# Release Notes for Cisco Webex Meetings Server Release 3.0

**First Published:** 2018-01-24

**Last Modified:** 2021-01-12

## Release Notes for Cisco Webex Meetings Server

These release notes describe new features, requirements, restrictions, and caveats for all versions of Cisco Webex Meetings Server Release 3.0. These release notes are updated for every maintenance release but not for patches or hot fixes. Each maintenance release includes the features, requirements, restrictions, and bug fixes of the previous releases unless mentioned otherwise. Before you deploy Cisco Webex Meetings Server, we recommend that you review these release notes for information about issues that may affect your system.

New customers can purchase Cisco Webex Meetings Server directly from Cisco Systems, Inc. or from a Partner sales representative.

Existing customers can obtain the Release 3.0 OVA file by using the Product Update Tool (PUT): http://upgrad.cloudapps.cisco.com/upgrad/jsp/index.jsp

To download the latest software updates for this product, visit: http://software.cisco.com/download.

Select **Products** > **Conferencing** > **Web Conferencing** > **WebEx Meetings Server** > **WebEx Meetings Server 3.0**.

### Finding Documentation

For administration documentation, visit: http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/tsd-products-support-series-home.html.

Provide the following URL to your users: http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-user-guide-list.html.

### New and Changed Features for Cisco Webex Meetings Server Release 3.0MR3

This section describes what is new for Cisco Webex Meetings Server Release 3.0MR3.

**Attention** The 3.0MR3 software update is only for systems that are currently running Cisco Webex Meetings Server Release 3.0.1.27, 3.0.1.1068, 3.0.1.2083, and later.

For information about important new upgrade considerations, see Webex Productivity Tools, on page 3 and Supported Upgrade Paths, on page 9.

## 3.0MR3 Security Patch 4

We've updated the following components:

- Webex Meetings Client 39.5.27.43
- Network Recording Player 39.5.27.43
- Webex Meetings desktop app 39.5.27.43

We've also added support for TFS and URL-Protocol, for starting meetings and playing NBR recordings.

This patch introduces support for MacOS 11, Big Sur.

## Health Checker for Mac

To match the functionaly avaible for Microsoft Windows, this maintenance release includes Health Checker for Mac.

## Updated Browser Support

This maintenance release adds support for the following browsers:

### Microsoft Windows

- Chrome versions 77 and 78
- Firefox versions 69 and 70

### Mac

- Chrome versions 77 and 78
- Firefox versions 69 and 70
- Safari version 13

## Updated CUCM Support

This maintenance release adds support for Cisco Unified Communications Manager Release 11.5 SU8, 12.5, and Release 12.5(1) SU1.

## Updated macOS Support

We've added support for macOS Catalina (Version 10.15).

## Video-Centric Experience for Meetings

This release provides a new in-meeting experience that allows hosts and meeting participants to customize how they want to view a meeting. We've maximized the meeting space available for video meetings, added new layouts, and simplified the meeting controls. For more information, see *Managing Webex Meetings Guide for Cisco Webex Meetings Server Release 3.0*.

**Attention** Cisco Webex Meetings Server Release 3.0MR3 supports the display of 1–6 video streams.

### Webex Meeting Client Application

This maintenance release supports Webex Meetings Application version 39.5.15.4 for Mac and Windows.

### Webex Network Recording Player

This maintenance release supports the following Cisco Network Recording Player versions:

- **Windows:** 39.5.15.4
- **Mac:** 39.5.15.4 (online), 39.05.12.00 (offline)

You can install the latest version from the **Downloads** page of your Cisco Webex site. When you download the Cisco Network Recording Player, select **Windows** or **Mac** from the operating system drop-down list. The Windows player is the default download.

### Webex Productivity Tools

This maintenance release requires Webex Productivity Tools version 2.82.7000.1229.

## New and Changed Features for Cisco WebEx Meetings Server Release 3.0MR2

This section describes what is new for Cisco WebEx Meetings Server Release 3.0MR2.

**Attention** The 3.0MR2 software update is only for systems that are currently running Cisco WebEx Meetings Server Release 3.0.1.27 or 3.0.1.1068, and later.

Update from 3.0 Patch 1 (3.0.1.33) to 3.0MR2 will fail. Before trying to update from 3.0 Patch 1 to 3.0MR2, see, Update from 3.0 Patch 1 Fails, on page 21 and apply the workaround for this issue.

### Automatically Enter the Full-Screen Video Mode

With this maintenance release, attendees can enable the **Automatically show me the full-screen video** option in the **Audio and Video Connection** dialogue box. If this option is enabled, the full-screen video view opens when the attendee connects to meetings.

### Cisco Webex Meeting Mobile Version Requirements

To start or join meeting from iOS or Android on a 3.0MR2 site, Cisco strongly recommends using the following application versions:

**Android:** Cisco Webex Meeting Mobile 11.2

**Apple iOS:** Cisco Webex Meeting Mobile 11.2

If a user joins a meeting started from CWMS Release 3.0MR2, by using an earlier versions either mobile app (11.1 or lower), video and VoIP may not work as expected. For more information, see Caveats, on page 22.

### Improved Default Avatar

The default avatar for anonymous call-in users is updated to a more intuitive phone icon, instead of the **CU** initials.

## Mac 64-bit Support

The Webex Desktop App on Mac now supports 64-bit, which is required by the latest and future macOS versions.

## Optimization for High Resolution Displays: Application Sharing Dialogues

The application sharing dialogues are optimized for high-resolution monitors—3K or higher. Support for higher display resolutions is limited to Microsoft Windows 7 or later.

## Optimization for High Resolution Displays: Consistency Across Multiple Monitors

WebEx behavior and consistency is improved in multiple-monitor environments—particularly when moving windows between monitors that have different resolution settings.

## Optimization for High Resolution Displays: File Transfer and File Sharing Dialogues

File transfer and file sharing dialogues are now optimized for high-resolution monitors. The **Closed Caption** panel is optimized for high-resolution monitors, and can be controlled through the text zoom setting in Windows. Support for higher display resolutions is limited to Windows 7 or later.

## Improved Problem Reporting

Microsoft Windows users can now easily report problems with CWMS, by clicking **Help** > **Generate Problem Report**.

## Lock Video Window Focus to a Specific Participant

Attendees can now lock the video window focus to the meeting participant of their choice. This applies to the main video window, as well as to any of the thumbnail windows on the first page.

**Note** Attendees cannot lock the main window, if the host locks the main window for all participants.

## Single Participant Meetings End After a Set Time

Meetings now automatically end at a specified time, when there is only one person who is left in the meeting.

Site administrators can specify the time in the **Common Site Settings**.

This feature is enabled by default.

## Switch Between Full Video and Full Content View

Users can switch between a full video screen and the full content view, even when content is being shared.

