

# Cisco Wireless IP Phone 8821 Release Notes for Firmware Release 11.0(5)

**First Published:** 2019-04-11

**Last Modified:** 2020-08-12

## Cisco Wireless IP Phone 8821 Release Notes for Firmware Release 11.0(5)

These release notes support the Cisco Wireless IP Phone 8821 Firmware Release 11.0(5).

The following table describes the systems and versions that the phone requires.

System	Minimum Version	Recommended Versions
Cisco Unified Communications Manager	9.1(2)	10.5(2), 11.0(1), 11.5(1), and later
Cisco Unified Communications Manager Express	10.5 through Fast Track	11.0, 11.5, 11.7 (native support), and later
Cisco Unified Survivable Remote Site Telephony	10.5	11.0, 11.5, 11.7, and later
Cisco Wireless LAN Controller	8.0.121.0	8.0.152.0, 8.2.170.0, 8.3.143.0, 8.5.140.0, 8.8.120.0
Cisco IOS Access Points (Autonomous)	12.4(21a)JY	12.4(25d)JA2, 15.2(4)JB6, 15.3(3)JF1
Cisco Meraki	MR 25.9, MX 13.33	MR 25.11, MX 13.33

### New and Changed Features

The following sections describe the features that are new or have changed in this release.



**Note** Some features may require the installation of a Cisco Unified Communications Manager Device Package. Failure to install the Device Package before the phone firmware upgrade may render the phones unusable.

### Features Available with the Firmware Release

The following sections describe the features available with the Firmware Release.

## New Chargers for the Cisco Wireless IP Phone 8821

The Cisco Wireless IP Phone 8821 Desktop Charger and Cisco Wireless IP Phone 8821 Multi Charger are improved. The new versions charge the Cisco Wireless IP Phone 8821 battery to a higher level to improve the talk time.

The new chargers look similar to the old versions. The new chargers have these visual clues to differentiate them from the old chargers:

- Desktop charger: has the voltage label “4.35V Battery Charging” on the back.
- Multicharger: has the voltage label “4.35V Battery Charging” on the back.

The following table shows the differences in talk time when you use the new desktop charger and multicharger.

**Table 1: Comparison of Talk Times**

Condition	Original Chargers	New Chargers
Phone charged in charger, with wall adapter, or with USB Phone running Firmware Release 11.0(4)SR3 or earlier	9.5 hours	9.5 hours
Phone charged in charger, with wall adapter, or with USB Phone running Firmware Release 11.0(5) or later	11.5 hours	11.5 hours
Spare battery charged in the charging slot	9.5 hours	11.5 hours

### Where to Find More Information

- *Cisco Wireless IP Phone 8821 and 8821-EX Accessory Guide*
- *Cisco Wireless IP Phone 8821 and 8821-EX Administration Guide*
- *Cisco Wireless IP Phone 8821 and 8821-EX User Guide*

## Features Available with the Latest Cisco Unified Communications Manager Device Pack

The following sections describe features in the release which require the new firmware and the latest Cisco Unified Communications Manager Device Pack. The applicable device packs are released after the firmware release.

For information about the Cisco Unified IP Phones and the required Cisco Unified Communications Manager device packs, see the following URL:

[http://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cucm/compat/devpack\\_comp\\_mtx.html](http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/compat/devpack_comp_mtx.html)

## Configuration Field Changes

This feature adds new fields to support new features and removes several fields because they are no longer required. These fields display in the **Product Specific Configuration Layout** pane of the following pages of the Cisco Unified Communications Manager Administration:

- **Device > Phone**
- **Device > Device Settings > Common Phone Profile**

The following fields are new:

- Customer Support Upload URL. For more information, see [Serviceability Enhancements, on page 4](#).
- Disable TLS 1.0 and TLS 1.1 for Web Access. For more information, see [Security Enhancements, on page 3](#).
- Divert Alerting Call. For more information, see [User Interface Enhancements, on page 4](#).
- Allow Vibrate URI When On Call. For more information, see [User Interface Enhancements, on page 4](#).

