Cisco IP Conference Phone 8832 Multiplatform Phones Release Notes for Firmware Release 11.3(2)

First Published: 2020-08-17

Release Notes

Use these release notes with the Cisco IP Conference Phone 8832 Multiplatform Phones running SIP Firmware Release 11.3(2).

The following table describes the individual phone requirements.

Phone	Support Requirements
Cisco IP Conference Phone 8832 Multiplatform Phones	BroadSoft BroadWorks 23.0 MetaSphere CFS version 9.5 Asterisk 11.0

Related Documentation

Use the following sections to obtain related information.

Cisco IP Conference Phone 8832 Documentation

See the publications that are specific to your language, phone model, and multiplatform firmware release. Navigate from the following Uniform Resource Locator (URL):

https://www.cisco.com/c/en/us/products/collaboration-endpoints/ip-phone-8800-series-multiplatform-firmware/index.html

New and Changed Features

Access Control to LDAP Directory

You can control access to the LDAP directory on the phone. When you configure the phone with an LDAP directory and leave the user credentials empty, the phone prompts for either the username and password or the client DN and password to access the LDAP directory.

If you configure the user credentials in the administrator web interface or in the configuration file, the user can access the LDAP directory without entering credentials.

Where to Find More Information

- *Cisco IP Conference Phone 8832 Multiplatform Phones Administration Guide*
- *Cisco IP Conference Phone 8832 Multiplatform Phones User Guide*

ACD Feature Sync

You can enable a phone to restore the last local status as ACD initial status or can get the ACD initial status from the server. In the phone administrator web page, you can enable this feature in the **ACD Status** field from **Voice** > **Ext(n)** > **ACD Settings**.

Where to Find More Information

Cisco IP Conference Phone 8832 Series Multiplatform Phones Administration Guide

ACD Status Is Available after Sign-in

You can set the user's Automatic Call Distribution (ACD) status to Available automatically when the user signs in as a call center agent. The user doesn't need to manually set the ACD status to Available on the phone.

To enable this feature, use the **Auto Available After Sign-In** filed under the **ACD Settings** section from **Voice** > **Ext**.

Where to Find More Information

- *Cisco IP Conference Phone 8832 Multiplatform Phones Administration Guide*
- *Cisco IP Conference Phone 8832 Multiplatform Phones User Guide*

Automatic RTP Transport Selection

Your phone now supports automatic RTP (Real-time Transport Protocol) transport selection. A new option **Strict** is added to the **Secure Call Option** parameter. When this paramer is set to **Strict** and SIP transport is set to TLS, it allows SRTP only. If SIP transport is set to UDP/TCP, it allows RTP only.

Where to Find More Information

- *Cisco IP Conference Phone 8832 Multiplatform Phones Administration Guide*

Call Forwarding Enhancements

The enhancements provide a unified interface for the settings of call forwarding on the phone. The call forwarding has the following modes:

- Feature key synchronization (FKS)
- BroadSoft's Extended Services Interface (XSI) Synchronization
- Local

When you enable the settings for certain call forwarding type (such as, call forward all, call forward busy, or call forward no answer), the corresponding menu items display on the phone screen.

You can enable the call forwarding services in the **Supplementary Services** section under **Voice** > **Phone** on the phone web page.

The settings of call forwarding can be synchronized between the server and the phone by the following ways:

1. FKS
2. XSI Synchronization

If you want to make the settings of call forwarding on the local phone take effect, you need to disable FKS and XSI first. The priority of taking effect for call forwarding setting in the supported modes is: FKS > XSI > Local.

Where to Find More Information

- *Cisco IP Conference Phone 8832 Multiplatform Phones Administration Guide*
- *Cisco IP Conference Phone 8832 Multiplatform Phones User Guide*

Directory Enhancements

The phone now supports the following enhancements:

- **All directories** screen: A new phone screen that works as a landing page where users can search contacts from all enabled directories. To enable this feature, use the **Browse Mode Enable** and **Search All Enable** fields under the **Directory Services** section in **Voice** > **Phone** of the phone administration web page. Users press **Contacts** on the phone to access the **All directories** screen.

  You can also control the maximum number of contacts displayed on the **All directories** screen. To configure the maximum number, use the **Max Display Records** field.