## Switch to Classic Screen Sharing Mode in Microsoft Windows 10

By default, CWMS uses advanced screen sharing in Microsoft Windows 10. Advanced screen sharing prevents crosshatch-patterned windows from appearing for others where meeting panels are open on your screen. However, if you experience problems, or if your computer does not support advanced screen sharing, you can switch to classic screen sharing.

## Updated Browser Support

This maintenance release adds support for the following browser versions:

**Microsoft Windows**

- Chrome Version: 67 and 68
- Firefox Version: 61
- Edge (Windows 10 only): 42.17134.1.0

**Mac**

- Chrome Version: 67 and 68
- Firefox Version: 61

## Updated Cisco Jabber Support

This maintenance release adds support for Cisco Jabber Release 12.1.0 with some limitations.

The following defect is open for Cisco Jabber Release 12.1.0:

| Identifier | Severity | Description |
|---|---|---|
| CSCvm06144 | 3 | Cannot start meeting from Jabber client if OS user name and region language are Asian language |

For more information about other Jabber limitations, see Caveats, on page 22.

## Updated CUCM Support

This maintenance release adds support for Cisco Unified Communications Manager Release 11.5 SU5.

## Updated macOS Support

This maintenance release adds support for macOS High Sierra 10.13.6 and macOS Sierra 10.12.6.

## Updated UDP Port Requirements

This maintenance release adds new UDP ports for medium and large (including expanded) systems. The following additional UDP ports are now required for audio and video data transmission:

- **Medium system:** 9010 and 9011
- **Large system:** 9008 and 9009

Before you upgrade or update a Medium or Large system to CWMS Release 3.0MR2, the required ports must be open. There are no new port requirements for Micro or Small systems. For more information, see the *Planning Guide for Cisco WebEx Meetings Server Release 3.0*.

## WebEx Meeting Client Application

This maintenance release supports WebEx Meetings Application version 32.15.20.116 for Mac and Microsoft Windows.

### WebEx Network Recording Player

This maintenance release supports the following Cisco Network Recording Player versions:

- **Windows:** 32.15.20.116
- **Mac:** 32.15.20.57

You can install the latest version from the **Downloads** page of your Cisco WebEx site. When you download the Cisco Network Recording Player, select **Windows** or **Mac** from the operating system drop-down list. The Windows player is the default download.

### WebEx Productivity Tools

This maintenance release supports WebEx Productivity Tools version 2.82.7000.1213 for Windows.

## New and Changed Features for Cisco WebEx Meetings Server Release 3.0MR1

This section describes what is new for Cisco WebEx Meetings Server Release 3.0MR1.

**Attention** The 3.0MR1 software update is only for systems that are currently running Cisco WebEx Meetings Server Release 3.0.1.27 or later.

Updating from Release 3.0 Patch 1 (3.0.1.33) to Release 3.0MR1 fails. Before you update from the 3.0 Patch 1 to Release 3.0MR1, see Update from 3.0 Patch 1 Fails, on page 21 and apply the workaround for this issue.

### Recording Playback over IRP in the DMZ Network

Starting with this maintenance release, port 64002 is used for recording playback, which is initiated from an external network over IRP. For more information about port configuration, see the *Planning Guide and System Requirements for Cisco WebEx Meetings Server Release 3.0* available from https://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-and-configuration-guides-list.html.

### Updated Browser Support

This release adds support for the following browser versions:

**Windows:**

- Chrome Version 66
- Firefox Version 60
- IE Version 11
- Edge (Windows 10 only) Version 42.17134.1.0

**Mac:**

- Chrome Version 66
- Firefox Version 60
- Safari Version 11.1

### Updated Citrix Support

This maintenance release adds support for Citrix XenDesktop and Citrix Web Interface 7.12 and 7.15.

### Updated CUCM Support

This maintenance release adds support for Cisco Unified Communications Manager Release 11.5 SU4 and Release 12.0(1) SU1.

### Updated macOS Support

This maintenance release adds support for macOS High Sierra 10.13.4.

### Updated VMWare ESXi Support

This maintenance release adds support for ESXi/vCenter 6.5.

**Important** Before updating ESXi to 6.5, verify that your datastore is formatted with VMFS 5. ESXi 6.5 hosts cannot access VMFS 3 datastores. ESXi hosts must meet the minimum hardware requirements for ESXi6.5.

### WebEx Meeting Client Application

This release supports WebEx Meetings Application version 31.23.4.23 for Windows and Mac.

### WebEx Network Recording Player

This release supports the following Cisco Network Recording Player versions:

- **Windows:** 31.23.4.23
- **Mac:** 31.0.0.1100

### WebEx Productivity Tools

This release supports WebEx Productivity Tools version 2.82.7000.1202 for Windows.

## New and Changed Features for Cisco WebEx Meetings Server Release 3.0

This section describes features that are new or changed in this release.

For a complete list of system requirements, see the *Cisco WebEx Meetings Server Planning Guide and System Requirements Release 3.0*. Visit http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html.

All supported features from Cisco WebEx Meetings Server (CWMS) Release 2.8 (including features added in Maintenance Releases) are supported in CWMS 3.0. The data sheet for Cisco WebEx Meetings Server provides an overview of the features and benefits of CWMS. Visit http://www.cisco.com/en/us/prod/collateral/ps10352/ps10362/ps12732/data_sheet_c78-717754.html.

### Approve Hosts

You can require administrator approval of requests for Host privileges on the system. You can also enable automatic approval for requests and specify domains, from which to accept all requests and domains from which to reject all requests. The system handles all automatic approvals within 24 hours.

**Note** All requests that do not match the approval or rejection criteria require manual approval or rejection.

As a site administrator, you receive email notification about all requests for Host privileges and can choose to either approve or reject the requests. Host privileges require a license. A request from a formerly licensed Host can be approved only if there is an available license.

For more information about how to manage licenses and this feature, see the *Administration Guide for Cisco WebEx Meetings Server Release 3.0*.

## Avatars (Profile Pictures)

By default, an image with each account holder's initials (an avatar) appears next to their name in the meeting client. You can enable this feature to allow them to change their default avatar to an image of their choosing. You'll find the setting on the **Meeting Settings** page in Site Administration.

Account holders can crop their new image before they upload it on their **Account Settings** page. The supported file types are PNG, JPG, JPEG, and GIF. The system stores all avatar images as JPG files. Therefore, if the uploaded file is an animated GIF, the system displays only the first frame. The minimum dimensions are 60 by 160 pixels and the maximum file size is 5 MB.

## Cisco Jabber Support

This release adds support for Cisco Jabber Release 11.9.1.

## Closed Captioning Support with the Media Viewer Panel

Hosts can use the Media Viewer Panel and a third-party closed-captioning service to provide closed captioning for their meetings. This feature improves the Section 508 compliance level for Cisco WebEx Meetings Server. You'll find the setting on the **Meeting Settings** page in Site Administration.