The following fields are no longer displayed:

- WLAN Profile 1 prompt mode
- Local Contacts Access
- Favorites Access
- IPv6 Log Server
- FIPS Mode
- IPv6 Load Server
- Detect Unified CM Connection Failure
- Simplified New Call UI

### Where to Find More Information

*Cisco Wireless IP Phone 8821 and 8821-EX Administration Guide*

## Security Enhancements

You can improve security over phones that act as an HTTPS server. With the parameter **Disable TLS1.0 and TLS1.1 for web access**, you can apply TLS1.0, TLS1.1, and TLS 1.2 mode, or just TLS 1.2 mode to any phone, or group of phones that function as an HTTPS server.

For other configurations, you configure TLS protocols on the Cisco Unified Communications Manager. As of Cisco Unified Communications Manager Release 12.0, there are TLS settings configured by a CLI command. See *Release Notes for Cisco Unified Communications Manager and IM & Presence Service, Release 12.0(1)* for information about new CLI commands on Cisco Unified Communications Manager.

You set the **Disable TLS1.0 and TLS1.1 for web access** field in the Product Specific Configuration Layout pane of your Cisco Unified Communications Manager. Install the latest device package for this feature to function.

The ability to disable TLS1.0 and TLS1.1 is supported on Cisco Unified Communications Manager Release 11.5(1)SU3 and later.

Also included in this feature are:

- Support for the Cisco Discovery Protocol (CDP).
- Removal of all the IPv6 configuration fields displayed on Cisco Unified Communications Manager and on the phone.

### Where to Find More Information

- *Cisco Wireless IP Phone 8821 and 8821-EX Administration Guide*

## Serviceability Enhancements

You can support your users with these new functions:

- You can use the Audio Diagnostics function to troubleshoot audio problems.
- You can configure Problem Report Tool (PRT) reports to automatically upload to a remote server.
- You can request a PRT with the X/Open System Interface (XSI) CiscoIPPhoneExecute object.
- You can request a PRT from the phone administration web page.
- You can generate and delete Java core dumps from the phone administration web page.

### Where to Find More Information

- *Cisco Wireless IP Phone 8821 and 8821-EX Administration Guide*
- *Cisco Unified IP Phone Services Application Development Notes for Cisco Unified Communications Manager and Multiplatform Phones*

## User Interface Enhancements

You control the following user interface changes:

- You can control if the **Decline** softkey displays when the users have incoming calls.  
To support the **Decline** function, you set the **Divert Alerting Call** field in the **Product Specific Configuration** pane of the Cisco Unified Communications Manager Administration **Device > Phones** page.
- You can control if an active phone can vibrate when it receives the Vibrate URI command in an XSI message. By default, the phone doesn't vibrate.  
To enable phones to vibrate, you enable the **Allow Vibrate URI When On Call** field in the **Product Specific Configuration** pane of the Cisco Unified Communications Manager Administration **Device > Phones** page.
- Battery information displays in the phone web page and in the Status menu on the phone.

Users will experience the following changes:

- When the phone is in the Cisco Wireless IP Phone 8821 Desktop Charger, the ringer can now be set to a higher volume level.
- The header row of the screen can display the battery charge level as a percentage beside the generic icons. The field **Battery percentage** in the **Settings** menu on the phone controls the display of the percentage charge level.
- Users can add or update local contacts from the **Recents** app.
- Users see the **Favorites** softkey on the main screen for quick access to the Favorites list. The Favorites list is also available from the **Contacts** app.
- In the Local contacts list, users see the Delete option when they highlight a contact and press **More** . In the previous release, the Delete option was only available on the **Details** screen.

Entries in the phone configuration menus and the phone web page related to IPv6 don't display. The phone doesn't support IPv6.

#### Where to Find More Information

- *Cisco Wireless IP Phone 8821 and 8821-EX Administration Guide*
- *Cisco Wireless IP Phone 8821 and 8821-EX User Guide*

## User Guide Improvements for the Visually-Impaired

Users who are visually-impaired or blind can now read the *Cisco Wireless IP Phone 8821 and 8821-EX User Guide* using a JAWS® reader. The online HTML version of the document includes alternate text to the graphics and other improvements.

