

Cisco Security Advisory: Multiple Cisco WebEx WRF Player Vulnerabilities

Advisory ID: cisco-sa-20091216-webex

<http://www.cisco.com/warp/public/707/cisco-sa-20091216-webex.shtml>

Revision 1.1

Last Updated 2009 December 23 1800 UTC (GMT)

For Public Release 2009 December 16 1600 UTC (GMT)

Please provide your [feedback](#) on this document.

Contents

[Summary](#)

[Affected Products](#)

[Details](#)

[Vulnerability Scoring Details](#)

[Impact](#)

[Software Versions and Fixes](#)

[Workarounds](#)

[Obtaining Fixed Software](#)

[Exploitation and Public Announcements](#)

[Status of this Notice: FINAL](#)


[Distribution](#)

[Revision History](#)

[Cisco Security Procedures](#)

Summary

Multiple buffer overflow vulnerabilities exist in the Cisco WebEx Recording Format (WRF) Player. In some cases, exploitation of the vulnerabilities could allow a remote attacker to execute arbitrary code on the system of a targeted user.

The Cisco WebEx WRF Player is an application that is used to play back WebEx meeting recordings that have been recorded on the computer of an on-line meeting attendee. The WRF Player can be automatically installed when the user accesses a WRF file that is hosted on a WebEx server. The WRF Player can also be manually installed for offline playback after downloading the application from www.webex.com .

If the WRF Player was automatically installed, the WebEx WRF Player will be automatically upgraded to the latest, non-vulnerable version when users access a WRF file hosted on a WebEx server. If the WebEx WRF Player was manually installed, users will need to manually install a new version of the player after downloading the latest version from www.webex.com .

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20091216-webex.shtml>.


[\[Expand all sections\]](#) [\[Collapse all sections\]](#)

☐ Affected Products

☐ Vulnerable Products

The vulnerabilities disclosed in this advisory affect the Cisco WebEx WRF Player. Microsoft Windows, Apple Mac OS X, and Linux versions of the player are affected. Affected versions of the WRF Player are those prior to the "first fixed" versions, which are shown in the section "[Software Versions and Fixes](#)" of this advisory.

To check if a Cisco WebEx server is running an affected version of the WebEx client build, users can log in to their Cisco WebEx server and go to the Support -> Downloads section. The version of the WebEx client build will be displayed on the right-hand side of the page under "About Support Center", for example "Client build: 27.11.0.3328."

Cisco recommends that users upgrade to the most current version of the player that is available from <http://www.webex.com/downloadplayer.html> . However, users can verify the installed version of the WRF Player to determine if it is affected by these vulnerabilities. In order to do so, an administrator must examine the version numbers of the installed files and determine if every version of the files contains the fixed code. Detailed instructions on how to verify the version numbers are provided in the following sections.

Microsoft Windows

There are three dynamically linked libraries (DLLs) that were updated on the Microsoft Windows platform in order to address the vulnerabilities described in this advisory. These files are located in the folder C:\Program Files\WebEx\Record Playback. The version number of the DLLs can be identified by browsing the Record Playback directory in Windows Explorer and right clicking the file name in order to view the properties. The version or details tab of the properties page provides details on the library version. The table below gives the first fixed version number for each DLL. If the installed versions are equal to, or greater than the versions provided in the table, the system is not vulnerable.

Library	T26	T27
atas32.dll	2.5.49.4	2.6.10.1
ataudio.dll	26.2009.6.6	27.2009.6.17
atrpuui.dll	921.2008.7.2326	921.2009.6.2027

Mac

There are two package bundles that were updated on the Macintosh platform in order to address the vulnerabilities described in this advisory. These files are located in each users home directory, which can be accessed in ~/Library/Application Support/WebEx Folder/824 for systems connected to servers running T26 and ~/Library/Application Support/WebEx Folder/924 for systems connected to servers running T27. The version can be located by browsing the appropriate folder in the Finder and control-clicking the file name. Once the menu is displayed, select “show package contents” and then double clicking the Info.plist file. The version number is shown at the bottom of the displayed table.

Bundle	T26	T27

ataudio.bundle	7.5.0.5	8.5.0.2
WebEx Player.app	8.0.1.3	10.14.11.7

Linux

There are two shared objects that were updated on the Linux platform in order to address the vulnerabilities described in this advisory. These files are located in the ~/.webex directory. The version number of the shared object can be obtained by performing a directory listing with the 'ls' command. The version number is provided after the .so extension. The following table provides the first non-vulnerable version of each object.