## Extend or Reduce Your System Capacity

The base deployment models are micro (50), small (250), medium (800) and large (2000). You can extend the capacity of a large deployment, from 2000 up to 4000 ports. You can reduce the capacity of an extended system deployment, down to the base large deployment of 2000 ports.

To extend or reduce the system capacity, you add or remove up to 3 extension units. Each unit of growth consists of the following components:

- One media
- One web
- One IRP (only if public access is enabled)

**Note** Each extension unit adds up to 700 more ports, up to the maximum 4000 ports for the system. When you add 3 extension units, you double the system capacity by adding 700 + 700 + 600 ports.

The Extended Capacity feature requires a license. For more information, contact your Cisco Account Manager. You can also see the “Managing Your System Capacity” chapter in the *Administration Guide for Cisco WebEx Meetings Server*.

### Prerequisite to Upgrade a Multi-Data Center System

To prepare a multi-data center (MDC) system for the upgrade to CWMS Release 3.0, we recommend that you back up all certificates and the private key. For security reasons, we recommend that you back up private keys to FIPS 140-2 certified storage. For more information, see the **Before You Begin an Upgrade** and the **Restoring an SSL Certificate after Disaster Recovery** sections of the *Administration Guide for CWMS Release 3.0*.

These steps are not required for a non-MDC system. For a single data center, certificate configuration is restored when the upgrade is complete.

### Updated Browser Support

This release adds support for the following browser versions:

**Windows:**

- Edge (Windows 10 only) 40.15063
- Firefox Version 56–57
- Google Chrome Version 61–63
- IE: 11.0.9600

**Mac:**

- Chrome Version: 61–63
- Firefox Version: 56–57
- Safari Version: 11

### WebEx Meeting Client Application

This release supports WebEx Meetings Application version 31.20.2.18 for Windows and Mac.

### WebEx Network Recording Player

This release supports the following Cisco Network Recording Player versions:

- **Windows:** 31.20.2.18
- **Mac:** 31.0.0.1100

### WebEx Productivity Tools

This release supports WebEx Productivity Tools version 2.82.7000.1198 for Windows.

The following issue, present in earlier releases is resolved. While using Productivity Tools to schedule a meeting, hosts received the following message in error:

Only 99 invitees can actually join the online meeting.

## Supported Upgrade Paths

This release of Cisco Webex Meetings Server supports upgrades from release 1.5 to 3.0. The following points apply:

- An upgrade is defined as a replacement of the system to deploy major modifications that we made to the system.
- An update is defined as an incremental modification of the system. Updates deploy fixes and minor improvements.
- An update retains all data from the original system. An upgrade retains all data from the original system, except for the logs.
- 

  **Important** You cannot change the audio encryption type (Audio Encrypted -AE/Audio Unencrypted -AU) for the system, during an upgrade or during an update. After deployment, the only way to change a system from one type of audio encryption to the other is to deploy a new system.
- When upgrading, you cannot skip a major version of the software and go directly to a companion maintenance release (MR). For more information, see the following table.

Use the following table to determine your upgrade path to Cisco Webex Meetings Server Release 3.0.

| Installed Release | To Release | Path |
|---|---|---|
| 1.5 to 1.5MR4 | 3.0 | **1.** Update to 1.5MR5.<br>**2.** Update to 1.5MR5 Patch 2 or later.<br>**3.** Upgrade to 2.8.<br>**4.** Update to 2.8MR1.<br>**5.** Update to 2.8MR1 Patch 2 or later.<br>**6.** Upgrade to 3.0. |
| 1.5 MR5 | 3.0 | **1.** Update to 1.5MR5 Patch 2 or later.<br>**2.** Upgrade to 2.8.<br>**3.** Update to 2.8MR1.<br>**4.** Update to 2.8MR1 Patch 2 or later.<br>**5.** Upgrade to 3.0. |
| 1.5 MR5 Patch 2 or later | 3.0 | **1.** Upgrade to 2.8.<br>**2.** Update to 2.8MR1.<br>**3.** Update to 2.8MR1 Patch 2 or later.<br>**4.** Upgrade to 3.0. |

| Installed Release | To Release | Path |
|---|---|---|
| 2.0 to 2.0MR8 | 3.0 | **1.** Update to 2.0MR9.<br>**2.** Update to 2.8.<br>**3.** Update to 2.8MR1.<br>**4.** Update to 2.8MR1 Patch 2 or later.<br>**5.** Upgrade to 3.0. |
| 2.0MR9 or later | 3.0 | **1.** Update to 2.8.<br>**2.** Update to 2.8MR1.<br>**3.** Update to 2.8MR1 Patch 2 or later.<br>**4.** Upgrade to 3.0. |
| 2.5 to 2.5MR5 | 3.0 | **1.** Update to 2.5MR6.<br>**2.** Update to 2.8.<br>**3.** Update to 2.8MR1.<br>**4.** Update to 2.8MR1 Patch 2 or later.<br>**5.** Upgrade to 3.0. |
| 2.5MR6 or later | 3.0 | **1.** Update to 2.8.<br>**2.** Update to 2.8MR1.<br>**3.** Update to 2.8MR1 Patch 2 or later.<br>**4.** Upgrade to 3.0. |
| 2.6 to 2.6MR2 | 3.0 | **1.** Update to 2.6MR3.<br>**2.** Update to 2.8.<br>**3.** Update to 2.8MR1.<br>**4.** Update to 2.8MR1 Patch 2 or later.<br>**5.** Upgrade to 3.0. |
| 2.6MR3 or later | 3.0 | **1.** Update to 2.8.<br>**2.** Update to 2.8MR1.<br>**3.** Update to 2.8MR1 Patch 2 or later.<br>**4.** Upgrade to 3.0. |

| Installed Release | To Release | Path |
|---|---|---|
| 2.7 to 2.7MR2 | 3.0 | **1.** Update to 2.7MR3<br>**2.** Update to 2.7MR3 Patch 1 or later.<br>**3.** Upgrade to 3.0. |
| 2.7MR3 Patch 1 or later | 3.0 | Upgrade to 3.0. |
| 2.8 | 3.0 | **1.** Update to 2.8MR1.<br>**2.** Update to 2.8MR1 Patch 2 or later.<br>**3.** Upgrade to 3.0. |
| 2.8MR1 | 3.0 | **1.** Update to 2.8MR1 Patch 2 or later.<br>**2.** Upgrade to 3.0. |
| 2.8MR1 Patch 2 or later | 3.0 | Upgrade to 3.0. |
| 3.0 | 3.0MR1 or 3.0MR2 | Update to 3.0MR1 or 3.0MR2. |
| 3.0 | 3.0MR3 | **1.** Update to 3.0MR2 Patch 4 or Patch 5.<br>**2.** Push Productivity Tools to user desktops.[1]<br>**3.** Update to 3.0MR3. |

[1] The Webex Productivity Tools version must be 2.82.7000.1229 or later, to start the 3.0MR3 meeting client. Upgrade Productivity Tools, before you update Cisco Webex Meetings Server to 3.0MR3.