## Related Documentation

Use the following sections to obtain related information.

### Cisco Wireless IP Phone 882x Series Documentation

Refer to publications that are specific to your language, phone model, and call control system. Navigate from the following documentation URL:

<https://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/tsd-products-support-series-home.html>

The Deployment Guide is located at the following URL:

<https://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-implementation-design-guides-list.html>

### Cisco Unified Communications Manager Documentation

See the *Cisco Unified Communications Manager Documentation Guide* and other publications that are specific to your Cisco Unified Communications Manager release. Navigate from the following documentation URL:

<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html>

## Cisco Unified Communications Manager Express Documentation

See the publications that are specific to your language, phone model and Cisco Unified Communications Manager Express release. Navigate from the following documentation URL:

<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-express/tsd-products-support-series-home.html>

## Installation

### Installation Requirements

Before you install the firmware release, you must ensure that your Cisco Unified Communications Manager is running the latest device pack. The applicable device packs are released after the firmware release. After you install a device pack on the Cisco Unified Communications Manager servers in the cluster, you need to reboot all the servers.



**Note** If your Cisco Unified Communications Manager does not have the required device pack to support this firmware release, the firmware may not work correctly.

For information on the Cisco Unified Communications Manager Device Packs, see [http://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cucm/compat/devpack\\_comp\\_mtx.html](http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/compat/devpack_comp_mtx.html).

### Install Firmware Release 11.0(5) on Cisco Unified Communications Manager

Before you can use the phone firmware release on the Cisco Unified Communications Manager, you must install the latest Cisco Unified Communications Manager firmware on all Cisco Unified Communications Manager servers in the cluster.

#### Procedure

- 
- Step 1** Go to the following URL:  
<http://software.cisco.com/download/navigator.html?mdfid=284883944&i=rm>
- Step 2** Choose **Cisco IP Phone 8800 Series**.
- Step 3** Choose **Cisco Wireless IP Phone 8821**.
- Step 4** Choose **Session Initiation Protocol (SIP) Software**.
- Step 5** In the **Latest Releases** folder, choose **11.0(5)**.
- Step 6** Select the firmware file, click the **Download** or **Add to cart** button, and follow the prompts.  
Firmware file: cmterm-8821-sip.11-0-5-17.k3.cop.sgn
- Note** If you added the firmware file to the cart, click the **Download Cart** link when you are ready to download the file.
- Step 7** Click the + next to the firmware file name in the Download Cart section to access additional information about this file. The hyperlink for the readme file is in the Additional Information section, which contains installation instructions for the corresponding firmware.

- Step 8** Follow the instructions in the readme file to install the firmware.
- 

## Install Firmware Release 11.0(5) on Cisco Communications Manager Express

You must download the Cisco Wireless IP Phone 8821 firmware image file from the software download center.

For information on Cisco Unified Communications Manager Express support, see [http://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cucme/feature/phone\\_feature/phone\\_feature\\_support\\_guide.html](http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucme/feature/phone_feature/phone_feature_support_guide.html).

For more information about this procedure, refer to the “Install and Upgrade Cisco Unified CME Software” chapter in the *Cisco Unified Communications Manager Express System Administrator Guide* at this URL:

[http://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cucme/admin/configuration/manual/cmeadm.html](http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucme/admin/configuration/manual/cmeadm.html)

### Procedure

---

- Step 1** To access the firmware files, go to this URL:  
<https://software.cisco.com/download/navigator.html?mdfid=284729655&flowid=75283>
- Step 2** Choose **Cisco Wireless IP Phone 8821**.
- Step 3** Choose **Session Initiation Protocol (SIP) Software**.
- Step 4** Choose **11.0(5)** in the **Latest Releases** folder.
- Step 5** Click **Download** or **Add to cart** and follow the prompts.  
The file to download is `cmterm-8821.11-0-5-17.zip`
- Step 6** Extract the files from the zip file, manually copy them to the Cisco Unified Communications Manager Express TFTP server (router flash), and enable them for TFTP.
- 

## 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

### Health-Care Environment Use

This product is not a medical device and uses an unlicensed frequency band that is susceptible to interference from other devices or equipment.