- **Category** softkey: From the **All directories** screen, users press the **Category** softkey to display the **Directories** screen with all enabled directories. Users can access a directory from the list and perform further operations, such as to search contacts or to make a phone call.

  

  Note The simple search operation for the BroadSoft directory requires XSI actions version 22.0 or later.

- BroadSoft directory individual mode: This feature toggles the BroadSoft directory mode between the legacy mode and the individual mode. In the legacy mode, only one directory (called “BroadSoft directory”) displays on the phone. In the individual mode, you can choose to enable or disable each type of BroadSoft directory and name each type of the directory. If enabled, users can narrow their search to find their contacts quickly in a specific BroadSoft directory.

  To enable this individual mode, use the **Directory Individual Mode Enable** field from **Voice** > **Phone** > **XSI Phone Service** of the phone administration web page. To manage each type of the BroadSoft directory, use the following fields:

  - **Directory Personal Enable** and **Directory Personal Name**
  - **Directory Group Enable** and **Directory Group Name**
  - **Directory Enterprise Enable** and **Directory Enterprise Name**
  - **Directory GroupCommon Enable** and **Directory GroupCommon Name**
  - **Directory EnterpriseCommon Enable** and **Directory EnterpriseCommon Name**

Where to Find More Information

- *Cisco IP Conference Phone 8832 Multiplatform Phones Administration Guide*
- *Cisco IP Conference Phone 8832 Multiplatform Phones User Guide*

Display Caller Number for a Contact with Unresolved Characters

You can configure the phone to display the caller number instead of an unresolved caller name in the incoming call alerts.

By default, the phone displays both the caller name and the caller number in an incoming call alert. If the phone can't resolve the characters in caller name, the user sees boxes in place of the unresolved characters. If you have unresolved characters, configure the phone to display only the caller number with the **Replace Unresolved Caller Name with Number** field. Locate the field in the **Language** section on the **Voice** > **Regional** tab in the phone web interface.

Where to Find More Information

- *Cisco IP Conference Phone 8832 Multiplatform Phones Administration Guide*
- *Cisco IP Conference Phone 8832 Multiplatform Phones User Guide*

Feature Activation Code Sync

You can now enable feature activation code that synchronizes phone with the server to forward all calls to a destination contact.

To enable the feature, use the **Feature Activation Code Sync** field on the **Voice** > **Ext(n)** tab of the phone administration web page.

You can configure the feature activation code in the **Cfwd All Act Code** field on the **Voice** > **Regional** > **Vertical Service Activation Codes** of the phone administration web page.

Where to Find More Information

- *Cisco IP Conference Phone 8832 Multiplatform Phones Administration Guide*
- *Cisco IP Conference Phone 8832 Multiplatform Phones User Guide*

Firmware Release Numbering Change

Beginning with Firmware Release 11.3.(2), version number of the firmware load file name changes format. The format changes from `xx-x-xMPP-xxx` to `xx-x-xMPPxxxx-xxx`.

The change doesn't impact the firmware releases before 11.3(2). See the following examples for valid firmware versions:

- For firmware releases before 11.3(2):

  sip*yyyy*.*11*-*0*-*1*MPP-*376*

  Where *yyyy* indicates the phone model or phone series; *11* is the major version; *0* is the minor version; *1MPP* is the micro version; and *376* is the build number.

- For firmware release 11.3(2) and later:

sip*yyyy*.*11*-*3*-*2*MPP*0001*-*609*

Where *yyyy* indicates the phone model or phone series; *11* is the major version; *3* is the minor version; *2MPP0001* is the micro version; and *609* is the build number.

The change is in the micro version number. For the first release of Firmware 11.3(2), *0001* is appended to the micro version number. This change impacts firmware upgrade and firmware version comparison.

Where to Find More Information

Cisco IP Conference Phone 8832 Multiplatform Phones Administration Guide

ICE Implementation on MPP

Implementation of Interactive Connectivity Establishment (ICE) on Multiplatform Phones (MPP) provides the most optimized and direct media path for audio and video calls. Before this implementation, the media path traversed through a cloud-hosted media server. With ICE, the resources used by the media relay nodes are reduced by 90%. When you enable ICE, all Webex calls with MPP phones negotiate the most optimized path with this feature.

To configure this feature you modify the database at a tenant or device level. Only Cisco Service Readiness Engineering (SRE) team can modify this feature. MPP supports full ICE mode as per RFC-5245.