**Note** All updates require downtime. For Multi-data centers, you update both data centers simultaneously.

**Caution** Do not click **Restart** for one data center until the update for the other is complete, and both display the **Restart** button.

For more information, see the following documents:

- *Administration Guide for Cisco Webex Meetings Server Release 3.0*: http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html
- *Planning Guide and System Requirements for Cisco Webex Meetings Server Release 3.0*: http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-and-configuration-guides-list.html

### Updating Your High-Availability System

For systems with an existing High Availability (HA) system already attached, the HA system automatically updates when you update the primary system. Ensure that all HA virtual machines are turned on and running before you start the update process.

To add a High Availability (HA) system to your primary system, first deploy the HA system. Then update the HA system to the same version as the primary system. The HA system restarts at the end of the update process. We recommend that you wait an extra 15 minutes after the restart, before you begin to add the HA system to the primary system.

For more information, see the *Cisco Webex Meetings Server Administration Guide* for your release:

http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-guides-list.html

## Limitations and Restrictions

### Audio-only Meetings

Under the following circumstances, a meeting can continue for more than the 24-hour maximum meeting duration:

- All attendees for a regular Webex meeting are dial in (audio-only).
- No attendee starts the web portion of the meeting.

In this case, the meeting continues as long as one attendee remains in the conference. If all dial-in attendees disconnect from the conference, the meeting ends within 24 hours of the start time. The meeting ends immediately if the meeting ran past the scheduled end time.

**Note** This scenario applies only to regular Webex meetings joined only by dial-in participants. This scenario does not apply to Personal Conference Number (PCN) meetings, or to regular Webex meetings joined by web participants.

### Internet Reverse Proxy Removal

As part of the Internet Reverse Proxy (IRP) node removal process, the Admin virtual machine sends a remove message to the IRP server. The message removes the IRP server and therefore all external access to the system. The message is sent as clear text, and it is unauthenticated. Well-crafted malicious code could replicate this behavior and lead to a denial of service.

We recommend that you limit access to port 64616, on the IRP node, to the Admin virtual machine only.

### Productivity Tools

#### EMC SourceOne

WebEx Productivity Tools does not support EMC SourceOne. Users of EMC SourceOne can experience performance issues.

## Incompatible Versions

Each release of Cisco WebEx Meetings Server supports a specific version of the Cisco WebEx Productivity Tools client. Download the supported version of Productivity Tools from the Downloads link on your Cisco WebEx Meetings Server website. Using incompatible versions of these two applications can cause issues.

## Updating a Recurring Meeting Scheduled from Microsoft Outlook

This release has the following limitations when updating a single instance of a recurring meeting series that was scheduled from the Microsoft Outlook integration:

- User does not see the "Add WebEx Meeting" option: User schedules a standard recurring meeting series from Outlook. When the user attempts to update a single instance of the series, the user does not see the option to add the WebEx component to the meeting. In this instance, we recommend that the user schedules a new meeting that includes the WebEx option, or change the entire recurring meeting series to include the WebEx component.
- WebEx is not removed from meeting exceptions: User schedules a recurring meeting series. User edits one or more instances to indicate a different time or date, then cancels the recurring meeting series. In this instance, the meetings that were edited are not canceled in Outlook. However, the WebEx information that is retained with the meetings are no longer valid.
- Canceled meetings still display on web page: User schedules a recurring meeting series from Microsoft Outlook. User deletes a meeting instance from the series, then adds WebEx to the recurring meeting series. In this instance, the meetings that were deleted from the original recurring meeting series will still display on the Cisco WebEx Meetings Server website.
- Updates not reflected in meeting exceptions: User schedules a recurring meeting series from Microsoft Outlook. User edits a single instance of the meeting series by changing the meeting topic, list or attendees, or location. User then edits the meeting content in the entire recurring meeting series. In this instance, any updates made to the series are not reflected in the meetings that were updated separately.
- WebEx component does not reflect future meeting time: User schedules a WebEx meeting from Microsoft Outlook. The meeting time passes. The user drags one instance of the series to a time in the past, then updates it to reflect a time in the future. In this instance, the WebEx component of the meeting remains the same. It cannot be updated to reflect a future time.
- When the user makes any change to a single occurrence of a meeting series, this occurrence is assigned a new meeting ID from the server. The user must ensure to send an updated meeting notification, with the new meetingID, to all the invitees.

## Recording Limitations

The maximum recording size, per recording, is 2.2 GB (existing system limit). For Multi-data Centers, ensure that there is sufficient storage capacity available for all data centers. The maximum number of recordings depends on your storage server capacity. You can estimate the required storage server size for a typical five-year period using the following formula:

Estimated hours of meetings that you expect to be recorded per day * 50-100 MB per hour of recording * five years * 24 hours per day * 365 days per year

There are no per-user storage limitations. The system stores recordings indefinitely until users delete them. To prevent important recordings from being accidentally deleted, there is no setting to enable the automatic deleting of recordings. The storage server retains recordings marked for deletion for up to six months. During that time, users can still archive the recordings to other media.

When you configure a storage server and check **Record** under **Administration Dashboard** > **Settings** > **Meetings** > **Participant Privileges**, the **Record** setting is a system-wide setting. There are no individual

meeting settings or preferences for recordings. You can also enable or disable recording by Session Types, which you assign to users.

## Session Types

A session type is a predefined bundle of features and options (a profile) that site administrators can customize and assign to users. The default session (meeting) type is the PRO session type. Because of the relationships between the PRO session type and the custom session types, we recommend that you do not modify the PRO session type. The best practice is to create a custom session type to modify.

## SSO and Email Address Changes

With this release, the Identity Provider (IdP) server can use any unique and static Active Directory (AD) field as the NameID for SSO configuration. If you plan to use the email address change feature, the email AD field is not static. Change the mapping for the NameID field on the IdP server to a unique AD field other than email. If you do not plan to use the feature to change email addresses, there is no requirement to change the mapping for the NameID field.

**Caution** If the NameID field is mapped to the email AD field and you change user email addresses, the system creates a new user account for each changed address.

If you plan to change the NameID field mapping from email to another field (such as EmployeeNumber), users must prepare for the change. After you update the NameID fields in AD, have the users log in to CWSM before you change the email addresses. Otherwise, when both the NameID and email address change, no attribute matches the CWMS profile. In this scenario, the existing profile loses the ablity to log into the system and the system creates a new profile.

Outlook synchronizes with the Exchange server once a day. If you change an existing user's email address on the Exchange server, the change does not immediately propagate to Outlook. Until synchronization occurs, the system receives the user's former email address and issues a notice that the user cannot be found. A delegate (proxy) user cannot schedule a meeting for the user, or identify them as an alternate host, until after Outlook synchronizes with the Exchange server.