## Recording Tone Volume Limitation

If you use the recording feature, we recommend that you change the Recording Tone Local Volume configured in Cisco Unified Communications Manager. Change the field from the default of 100 to 20.

The CUCM device packs (October 2017 and later) have the default set to 20.

For more information, look at CSCvc14605 using <https://tools.cisco.com/bugsearch>.

## TLS 1.2 Tunnel Limitation with ISE 2.0 to 2.3

To support a TLS 1.2 tunnel between the phone and the Cisco Identity Service Engine (ISE) server, the ISE patch to resolve [CSCvm03681](#) must be applied. This patch is required for ISE servers running Release 2.0 to 2.3; ISE Release 2.4 and later include the patch.

## Caveats

### View Caveats

You can search for caveats using the Cisco Bug Search tool.

Known caveats (bugs) are graded according to severity level, and can be either open or resolved.

### Before you begin

To view caveats, you need the following items:

- Internet connection
- Web browser
- Cisco.com user ID and password

### Procedure

---

- Step 1** Perform one of the following actions:
- Use this URL for all caveats:  
<https://bst.cloudapps.cisco.com/bugsearch/search?kw=&pf=prdNm&pfVal=286308995&rls=11.0%285%29&sb=anfr&bt=custV>
  - Use this URL for all open caveats:  
<https://bst.cloudapps.cisco.com/bugsearch/search?kw=&pf=prdNm&pfVal=286308995&rls=11.0%285%29&sb= afr&bt=custV>
  - Use this URL for all resolved caveats:  
<https://bst.cloudapps.cisco.com/bugsearch/search?kw=&pf=prdNm&pfVal=286308995&rls=11.0%285%29&sb=fr&bt=custV>
- Step 2** When prompted, log in with your Cisco.com user ID and password.
- Step 3** (Optional) Enter the bug ID number in the Search for field, then press **Enter**.
-

## Open Caveats

The following list contains the severity 1, 2, and 3 defects that are open for the Cisco Wireless IP Phone 8821 that use Firmware Release 11.0(5).

For more information about an individual defect, you can access the online record for the defect from the Bug Search Toolkit. You must be a registered Cisco.com user to access this online information.

Because 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 open defects or to view specific bugs, access the Bug Search Toolkit as described in [View Caveats, on page 8](#).

- CSCuw10789 Configuration: RTP/sRTP Port Range Configuration
- CSCvh27418 Transfer soft key shall be grey before C answer while semi-transfer is disabled
- CSCvh47665 No Secure tone played on protected phones while enable speaker
- CSCvi80433 Phone doesn't process the EAP request frame, causing de-registration
- CSCvj31950 Intermittent "\"Device or resource busy\" can still happen
- CSCvk22665 8821 display comes on sometimes when on call with shared line
- CSCvk59324 CCKM roaming failure then call dropped on roaming stress test bed
- CSCvm04637 Continuous scan busy is reproducible on Conducted test bed
- CSCvm58907 Firmware sometimes couldn't complete the fresh association
- CSCvm66028 Phone will eventually loose WiFi when roaming between 2 AP's set at 80MHz/40MHz
- CSCvm69293 Network configuration info not displayed on current wlan profile
- CSCvm74978 8821 phone sometimes couldn't receive the EAP identity request on 2.4G JFW test bed.
- CSCvm87368 Phone can't get ip address when DHCP option 150 field configured with MaxLength
- CSCvm91475 Can't answer incoming call for a while when hold reversion is 20s with about 20 call sessions
- CSCvm94269 DTIM period in WLAN Diags shows as 3 sometimes
- CSCvn81608 Java process sometimes has significant delay in receiving events from wlanmgr after OOR & In Range
- CSCvm95611 XML message does not display on lock screen if http url priority is 1 or 2
- CSCvn41362 cp8821: "\"CAL Text#\" displayed in "\"incoming call toast\""
- CSCvn43154 No "\"details\" softkey in multi-leg call history
- CSCvo03077 Conference call still in held mode when all the other parties ended the call
- CSCvo26159 8821 failing to roam flexconnect over the air after reassoc\_resp it tries to auth with previous AP
- CSCvo30508 Softkey options shouldn't be shown in line missed calls page if blank
- CSCvo32881 Both speaker icon displayed when setting auto answer with speaker on shared line
- CSCvo44285 Multiple Vulnerabilities in qt