To enable ICE on MPP, the variable **`ICE_STUN_Enable`** in the device profile is modified with the following syntax.

```
<STUN_Enable ua="na">Yes</STUN_Enable>

<ICE_STUN_Enable ua="na">Yes</ICE_STUN_Enable>

<STUN_Server ua="na">10.89.68.76</STUN_Server>
```

The configuration variable `ICE_STUN_Enable` is hidden on the phone web interface. The others are shown on the phone web interface.

This feature cannot be configured or modified from the phone web interface. The end user can't modify this feature.

LDAP Cache for SIP User Credentials

The phone now saves the LDAP user credentials in a local cache when the credentials are configured manually on the phone, administration web page, or phone configuration XML file (cfg.xml). In addition to the host user of the phone, the LDAP cache mechanism is also applicable for the users who sign into the phone with the Flexible Seating or Extension Mobility feature.

The cached LDAP user credentials are associated with the SIP user ID. When a user accesses the LDAP directory, the phone checks the LDAP cache to locate the user's credentials. If the credentials are found in the cache, the user can access the LDAP directory without the need to sign in.

The phone can save up to 50 user credentials. The phone removes the least-used credentials when the cache size limit is reached.

Where to Find More Information

- *Cisco IP Conference Phone 8832 Multiplatform Phones Administration Guide*
- *Cisco IP Conference Phone 8832 Multiplatform Phones User Guide*

LDAP StartTLS Support

The phone now supports Start Transport Layer Security (StartTLS) for the communications between the phone and the LDAP server. StartTLS begins as a plain text connection over the standard LDAP port. It provides the flexibility for encrypted or unencrypted communications according to the actual situation of the LDAP server. If the server supports to upgrade the connection to TLS, then StartTLS encrypts the communications using TLS. Otherwise, the communications are unencrypted, for example, in plaintext.

To enable this feature, use the **StartTLS Enable** field under the **LDAP** section in **Voice** > **Phone** of the phone administration web page.

Where to Find More Information

- *Cisco IP Conference Phone 8832 Multiplatform Phones Administration Guide*

Menu Visibility Configuration

You can configure the phone to:

- show or hide specific menu items on the phone screen.
- enable or disable the personal directory.
- enable or disable the ability to search for contacts in all the directories.

By default, all the menu items, the personal directory, and the feature of contact search in all directories are available to users. You can hide particular items with the fields in the **Menu Visibility** and **Directory Services** sections on the **Voice** > **Phone** tab in the phone web interface.

If you hide a menu item, it doesn't display on the phone screen. If you disable the personal directory, users can't see **Personal address book** on the phone screen or the **Personal Directory** tab in the phone web interface. In this case, users can't add contacts from the call history. If you disable the contact search in all directories, users can only search for contacts in a selected directory, instead of all the directories.

Where to Find More Information

- *Cisco IP Conference Phone 8832 Multiplatform Phones Administration Guide*
- *Cisco IP Conference Phone 8832 Multiplatform Phones User Guide*

Reverse Name Lookup for Inbound Calls using Broadsoft Directories

The reverse name lookup searches the phone's external directories. When a search succeeds, the name is placed in the call session and in the call history. For simultaneous multiple phone calls, reverse name lookup searches for a name to match the first call number. When the second call connects or is placed on hold, reverse name lookup searches for a name to match the second call. The reverse lookup searches the external directories for 8 secs, if in 8secs there is no result found, there will be no display of the name. If a result is found in 8secs, the name is diplayed on the phone. The external directory search priority order is : **BroadSoft(XSI) > LDAP > XML**.

Where to Find More Information

Cisco IP Conference Phone 8832 Series Multiplatform Phones Administration Guide

Reverse Name Lookup for Local Directory

This feature enables to do a reverse name lookup against local contacts for BroadWorks server call logs. If the call number of server call logs matches that in the local directory, the call name of server call logs will be replaced with contact name in the local directory. Also, if the call number does not match any entry in local directory, the call number will do caller id mapping and lookup the local directory again.