Manually synchronizing the systems does not solve this issue. This limitation is not a CWMS issue; it is the result of Outlook and Exchange design.

*See also* About SSO Configuration, on page 18.

## Microsoft Edge Browser

The Microsoft Edge browser does not support the playback of Webex recordings.

## vCenter 6.5 Support

When you deploy the CWMS OVA file on vCenter 6.5, the following restrictions apply:

- Because of browser limitations and the CWMS OVA file size of 16GB, you must deploy the OVA file by using the URL and not the local file upload.
- Choose the vCenter FLASH based client. This selection is required to successfully populate the vApp properties for VM configuration: hostname, domain, IP address, subnet and DNS configuration.

### Virtual Desktop Infrastructure

The following limitations and restrictions are known to affect virtual desktop infrastructure (VDI) environments.

- Citrix Virtual Apps and Desktops is the only desktop virtualization software supported for this release of Cisco Webex Meetings Server.
- An architectural limitation of the virtual desktop environment can affect video quality. The frame rate may be low, causing a suboptimal experience when sending video.
- Some video files cannot be shared in a virtual desktop environment.
- Remote Access and Access Anywhere are not supported in virtual desktop environments. The underlying Citrix platform removes the Remote Access and Access Anywhere agents after the operating system restarts.

## Important Notes

### CWMS Licensing

#### Multi-data Center Licensing

Multi-data Center (MDC) licensing is required to join data centers to a system. Each data center requires an MDC system license; a MDC system requires a minimum of two licenses, one for each data center. A Single-data Center (SDC) does not require a system license. See "About MDC Licensing" in the Cisco Webex Meetings Server Administration Guide for your release: http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-guides-list.html.

#### Host Licensing

The way Host (user) licenses are counted changed significantly in release 2.5. A user can host a maximum of two simultaneous meetings, consuming only one license. Previously, a user that hosted multiple meetings consumed multiple licenses. A Host licenses is not required to schedule or attend a meeting. See "License Status of Users" in the Cisco Webex Meetings Server Administration Guide for your release: http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-guides-list.html.

#### Extended Capacity Licensing

The base deployment models are micro (50), small (250), medium (800) and large (2000). You can extend the capacity of a large deployment, from 2000 up to 4000 ports. You can reduce the capacity of an extended system deployment, down to the base large deployment of 2000 ports.

To extend or reduce the system capacity, you add or remove up to 3 extension units. Each extension unit adds up to 700 more ports, up to the maximum 4000 ports for the system. When you add 3 extension units, you double the system capacity by adding 700 + 700 + 600 ports.

To enable this feature, you require an Extended Capacity license.

### Hypervisor Support

Cisco Webex Meetings Server runs on VMware virtual machines.

- Both VMware vSphere and VMware vCenter are required to deploy Cisco Webex Meetings Server. Using the vSphere client, you deploy the Cisco Webex Meetings Server OVA file on an ESXi host managed by vCenter.
- Purchase VMware vSphere 5.5, or 6.0 for use as the hypervisor platform for Cisco Webex Meetings Server.
  - Buy vSphere directly from Cisco on the GPL (Global Price List). Cisco is an approved VMware partner and distributor. This is convenient for those who want to purchase everything from a single vendor.
  - Purchase vSphere directly from VMware, through enterprise agreements you have directly with VMware.
- Cisco Webex Meetings Server does not support other hypervisors.
- For more information about hypervisor requirements, see the *Planning Guide and System Requirements for Cisco Webex Meetings Server* at http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html.

## About Using Self-Signed Certificates

We strongly recommend using a publicly signed certificate instead of the provided self-signed certificate. User's browsers trust publicly signed certificates because the list of Root Certificate Authority certificates installed on the computer establishes trust.

For Multi-data Center systems using self-signed certificates, the user receives multiple certificate warnings and must trust and install all certificates to use the system.

When using self-signed certificates, some users might have difficulty joining meetings because browsers by default do not trust such certificates. Users are required to explicitly establish trust in this case before they can proceed to join a meeting on your site. Some users might not understand how to establish trust with such a certificate. Others might be prevented from doing so by administrative settings. Use publicly signed certificates whenever possible to provide the best user experience.

The User Guide provides more information about this issue for users. See the "Meeting Client Does Not Load" topic in the "Troubleshooting" chapter of the *Cisco Webex Meetings Server User Guide* at http://www.cisco.com/en/us/products/ps12732/products_user_guide_list.html.

## Supported Ciphers

Cisco Webex Meetings Server supports the following ciphers:

**TLS Version 1.1**

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1)
- TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048)
- TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048)

**TLS Version 1.2**

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1)
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1)

- TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1)
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1)
- TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048)
- TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048)
- TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048)
- TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048)

## TLS Support

This release supports TLS 1.1 and later; TLS 1.0 is not supported, with one exception. Client connections from Cisco Webex Meetings Server (CWMS) to an SMTP server using TLS 1.0 are supported.

## About SSO Configuration

This release supports using any unique Active Directory (AD) field as NameID for SSO configuration. We recommend following AD attributes for NameID for SSO configuration:

- Email
- SAMAccountName
- UserPrincipalName (UPN)
- TelephoneNumber
- EmployeeNumber
- ObjectSid

### Mandatory SAML Assertion Attributes

The following SAML assertion attributes are required for the Auto Account Creation feature:

- lastname
- firstname
- email

**Important** The email attribute is always required, even if Auto Account Creation and Auto Account Update are disabled in the SSO configuration.

## Expanding Your System

If you have VMware snapshots on your existing (pre-expansion) system, remove them before beginning the expansion.

System expansion requires Virtual Machine Disk (VMDK) attaching, from the original system to the target (expanded) system. If you leave snapshots on the original system and attach it to the target system, the target system won't power on because of snapshot inconsistency.

### Productivity Tools Upgrade Notice

If a previously deployed Productivity Tools package has a different version or build number from a newly deployed Productivity Tools package and the upgrade is not blocked, your Productivity Tools client will notify you with an upgrade warning dialog box.

### SNMP v2 Community Names

There is no default SNMP v2 community name entry in this release of Cisco Webex Meetings Server. The system will remove the existing Cisco Webex Meetings Server 1.0 default Community Name, "CWS-Public," after upgrading. Only user-added SNMP v2 community names are maintained.

### End of Support Announcements

Cisco WebEx will not support the following browsers after February 2018:

- Microsoft Internet Explorer 7
- Microsoft Internet Explorer 8
- Microsoft Internet Explorer 9

**Note** End of support for these browsers includes Compatability Mode.

Cisco WebEx will not support the following operating systems after February 2018:

- Windows Vista
- Mac OSX 10.7
- Mac OSX 10.8

Cisco WebEx is also retiring sharing of .swf files in meetings. Users will no longer be able to select .swf files from the **File Share** option in the meetings.