- CSCvo45817 Multiple Vulnerabilities in curl
- CSCvo88229 GNU C Library parse\_reg\_exp Denial of Service Vulnerability

## Resolved Caveats

The following list contains the severity 1, 2, and 3 defects that are resolved for the Cisco Wireless IP Phone 8821 that use Firmware Release 11.0(5).

For more information about an individual defect, you can access the online record for the defect from the Bug Search Toolkit. You must be a registered Cisco.com user to access this online information.

Because 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 resolved defects or to view specific bugs, access the Bug Search Toolkit as described in [View Caveats, on page 8](#).

- CSCvh15285 DNS info got lost after phone power off/on when DHCP in off status
- CSCvh27809 Focus and soft key error while press up-down hard key during conference
- CSCvh38919 8821: Speaker fail to ring when insert headset
- CSCvh50578 Pressing red button can not cancel new call when PTT is opened
- CSCvh50994 No error toast prompts while cBarge failed due to maximum participants has been reached
- CSCvh89574 Pressing Green button to make a call - missing in PD/CD & Line View
- CSCvh99185 WLAN diags AP details only shows channels 36-48
- CSCvi24947 Display will not off while phone has one-way incoming intercom call
- CSCvi66235 PB: When configuring a Favorite, middle button can dial number by mistake when in Contact details
- CSCvi66773 PB: Pressing green button should not bring up call view when highlight on Unassigned
- CSCvi68937 8821 advertises dongle MAC instead of phone MAC via CDP
- CSCvi78358 8821 can't save debug command after reset or power-cycle
- CSCvj02218 Park resume is greyed out in 8821 registered in CME
- CSCvj07546 Phone de-registered due to re-IP during overnight testing
- CSCvj23342 Call could be dropped when OOR more than 1 minute
- CSCvj42007 DUT don't vibrate sometimes when pickup call with DND enable
- CSCvj43956 New call soft key not work while focus on BLF speed dial
- CSCvj44014 Back from intercom call details, phone's UI turn to blank
- CSCvj45498 Ringer shouldn't play thru headset in Australia network locale when inserting headset during ringing
- CSCvj46981 "Battery charging\" toast not display when power charging with USB cable.
- CSCvj47001 Ringer for incoming call switches to headset after docked when ringer output is set to speaker

- CSCvj53208 White screen flash while charging powered off phone
- CSCvj54504 Blank call view after end the call on one line and then resume call on another line
- CSCvj54731 Should delay ringer output for 4 sec if 2nd call comes in immediately after 1st call is ended
- CSCvj55168 ip can be pinged after dhcp address released through \"wifi interface\"
- CSCvj55253 Can't move focus to other lines with nav-button when phone is in dialing.
- CSCvj64735 Voicemail icon shows on the second line and intercom line even there is only vm on first line
- CSCvj70382 Back to use correct username from wrong one, phone failed to connect to Auto AP with EAP-FAST
- CSCvj75229 Phone does not re-connect to first WLAN profile after disable/enable
- CSCvj84131 Decline not work on the line not configured to VM, when another line configured to VM
- CSCvj88754 Failed to Log Out from personal directory
- CSCvj94399 Sometimes(90%) ringer is very small in hold reversion state when ringer volume is maximized
- CSCvj94952 On Phone's LCD, the DN has not been changed after access hCluster successfully with EMCC method
- CSCvj96861 Application Button still works when DUT is not idle Although button priority is low
- CSCvk03109 When DNR is enabled and a higher priority MLPP call comes in, the ringer is not played on the phone.
- CSCvk09649 Incoming call will be auto answered when connect bluetooth headset to phone and hold the first call.
- CSCvk21292 8821 sipcc keep holding wakelock in OOR
- CSCvk25979 Phone eventually not able to receive auth response
- CSCvk30176 No response while press conf soft key after merge all on secured SRST
- CSCvk33875 Screenpng does not work when 8821 is sleeping
- CSCvk65315 Download application multiple times when press the application button
- CSCvm05950 Phone stuck at black screen during stress test
- CSCvm16421 EAP authentication triggered by wpa\_suppllicant got interrupted and causing de-registration
- CSCvm23580 8821 dhcp exit and reboot after switching wlan profiles
- CSCvm40695 4-way handshake got interrupted by reassoc request thereby causing de-registration
- CSCvm46026 8821 : Java crash and connectivity lost
- CSCvm47856 Multiple Vulnerabilities in linux
- CSCvm50336 CIAM alerts of Linux/Linux for cygnus: CVE-2018-1130, CVE-2018-11506, CVE-2018-11508