Where to Find More Information

- *Cisco IP Conference Phone 8832 Multiplatform Phones Administration Guide*
- *Cisco IP Conference Phone 8832 Multiplatform Phones User Guide*

SIP Proxy Redundancy Enhancement

The SIP Proxy Redundancy enhancements are:

- Increase support for up to six NAPTR records and six SRV records in a DNS query
- Add ability to seamless switch between different SIP transport protocols during server failover and failback
- Add ability to disable SIP proxy failback. Set the **Proxy Fallback Intvl** parameter to `0` in the phone web interface or the configuration file.
- Retain an active call on the fallback server until after the call completes. After the call completes, if the primary server is available and the failback conditions are met, then perform the failback.

Where to Find More Information

Cisco IP Conference Phone 8832 Multiplatform Phones Administration Guide

User Access Authentication Control to Phone Menus

You can configure if user requires authentication to access phone menus, softkeys, and buttons. You can customize the authentication control from the **Require Authentication for LCD Menu Access** parameter on the **Voice** > **Phone** of the phone administration web page.

Where to Find More Information

- *Cisco IP Conference Phone 8832 Multiplatform Phones Administration Guide*
- *Cisco IP Conference Phone 8832 Multiplatform Phones User Guide*

Upgrade the Firmware

You can upgrade the phone firmware with TFTP, HTTP, or HTTPS. After the upgrade completes, the phone reboots automatically.

Before you begin

To avoid an upgrade failure, first upgrade the phone firmware to **11.3.1 MSR2-6**.

For more information, see Cisco IP Conference Phone 8832 Multiplatform Phones Release Notes for Firmware Release 11.3(1)SR2.

This issue typically occurs when you upgrade the phone firmware from one of the following versions to 11.3.2:

- 11.2.3
- 11.2.3 MSR1-1
- 11.3.1
- 11.3.1 MSR1-3

Procedure

Step 1 Click this link:

https://software.cisco.com/download/home/286311392

On the **Software Download** web page that is displayed, ensure that **IP Phone 8800 Series with Multiplatform Firmware** is selected in the middle pane.

Step 2 Select **IP Conference Phone 8832 with Multiplatform Firmware** in the right pane.

Step 3 On the next page that is displayed, select **Multiplatform Firmware**.

Step 4 Under **Latest Release**, select **11.3.2**.

Step 5 (Optional) Place your mouse pointer on the file name to see the file details and checksum values.

Step 6 Download the corresponding file.

`cmterm-8832.11-3-2MPP0001-609_REL.zip`

Step 7 Click **Accept License Agreement**.

Step 8 Unzip the file and place the files in the appropriate location on your upgrade server.

The appropriate location is the TFTP, HTTP, or HTTPS download folder, depending on the protocol that you want to use for the upgrade.

Note If you miss the step to upgrade the phone firmware to **11.3.1 MSR2-6**, then you must place the file under the root directory of the TFTP, HTTP, or HTTPs upgrade server.

Example:

`http://10.73.10.223/sip8832.11-3-2MPP0001-609.loads`

If the file is placed under a non-root directory of the upgrade server, the upgrade fails.

Example:

`http://10.73.10.223/firmware/sip8832.11-3-2MPP0001-609.loads`

Step 9 Upgrade the phone firmware with one of these methods.

- Upgrade the phone firmware from the phone administration web page:
  a. On the phone administration web page, go to **Admin Login** > **Advanced**, **Voice** > **Provisioning** > **Firmware Upgrade**.
  b. In the **Upgrade Rule** field, enter the load file URL as described below.

     Load file URL format:

`<upgrade protocol>://<upgrade server ip address>[:<port>]>/<file name>.loads`

Examples:

`http://10.73.10.223/sip8832.11-3-2MPP0001-609.loads`

`https://server.domain.com/sip8832.11-3-2MPP0001-609.loads`

c. Click **Submit All Changes**.

- Upgrade the phone firmware directly from your web browser:

  In the address bar of your web browser, enter the phone upgrade URL as described below.

  Phone upgrade URL format:

  `<phone protocol>://<phone ip address>[:<port>]/admin/upgrade?<load file URL>`

  Load file URL format:

  `<upgrade protocol>://<upgrade server ip address>[:<port>]/<file name>.loads`

  Examples:

  `https://10.74.10.225/admin/upgrade?http://10.73.10.223/sip8832.11-3-2MPP0001-609.loads`

  `https://10.74.10.225/admin/upgrade?https://server.domain.com/firmware/sip8832.11-3-2MPP0001-609.loads`

Note Specify the `<file name>.loads` file in the URL. The `<file name>.zip` file contains other files.