### Translated Documentation

Translated documentation for this release of Cisco Webex Meetings Server is published 4–6 weeks after the English-language release.

## Known Issues and Notices

### Apple iOS 6.x and SSO

There is a known issue with Apple iOS 6.x. Single sign-on (SSO) does not work for internal users of iPad/iPhone who are using the Safari 6 web browser. An Apple defect that is fixed in iOS 7 caused this issue. The Safari bug ID is 13484525.

## Audio Configuration

On your audio configuration settings, G.711 provides better voice quality than G.729. See “About Configuring Your Audio Settings” in the *Cisco Webex Meetings Server Administration Guide* for more information.

## Automatic Upgrade Fails for an HA System

Automatic upgrade fails for a system configured with High Availability (HA). To work around this issue, log on to the newly-deployed Admin system. Open the CLI and run the following command:

**sed -i "s/find/findall/g" /opt/cisco/webex/webadmin/scripts/remoteGetSecondaryVMs**

After the script runs, repeat the update procedure.

## Cannot Share .mp4 Video File Format on Windows

When using QuickTime, the following message may appear: “QuickTime failed to initialize. Error # –2093. Please make sure QuickTime is properly installed on this computer.”

This error message can indicate that the file QuickTime.qts is missing, moved, or unusable. The QuickTime.qts file is located in the \WINDOWS\SYSTEM directory. To resolve this symptom, completely remove and reinstall QuickTime.

1. Download the latest version of the QuickTime Player http://www.apple.com/quicktime/download/.
2. Uninstall QuickTime using the **Add or Remove Programs** control panel. Ensure that you select **Uninstall Everything**.
3. Delete the contents of the Temp folder, C:\WINDOWS\TEMP (if it exists).
4. Install QuickTime using the version of the QuickTime you downloaded.
5. Restart Windows.

## Dashboard Issue Failure to Display Meetings That Have Started

In this release of Cisco Webex Meetings Server, the dashboard can fail to display certain meetings as having started. This issue occurs in the following scenario:

A meeting is scheduled with the **Allow participants to join teleconference before host** setting enabled. A participant joins the meeting by phone but does not join the web portion. The dashboard should indicate that this meeting has started and has one participant but it does not. This issue can cause users to schedule multiple meetings resulting in performance issues.

## Dial-in and Dial-Out Connections to an In-Progress Meeting

When a meeting fails over from one data center to another, the dial-in and dial-out connections to that meeting do not automatically reconnect. To reestablish the connections, participants hang up and manually dial back in.

This problem may occur when:

- The installed system is a large MDC.
- The meeting is started while one of the data centers is in Maintenance Mode or is powered down.
- When, after Maintenance Mode is turned off or the data center is powered on, another data center is powered off or placed into Maintenance Mode.

## IP Communicator 7.0.x Endpoints

IP Communicator 7.0.x endpoints joining CWMS meetings can introduce audio quality issues (echo and other noises) to a conference if either of the following conditions occur:

- IP Communicator is not muted.
- A participant using IP Communicator becomes the active speaker.

To prevent this issue, fine tune the IP Communicator environment (for example, the headset, microphone, and speaker) or use a different traditional phone.

## Keeping Your Hostname While Changing Your Virtual Machine IP Address

Never change the DNS entries for the hostnames that are configured in your deployment. You can change the hostname of a virtual machine that is part of your deployment. The corresponding IP address is picked up automatically from the DNS. To change the IP address of a virtual machine and keep the same hostname, perform the following steps:

1. Configure a temporary hostname in the DNS.
2. Change the hostname of the virtual machine to the temporary hostname that you configured.
3. Take the system out of maintenance mode for the new hostname change to take effect.

   Your original hostname is not part of the deployment after this change.
4. Change the IP address of the original hostname in the DNS to the new IP address.
5. Change the temporary hostname of the virtual machine to the original hostname.
6. Take the system out of maintenance mode for the hostname change to take effect.

   Now the original hostname is configured with your new IP address.

## Update from 3.0 Patch 1 Fails

Updating from Release 3.0 Patch 1 (3.0.1.33) fails because there is incorrect data in the cwms.pub file. Before you update from 3.0 Patch 1, apply the following workaround for this issue.

1. Go to https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvj70890.
2. Download the attached file: `fix_update.zip` and copy it to `/archive` directory on the primary Admin VM.
3. Use SSH to connect to the primary Admin VM, and navigate to the `/archive` directory.
4. Unzip the file: **unzip fix_update.zip**.
5. Make the unzipped file executable: **chmod +x fix_update**.
6. Run the executable: **./fix_update**.
7. After you see the `Success` message, proceed with the update.

## Upgrade Fails When Using VMware vCenter 6.5

The Cisco Webex Meetings Server upgrade can fail if you are using VMware vCenter 6.5. This issue occurs because the `ciscoOrion_versionStr.orion` variable is empty. You can work around the issue by

entering the correct CWMS version for the variable. For more information, see *Troubleshooting Guide for Cisco Webex Meetings Server Release*.

# Caveats

We report open and resolved customer-found bugs of severity 1 to 3.

**Procedure**

You can find details about listed bugs and search for other bugs by using the Cisco Bug Search Tool.

**Note** For more info on using the Bug Search, see Bug Search Tool Help.

## Closed Caveats in Cisco Webex Meetings Server Release 3.0MR3

There are no closed caveats for Cisco Webex Meetings Server Release 3.0MR3 (Build 3.0.1.3119).

## Open Caveats in Cisco Webex Meetings Server Release 3.0MR3

There are no open caveats for Cisco Webex Meetings Server Release 3.0MR3 (Build 3.0.1.3119).

## Resolved Caveats in Cisco Webex Meetings Server Release 3.0MR3

The following table lists caveats (bugs) that were open in a previous release, and fixed for this release.

***Table 1: Resolved Caveats in Cisco Webex Meetings Server Release 3.0MR3 (Build 3.0.1.3119)***

| Caveat ID Number | Severity | Description |
|---|---|---|
| CSCvr09779 | 4 | NFS storage mount procedure taking too long to reconnect storage causing various issues |

## Closed Caveats in Cisco WebEx Meetings Server Release 3.0MR2

The following table lists caveats that are closed in this maintenance release.

***Table 2: Closed Caveats for Cisco WebEx Meetings Server Release 3.0MR2 (3.0.1.2083)***

| Identifier | Severity | Description |
|---|---|---|
| CSCvm08749 | 3 | Edge cannot start 3.0MR1 meeting directly when downgraded from 3.0MR2, TFS can |

## Open Caveats in Cisco WebEx Meetings Server Release 3.0MR2

The following table lists caveats that are open in this maintenance release.