- CSCvm50340 CIAM alerts of Linux/Linux for cygnus for all phone models
- CSCvm50348 Multiple Vulnerabilities in linux for 8821 wireless phone
- CSCvm50349 Multiple Vulnerabilities in linux, port CSCvm11633 to 8821
- CSCvm50527 Linux Kernel Kerberos RxRPC Ticket Decoding Local Privilege Escalati ...
- CSCvm55729 Phone can't associate to AP after inter-profile roaming, enable new profile after OOR
- CSCvm58866 4-way handshake failure due to invalid MIC in M2
- CSCvm59233 cURL and libcurl NTLM Password Buffer Overflow Vulnerability (CVE-2018-14618)
- CSCvm60777 Linux Kernel alarm\_timer\_nsleep() Function Integer Overflow Vulnerability (CVE-2018-13053)
- CSCvm69529 CDP shows previous IP for WLAN interface via CDP instead of wired USB dongle interface when docked
- CSCvm70501 8821 should not download WLAN config file from hCluster after EMCC login
- CSCvm75535 Phone will not connect to 2.4GHz enabled WiFi profile from a 5GHz enabled WiFi profile vice versa
- CSCvm85526 Phone crashed when DHCP option 66 field configured with MaxLength
- CSCvm87461 Call drop automatically after blowing into the Cisco 521/522 headset for 3-5 times during call
- CSCvm91396 No beep tone for hold revert while the other line in RIU status
- CSCvm92798 Multiple Vulnerabilities in linux
- CSCvm92833 Linux Kernel MIDI Driver Local Privilege Escalation Vulnerability (CVE-2018-10902)
- CSCvm95451 XMLSoft libxml2 xmlXPathCompOpEval() Function NULL Pointer Dereference Vulnera... (CVE-2018-14404)
- CSCvm98027 GreenKey failed to work when setting phone to offhook dialing mode
- CSCvm99207 BusyBox huft\_build Function Denial of Service Vulnerability (CVE-2015-9261)
- CSCvm99883 "Feature is unavailable" pops up on recipient phone UI on CME
- CSCvn35581 Multiple Vulnerabilities in openssl, part 2
- CSCvn37282 8821 phone freezes after receiving XSI msgs using priority 1
- CSCvn38253 "MIC mismatch" is seen in WLC log when 8821 fast roaming with 2802/3802 AP
- CSCvn49489 wpa\_supplicant EAPOL-Key Messages Information Disclosure Vulnerability
- CSCvn60806 8821 phone Incoming Call Toast not display when ringing and phone screen keeps dark
- CSCvn63436 Linux Kernel ALSA Driver Local Use-After-Free Vulnerability (CVE-2018-19824)
- CSCvn67226 Qt BMP Image Handler Remote Denial of Service Vulnerability
- CSCvn71400 Pressing Green key should not answer two incoming calls at the same time

