or LATM).

Workaround Do not make a call with muted video and audio.

CSCue02202

Symptom When an endpoint shares a presentation, then idles for a long period of time, the endpoint "forgets" the presentation and unshares.

Conditions Issue occurs after an endpoint shares a presentation and then idles for a long period of time.

Workaround Unplug the presentation source from the presentation cable, then reconnect it.

CSCuf08035

Symptom On some CTS-3000 systems, the Reverberation test does not record any data.

Conditions Navigate to Troubleshooting > Hardware, then click the CTX Tests tab and the Reverberation radio button. The test does not return any results.

Workaround There is no workaround.

Resolved Caveats in CTS Release 1.10.0

CSCud10852

Symptom CTS cannot view a presentation when one is shared from an EX90 endpoint.

Conditions When an EX90 endpoint shares a presentation with a CTS endpoint during the first 15 seconds of a call, the presentation does not display.

Workaround Share the presentation from the EX90 after the first 15 seconds of the call, or unshare and share presentation after 10 to 20 seconds.

CSCud31953

Symptom During a call between a CTS 3000 system and a TelePresence Server, the CTS 3000 system shows corrupted video.

Conditions Issue occurs during a non-MUX call between a CTS 3000 and a TelePresence server.

Workaround There is no workaround.

CSCud32378

Symptom When a CTS system calls in to MCU auto attendant, the introductory audio message drops after the first few seconds.

Conditions CTS endpoint calls in to MCU auto attendant.

Workaround There is no workaround.

Caveats in Prior CTS Releases

See the Cisco TelePresence Administration Software Release Notes home page on Cisco.com for information about prior CTS releases:

http://www.cisco.com/en/US/products/ps8332/prod_release_notes_list.html

Related Documents

Related Topic	Document Title
Software Documents	
How to configure, troubleshoot, and maintain the CTS using the administration Web interface.	- *Cisco TelePresence System Administration Guide* home page on Cisco.com.
Cisco command-line interface (CLI) information for configuring the Cisco TelePresence System.	- *Cisco TelePresence System Command-Line Interface Reference Guide*.
Cisco TelePresence Administration Software Compatibility Information.	- Cisco TelePresence Software Compatibility Matrix home page on Cisco.com.
How to troubleshoot the Cisco TelePresence System.	- *Cisco TelePresence System Troubleshooting Guide* home page on Cisco.com.
Unified CM configuration with the Cisco TelePresence System.	- *Cisco Unified Communications Manager Configuration Guide for the Cisco TelePresence System*
Cisco Unified Communications Manager Support page.	- Cisco Unified Communications Manager Support
How to use the Cisco TelePresence System, including the CTS Cisco Unified IP Phone.	- *Cisco TelePresence System User Guide*
Cisco TelePresence Touch 12 home page.	- Cisco TelePresence Touch
Cisco Unified IP Phones 7900 Series documentation.	- Cisco Unified IP Phones 7900 Series Maintain and Operate Guides
Cisco TelePresence System (CTS) hardware and software documentation, including information about CTS devices.	- TelePresence - Main Page on Cisco.com
Cisco TelePresence Administration Software documentation and software download page.	- Cisco TelePresence Administration Software
Roadmap of Cisco TelePresence System (CTS) hardware and software installation and configuration documents, including guides to install and operate optional software applications.	- Cisco TelePresence Administration Software Documentation Roadmaps
Cisco TelePresence Manager documentation home page.	- **Cisco TelePresence Manager**
Cisco TelePresence Multipoint Switch home page.	- Cisco TelePresence Multipoint Switch
Cisco TelePresence Recording Server information.	- Cisco TelePresence Recording Server
Cisco TelePresence System system message information.	- *Cisco TelePresence System Message Guide*

Session Initiation Protocol (SIP) page.	• Session Initiation Protocol (SIP)
Cisco TelePresence System EX Series home page.	• Cisco TelePresence System EX Series
Cisco TelePresence Video Communication Server (VCS) home page.	• Cisco TelePresence Video Communication Server (VCS)
Cisco TelePresence System MXP Series home page.	• Cisco TelePresence System MXP Series
Cisco TelePresence Interoperability Database	• Cisco TelePresence Interoperability Database

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.