*Table 3: Open Caveats for Cisco WebEx Meetings Server Release 3.0MR2 (3.0.1.2083)*

| Identifier | Severity | Description |
|---|---|---|
| CSCvj26311 | 3 | CWMS keep sending clear event 10 seconds before the triggering event |
| CSCvm10347 | 3 | Should not download file to user\appdata again when online play nbr after installed nbr msi |
| CSCvm13358 | 3 | Meeting client joined from Jabber cannot share multimedia files from presenter |

## Resolved Caveats in Cisco WebEx Meetings Server Release 3.0MR2

The following table lists caveats that were open in a previous release and that are fixed in this maintenance release.

*Table 4: Resolved Caveats for Cisco WebEx Meetings Server Release 3.0MR2 (3.0.1.2083)*

| Identifier | Severity | Description |
|---|---|---|
| CSCvj47476 | 2 | CWMS MACC crash on Media1 |
| CSCvk56421 | 2 | Guest users unable to join meetings after initial connection session expiration |
| CSCvm06724 | 2 | Outlook keeps disabling PT plugin because of slow loading. |
| CSCvj64772 | 2 | Video quality downgraded and show low bandwidth sometime |
| CSCvj16620 | 3 | Test meeting on Admin page not working when the Primary admin is down and Ha is UP |
| CSCvj60972 | 3 | Piling up of zombie processes leads to a machine going to DOWN state |
| CSCvi96135 | 3 | MACC stops handling any new SIP message |
| CSCvj26329 | 3 | splitMeeting when "tas findconf" behind of "macc endconf" |
| CSCvk23611 | 3 | Attendee cannot join exception meeting via series meeting URL if s/he logged in site in advance |
| CSCvk39163 | 3 | Incorrect translation for failed cucm sync string in sync completed notification email |

| Identifier | Severity | Description |
|---|---|---|
| CSCvk23643 | 3 | JBH attendee join a different mtg via series mtg URL if s/he logged in site in advance |
| CSCvk35712 | 3 | Media VM does not establish reverse connection to the IRP on port 64002 |
| CSCvk15922 | 3 | The error info is not friend and can't identify the problem clearly to customer. |
| CSCvk38192 | 3 | The post call meeting summary is not sending after every meeting |
| CSCvm11920 | 3 | Users Send E-mail from Mobile device Get Stuck In Draft Folder Outlook 2010 |
| CSCvk63371 | 3 | WebEx App not showing all meetings in MyMeetings list |
| CSCvj93519 | 3 | WebEx App shows error code 100200 for Apple iOS when joining, meeting now or scheduling meeting. |
| CSCvj67100 | 3 | Webex users got disconnected from their session |
| CSCvk29210 | 3 | When collecting infocap logs mmp/eureka/tahoe archives are collected for the day before |

## Closed Caveats for Cisco WebEx Meetings Server Release 3.0MR1

There are no closed caveats for Cisco WebEx Meetings Server Release 3.0MR1 (3.0.1.1068).

## Open Caveats for Cisco WebEx Meetings Server Release 3.0MR1

The following table lists caveats that are open in this maintenance release.

***Table 5: Open Caveats for Cisco WebEx Meetings Server Release 3.0MR1 (3.0.1.1068)***

| Identifier | Severity | Headline |
|---|---|---|
| CSCvj47476 | 2 | CWMS MACC crash on Media1 (with coredump file) |
| CSCvi96135 | 3 | MACC stops handling any new SIP message |
| CSCvj16620 | 3 | Test meeting on Admin page not working when the Primary admin is down and Ha is UP |

| Identifier | Severity | Headline |
|---|---|---|
| CSCvj26311 | 3 | CWMS keep sending clear event 10 seconds before the triggering event. |
| CSCvj26329 | 3 | splitMeeting when "tas findconf" behind of "macc endconf" |

## Resolved Caveats for Cisco WebEx Meetings Server Release 3.0MR1

The following table lists caveats that were open in earlier releases of Cisco WebEx Meetings Server, and resolved in this maintenance release.

***Table 6: Resolved Caveats for Cisco WebEx Meetings Server Release 3.0MR1 (3.0.1.1068)***

| Identifier | Severity | Headline |
|---|---|---|
| CSCvh85440 | 1 | Cisco WebEx Advanced Recording Format Remote Code Execution Vulnerability |
| CSCvh85453 | 1 | Cisco WebEx Advanced Recording Format Remote Code Execution Vulnerability |
| CSCvh48727 | 2 | Audio engine cannot handle multiple channel data properly |
| CSCvh54136 | 2 | Logged in user see error message when start\|schedule meeting after admin change it to attendee only |
| CSCvh56853 | 2 | Update OpenSSL in CWMS |
| CSCvh58236 | 2 | Total video minutes in meeting summary / custom reports inaccurate on CWMS 2.8 |
| CSCvh65396 | 2 | Cannot join meeting via Chrome, it launches many CiscoWebExStart process |
| CSCvh66600 | 2 | Chrome 62/63 is intermittently unable to launch a WebEx meeting or takes over a 1 minute to start |
| CSCvh70228 | 2 | Cisco WebEx Advanced Recording Format Player Remote Code Execution Vulnerability |
| CSCvh75126 | 2 | Our WebEx don't work with blackmagic capture card, across it connecting our camera. |
| CSCvh76987 | 2 | Sometimes cannot submit new password when change password via forgot link |
| CSCvi10746 | 2 | Cisco WebEx Clients Remote Code Execution Vulnerability |
| CSCvi12585 | 2 | CWMS Backup fails if HA Admin is in DB Read/Write Role |
| CSCvi18479 | 2 | DB backup failed on CWMS 3.0 with secure storage |

| Identifier | Severity | Headline |
|---|---|---|
| CSCvh94758 | 2 | Presenter should not auto leave meeting after share youtube video in DS about 15 mins |
| CSCvi23617 | 2 | uploaded a Logo under Extended Branding is not shown |
| CSCvi24996 | 2 | After modifying the session type, the CMWS API SM interface call failed. Can not schedule meeting |
| CSCvi37153 | 2 | Wrong timezone display for Brasilia & Fiji |
| CSCvi41008 | 2 | AS will freeze around 30s for one pair of presenter/attendee |
| CSCvi46739 | 2 | Meeting number showing as 0 on dashboard for the previous instance of the same PCN meeting |
| CSCvi48991 | 2 | Custom PT email template with %Meeting Number No Spaces% variable NOT working with some PT languages |
| CSCvi75489 | 2 | CWMS 2.8MR1 SSLGW crashes in slow client BW and large recrodings on the system |
| CSCvi76477 | 2 | <![CDATA shows before the webex link when send invite using productivity tools |
| CSCvc47765 | 2 | Increase HSTS max age timer |
| CSCvj62655 | 2 | Cron jobs stop working after reload |
| CSCvh96985 | 3 | CA Audit logs are not rotating |
| CSCvh98756 | 3 | DIMON logs are not rotating |
| CSCvi95251 | 3 | Raise hand feature is not showing notification in some cases |
| CSCvi18561 | 3 | Secure Teleconferencing Certificate showing warning that it will expire while its valid |
| CSCvi10537 | 3 | db_helath.sh is not working after CWMS 3.0 deploy until first reboot |
| CSCvh87477 | 3 | Audit log alarm message needs to be rewritten to portray correct symptom. |
| CSCvh49427 | 3 | Meeting Audit Log on CWMS 2.8 not pushed to remote Syslog server |

## Resolved Caveats in Cisco WebEx Meetings Server Release 3.0

The following table lists caveats that were open in earlier releases of Cisco WebEx Meetings Server, and resolved in this release.