- CSCvn78117 Move the connected BT headset OOR, audio path will be switched to phone's headset within 10s
- CSCvn78225 Multiple Vulnerabilities in linux
- CSCvn81758 No ring for hold reversion after disconnecting another active call
- CSCvn97100 Pressing green button can not dial out speed dial on line view
- CSCvo08243 Trolltech Qt QBmpHandler BMP File Buffer Overflow Vulnerability (CVE-2018-19873)
- CSCvo14601 Redial via press green key twice does not work when using off hook dialing
- CSCvo32268 Ring plays thru headset if inserting headset during ringing while on dock & ringer output is Speaker
- CSCvo40605 Softkey associated with two-digit numbers can not be accessed by pressing the index number
- CSCvo43854 Multiple Vulnerabilities in libxml2
- CSCvo44367 Multiple Vulnerabilities in busybox
- CSCvo47495 Linux Kernel USB Subsystem Data Size Checks Handling Vulnerability (CVE-2018-20169)
- CSCvo48068 Favorites highlight shifted when access by pressing index # if contact /w long name is assigned
- CSCvo54699 Cisco IP Phone 8821 Series CDP and LLDP Denial of Service Vulnerability (CVE-2019-1684)
- CSCvo57138 Cisco Wireless IP Phone 8821 and 8821-EX Path Traversal Vulnerability
- CSCvo57629 Cisco Wireless IP Phone 8821 and 8821-EX Series Cross-Site Request Forgery Vulnerability
- CSCvo58414 Cisco Wireless IP Phone 8821 and 8821-EX Authorization Bypass Vulnerability
- CSCvo64862 8821 not receiving audio alerts from 3rd party Alerting software like Momentum

## Cisco Unified Communication Manager Public Keys

To improve software integrity protection, new public keys are used to sign cop files for Cisco Unified Communications Manager Release 10.0.1 and later. These cop files have “k3” in their name. To install a k3 cop file on a pre-10.0.1 Cisco Unified Communications Manager, consult the README for the `cisco.version3-keys.cop.sgn` to determine if this additional cop file must first be installed on your specific Cisco Unified Communications Manager version. If these keys are not present and are required, you will see the error “The selected file is not valid” when you try to install the software package.

## Unified Communications Manager Endpoints Locale Installer

By default, Cisco IP Phones are set up for the English (United States) locale. To use the Cisco IP Phones in other locales, you must install the locale-specific version of the Unified Communications Manager Endpoints Locale Installer on every Cisco Unified Communications Manager server in the cluster. The Locale Installer installs the latest translated text for the phone user interface and country-specific phone tones on your system so that they are available for the Cisco IP Phones.

To access the Locale Installer required for a release, access <https://software.cisco.com/download/navigator.html?mdfid=286037605&flowid=46245>, navigate to your phone model, and select the Unified Communications Manager Endpoints Locale Installer link.

For more information, see the documentation for your particular Cisco Unified Communications Manager release.



---

**Note** The latest Locale Installer may not be immediately available; continue to check the website for updates.

---

## Cisco IP Phone Documentation Updates on Cisco Unified Communications Manager

The Cisco Unified Communications Manager Self Care Portal (Release 10.0 and later) and User Options web pages (Release 9.1 and earlier) provide links to the IP Phone user guides in PDF format. These user guides are stored on the Cisco Unified Communications Manager and are up to date when the Cisco Unified Communications Manager release is first made available to customers.

After a Cisco Unified Communications Manager release, subsequent updates to the user guides appear only on the Cisco website. The phone firmware release notes contain the applicable documentation URLs. In the web pages, updated documents display “Updated” beside the document link.



---

**Note** The Cisco Unified Communications Manager Device Packages and the Unified Communications Manager Endpoints Locale Installer do not update the English user guides on the Cisco Unified Communications Manager.

---

You and your users should check the Cisco website for updated user guides and download the PDF files. You can also make the files available to your users on your company website.



---

**Tip** You may want to bookmark the web pages for the phone models that are deployed in your company and send these URLs to your users.

---

## 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 NON-INFRINGEMENT 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](http://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)

© 2019–2020 Cisco Systems, Inc. All rights reserved.