Limitations and Restrictions

Phone Behavior During Times of Network Congestion

Anything that degrades network performance can affect phone audio and, in some cases, can cause a call to drop. Sources of network degradation can include, but are not limited to, the following activities:

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

Cisco IP Conference Phone 8832 Upgrade Workaround (CSCvt24809)

This Cisco IP Conference Phone 8832 fails to upgrade from 11.2.3, 11.2.3 MSR1-1, 11.3.1, or 11.3.1 MSR1-3 to 11.3.2. When the upgrade failure occurs, you receive one of the following error messages:

- `Upgrade Failed. Reason: File not found`
- `Upgrade Failed. Reason: Unknown error`

To fix this issue, use one of the following methods:

- Place the upgrade file (.loads) under the root directory of the TFTP, HTTP, or HTTPs server.

  For example, `http://10.73.10.223/sip8832.11-3-2MPP0001-609.loads`

- First upgrade the firmware of Cisco IP Conference Phone 8832 to 11.3(1) SR2, then upgrade the firmware to 11.3.2.

Multicast Paging Scripts Change to Empty after the Upgrade (CSCvu23613)

The default values of multicast paging scripts change from 800 to empty automatically after the upgrade to 11.3.2.

This behaviour typically occurs if the multicast paging scripts were not modified before the upgrade.

This behaviour doesn't occur if you have previously changed the multicast paging scripts to non-default values before the upgrade.

On the phone administration web page, you can check the values of multicast paging scripts from **Voice** > **Phone** > **Multiple Paging Group Parameters**.

After the upgrade, if you want to use the default values in the previous releases, you can configure the parameters on the administration web page.

The following list shows the default values of the multicast paging scripts in the previous releases:

- Before 11.3(1) firmware releases, the default values are:

  ```
  pggrp=224.168.168.168:34560;name=All;num=800;listen=yes;
  ```

- In 11.3(1) firmware release, the default values are:

  ```
  pggrp=224.168.168.168:34560;name=Group_1;num=800;listen=yes;pri=1;codec=g722
  ```

You can also configure the parameter in the phone configuration file with XML(cfg.xml) by entering a string in this format:

- `<Group_1_Paging_Script ua="na">pggrp=224.168.168.168:34560;name=All;num=800;listen=yes;</Group_1_Paging_Script>`
- `<Group_1_Paging_Script ua="na">pggrp=224.168.168.168:34560;name=GroupA;num=800;listen=yes;pri=1;codec=g711a;</Group_1_Paging_Script>`

Caveats

View Caveats

You can search for caveats (bugs) with the Cisco Bug Search tool.

Known caveats are graded according to severity level, and are either open or resolved.

Before you begin

You have your Cisco.com user ID and password.

Procedure

Step 1 Click one of the following links:

- To view all caveats that affect this release:

  https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286319904&rls=11.3(2)&sb=anfr&bt=custV
- To view open caveats that affect this release:

  https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286319904&rls=11.3(2)&sb=anfr&sts=open&bt=custV
- To view resolved caveats that affect this release:

  https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286319904&rls=11.3(2)&sb=anfr&sts=fd&bt=custV

Step 2 When prompted, log in with your Cisco.com user ID and password.

Step 3 (Optional) For information about a specific caveat, enter the bug ID number (*CSCxxnnnnn*) in the **Search for** field, and press **Enter**.

Open Caveats

The following list contains the severity 1, 2, and 3 defects that are open for the Cisco IP Conference Phone 8832 Multiplatform Phones that use Firmware Release 11.3(2).

For more information about an individual defect, you can access the online history for the defect by accessing the Bug Search tool and entering the Identifier (*CSCxxnnnnn*). You must be a registered `cisco.com` user to access this defect information.

Because the defect status continually changes, the list reflects a snapshot of the defects that were open at the time this report was compiled. For an updated view of the open defects or to view specific bugs, access the Bug Search Toolkit as described in View Caveats, on page 10.