*Table 7: Resolved Caveats for Cisco WebEx Meetings Server Release 3.0 (Build 3.0.1.27)*

| Identifier | Severity | Description |
|---|---|---|
| CSCvd97638 | 1 | Orion 3.0 - Spring Framework - CIAM alerts |
| CSCve10764 | 1 | Cisco WebEx Network Recording Player Remote Code Execution Vulnerability |
| CSCve10771 | 1 | Cisco WebEx Network Recording Player Buffer Overflow Vulnerability |
| CSCvg27731 | 1 | Evaluation of orion for Apache Tomcat October 2017 vulnerability |
| CSCvg54853 | 1 | Cisco WebEx Network Recording Player Remote Code Execution Vulnerability |
| CSCvg54868 | 1 | Cisco WebEx Network Recording Player Remote Code Execution Vulnerability |
| CSCvd97572 | 2 | Orion 3.0 - bind - CIAM alerts |
| CSCvd97577 | 2 | Orion 3.0 - curl - CIAM alerts |
| CSCvd97605 | 2 | Orion 3.0 - glibc - CIAM alerts |
| CSCvd97608 | 2 | Orion 3.0 - kernel - CIAM alerts |
| CSCvd97614 | 2 | Orion 3.0 - libcurl - CIAM alerts |
| CSCvd97622 | 2 | Orion 3.0 - libxslt - CIAM alerts |
| CSCvd97627 | 2 | Orion 3.0 - lighttpd - CIAM alerts |
| CSCvf36064 | 2 | Multiple Vulnerabilities in kernel |
| CSCvf36066 | 2 | Sudo Parsed tty Information Privilege Escalation Vulnerability |
| CSCvf36070 | 2 | Cisco WebEx Meetings Server libxml2 Vulnerabilities |
| CSCvf41006 | 2 | Cisco WebEx Meetings Server Denial of Service Vulnerability |
| CSCvf46318 | 2 | too many requests for meeting (re)scheduled from PT |
| CSCvf61657 | 2 | When scheduling/modifying meeting in PT, Outlook would freeze for a minute before finishing |
| CSCvf68695 | 2 | CWMS Unauthorized Meeting Greeting Modification |
| CSCvf74541 | 2 | xalan in ssotokenutil has vulnerabilities with CVSS 7.5 |
| CSCvf85562 | 2 | Cisco WebEx Meetings Server Cross-Site Scripting Vulnerability |
| CSCvg10757 | 2 | NodeManager constantly restarting Tahoe and CMS components on Media VM |
| CSCvg17788 | 2 | Remove DNS query for incorrect client requests |
| CSCvg19328 | 2 | On user session expiration, browsers flood the system with http requests. |
| CSCvg78837 | 2 | Cisco WebEx Network Recording Player Buffer Overflow Vulnerability |

| Identifier | Severity | Description |
|---|---|---|
| CSCvg78856 | 2 | Cisco WebEx Advanced Recording Format Player Remote Code Execution Vulnerability |
| CSCuy82973 | 3 | Evaluation of TNS Listener Poison Attack for Cisco WebEx Meetings Server |
| CSCvd97910 | 3 | Orion 2.8 - Nessus findings - multiple openssl vulnerabilities - version used in ruby |
| CSCve59084 | 3 | CWMS OVA can not be deployed on vCenter 6.5 |
| CSCvf36041 | 3 | Multiple Vulnerabilities in bind |
| CSCvf36060 | 3 | Multiple Vulnerabilities in glibc |
| CSCvf59152 | 3 | CWMS Blast Dial with Call Attempts Unlimited calls the participants only 20 sec |
| CSCvf72983 | 3 | Pausing a recording during a meeting, doesn't actually pause the entire recording but only audio |
| CSCvf79684 | 3 | space between first and last name. |
| CSCvf79907 | 3 | CMS_Audio_Ports_Limit value is returned to default after system restart |
| CSCvf91444 | 3 | Missing time zone for S. America Eastern Standard Time |
| CSCvg04041 | 3 | User email address change fails due to existing entry in wbxnbrshareparticipantsinfo table |
| CSCvg17453 | 3 | Cannot start recurrence meeting from Outlook invitation email when deleting single occurrence |
| CSCvg17669 | 3 | In scheduled meetings table in Today's tab, Host's first and last name are not sync with database |
| CSCvg25560 | 3 | MC sends site URL on rejoin |
| CSCvg30766 | 3 | can not join into CWMS Webex meeting by telephony call in |
| CSCvg40121 | 3 | /opt directory slowly growing in size due to temp files in /opt/cisco/webex/webadmin/ca/tmp |
| CSCvg41102 | 3 | DB replication is limited due to high number of ruby processes on HA Admin |
| CSCvg44570 | 3 | Blast dial does not consider country code and area code for matching user |
| CSCvg86214 | 3 | Cannot open the occurrence meeting if enable 'Add digital signature to outgoing messages' |
| CSCvg89736 | 3 | Recurrence Daily Every Week Day future meeting schedule always starts on Monday of the week |
| CSCvh01622 | 3 | CWMS meeting info using API, missing meeting_id |

### Open Caveats in Cisco WebEx Meetings Server Release 3.0

The following table lists caveats that are open in this release.

*Table 8: Open Caveats for Cisco WebEx Meetings Server Release 3.0 (Build 3.0.1.27)*

| Identifier | Severity | Description |
|---|---|---|
| CSCvh31629 | 3 | Video thumbnail views are missing in video fullscreen |
| CSCvh48727 | 3 | Audio engine cannot handle multiple channel data properly |
| CSCvh54136 | 3 | Logged in user see error message when start\|schedule meeting after admin change it to attendee only |
| CSCvj02258 | 3 | Auto-uprade to 3.0 fails from the system with HA |

### Closed Caveats in Cisco WebEx Meetings Server Release 3.0

There are no closed caveats for Cisco WebEx Meetings Server Release 3.0 (Build 3.0.1.27).

## Additional Information and Service Requests

For information about submitting a service request, and for additional information, you can go to http://www.cisco.com/c/en/us/support/index.html.

You can also subscribe to Cisco Security RSS feeds and receive notifications when new information is available. Content feeds are available in both the 1.0 and 2.0 versions of the RSS format. Visit http://tools.cisco.com/security/center/rss.x?i=44.