- CSCvv29937 Incoming Display ID shows incorrect value if PAB entry is deleted
- CSCvv20301 POR: Not all characters are shown in the character preview pop-up
- CSCvv19782 Phone can't send publish if Voice Quality Report Address is proxy domain+port
- CSCvv15154 When phone playing hold remind and have an incoming call,both hold remind and ringer not played
- CSCvv15106 bwks anywhere char encoding mismatch
- CSCvv32982 LDAP sing-in window is not popped up when using or psk in legacy mode
- CSCvv33336 Reverse name lookup against BS Dir failed if more than 1 results are received

Resolved Caveats

The following list contains the severity 1, 2, and 3 defects that are resolved for the Cisco IP Conference Phone 8832 Multiplatform Phones that use Firmware Release 11.3(2).

For more information about an individual defect, you can access the online history for the defect by accessing the Bug Search tool and entering the Identifier (*CSCxxnnnnn*). You must be a registered `Cisco.com` user to access this defect information.

Because the defect status continually changes, the list reflects a snapshot of the defects that were resolved at the time this report was compiled. For an updated view of the resolved defects or to view specific bugs, access the Bug Search Toolkit as described in the View Caveats, on page 10.

- CSCvr86301 Remote SDK: WebSocket Control Server URL waits 10 seconds after HTTP 401 Challenge
- CSCvs01888 CP-88xx-3PCC When Answer confirmation is set to ON there is one-way audio
- CSCvs31198 480 timeout value in Cadence tag is hardcoded to 60 seconds when infinite value is set
- CSCvt13644 88xx Voice Feedback Disables After Reboot if UI-User-Mode is Enabled
- CSCvt52323 Different select behaviour between softkey + circular select button - using XSI recents from server
- CSCvt52122 MPP phones - Transferor hears busy signal during consultative transfer
- CSCvs88350 MPP phones Multicast Paging Ended By Itself
- CSCvs31890 Multiple Vulnerabilities in linux_kernel
- CSCvs31786 Multiple Vulnerabilities in linux_kernel
- CSCvr61497 Upgrade libpcap to 1.9.1 and tcpdump to 4.9.3
- CSCvs54502 3pcc-8800: phone restarts when an incoming call arrive at second line
- CSCvs44645 Multiple Vulnerabilities in linux_kernel
- CSCvs35094 Linux Kernel i2400m_op_rfkill_sw_toggle() Function Memory Leak Denial of Service Vulnerability
- CSCvt26123 Evaluation of 8800 for expired certificates
- CSCvt79137 Multiple Vulnerabilities in linux_kernel
- CSCvs35121 Linux Kernel ath9k_wmi_cmd() Function Memory Leak Denial of Service Vulnerability
- CSCvs35119 Multiple Vulnerabilities in linux_kernel
- CSCvs62320 Multiple Vulnerabilities in linux_kernel
- CSCvs35092 Multiple Vulnerabilities in linux_kernel
- CSCvs44650 Linux Kernel vcs_write Write Access Prevention Vulnerability
- CSCvt26126 Evaluation of 8832 for expired certificates
- CSCvu57297 Multiple Vulnerabilities in linux_kernel
- CSCvu31850 Set_Local_Date and Set_Local_Time not Taking Effect
- CSCvu20649 MPP phones - unable to activate via device activation code
- CSCvs31788 Linux Kernel drivers/net/wireless/ath/ath9k/htc_hst.c Memory Leak Denial of Service Vulnerability
- CSCvt06292 Linux Kernel vc_do_resize Function Use-After-Free Vulnerability

- CSCvt50003 MPP phones listen to multicast paging group '800' by default
- CSCvu29263 Multiple Vulnerabilities in linux_kernel
- CSCvs70834 LDAP reverse lookup not pulling info from LDAP server on incoming INVITE
- CSCvs59424 3pcc-88xx: Phone is not uploading the config when Report To Server is set to On Local Change
- CSCvs54500 Error prompt during Profile Account Setup and default input alphanumeric
- CSCvu29265 Multiple Vulnerabilities in linux_kernel
- CSCvu88718 Call Filter In Settings Always Be Off
- CSCvu50856 libcurl curl_easy_unescape Heap Overflow Remote Code Execution Vulnerability
- CSCvu33942 Language Reverts to English After Reboot if Locale Server Connection is Lost
- CSCvv03397 MPP phones - when callee pauses recording caller can hear callee but callee does not hear caller

Cisco IP Phone Firmware Support Policy

For information on the support policy for phones, see https://cisco.com/go/phonefirmwaresupport.

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 following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

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.

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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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: https://www.cisco.com/c/en/us/about/legal/trademarks.html. 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. (1721R)