Shared Object	T26	T27
ataudio.so	1.0.26.7	1.27.13.1
atrecply	1.0.26.14	1.0.27.12


☐ Products Confirmed Not Vulnerable

The Cisco WebEx Player for the WebEx Advanced Recording Format (ARF) file format is not affected by these vulnerabilities.

No other Cisco products are currently known to be affected by these vulnerabilities.

[Top of the section](#) [Close Section](#)

☐ Details

The WebEx meeting service is a hosted multimedia conferencing solution that is managed by and maintained by Cisco WebEx. The WebEx Recording Format (WRF) is a file format that is used to store WebEx meeting recordings that have been recorded on the computer of an on-line meeting attendee. The WRF Player is an application that is used to play back and edit WRF files (files with .wrf extensions). The WRF Player can be automatically installed when the user accesses a WRF file that is hosted on a WebEx server (stream playback mode). The WRF Player can also be manually installed after downloading the application from www.webex.com  to play back WRF files locally (offline playback mode).

Multiple buffer overflow vulnerabilities exist in the WRF Player. The vulnerabilities may lead to a

crash of the WRF Player application, or in some cases, lead to remote code execution.

To exploit a vulnerability, a malicious WRF file would need to be opened by the WRF Player application. An attacker may be able to accomplish this by providing the malicious WRF file directly to users (for example, via e-mail), or by convincing users to visit a malicious website. The vulnerability cannot be triggered by users attending a WebEx meeting.

These vulnerabilities have been assigned the following Common Vulnerabilities and Exposures (CVE) identifiers:

- CVE-2009-2875
- CVE-2009-2876
- CVE-2009-2877
- CVE-2009-2878
- CVE-2009-2879
- CVE-2009-2880

[Top of the section](#) [Close Section](#)

▣ Vulnerability Scoring Details

Cisco has provided scores for the vulnerabilities in this advisory based on the Common Vulnerability Scoring System (CVSS). The CVSS scoring in this Security Advisory is done in accordance with CVSS version 2.0.

CVSS is a standards-based scoring method that conveys vulnerability severity and helps determine urgency and priority of response.

Cisco has provided a base and temporal score. Customers can then compute environmental scores to assist in determining the impact of the vulnerability in individual networks.

Cisco has provided an FAQ to answer additional questions regarding CVSS at

<http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html> .

Cisco has also provided a CVSS calculator to help compute the environmental impact for individual networks at

<http://intellishield.cisco.com/security/alertmanager/cvss> .

Multiple Cisco WebEx Player Buffer Overflow Vulnerabilities

Calculate the environmental score of [<all vulnerabilities in this advisory>](#)

CVSS Base Score - **9.3**

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Medium	None	Complete	Complete	Complete

CVSS Temporal Score - **7.7**

Exploitability	Remediation Level	Report Confidence
Functional	Official-Fix	Confirmed

[Top of the section](#) [Close Section](#)

Impact

Successful exploitation of the vulnerabilities described in this document could result in a crash of the Cisco WebEx WRF Player application, and in some cases, allow a remote attacker to execute arbitrary code on the targeted system with the privileges of the user running the WRF Player application.

[Top of the section](#) [Close Section](#)

Software Versions and Fixes


The table below contains "First Fixed" information for the Cisco WebEx WRF Player that is automatically downloaded from a WebEx site when a WRF hosted on a WebEx site is accessed (stream playback mode). Fixes are cumulative within a major release so for example, if release 27.10.1 is fixed, then release 27.10.2 will have the fix too.

Platform	Major Release 26.x	Major Release 27.x
Microsoft Windows	26.49.32; available now except lockdown sites	27.10.x; available now for non-PSO and non-lockdown sites

Mac OS X	26.49.35; available early February 2010	27.11.8; available now for non-PSO and non- lockdown sites
Linux	26.49.35; available early February 2010	27.11.8; available now for non-PSO and non- lockdown sites

PSO and lockdown sites running 27.x will receive the fixes for these vulnerabilities during the next emergency patching (EP) cycle. This advisory will be updated to indicate a specific timeline once one is available.

If the WRF Player was automatically installed, the WebEx WRF Player will be automatically upgraded to the latest, non-vulnerable version when users access a WRF file hosted on a WebEx server.

If the WebEx WRF Player was manually installed, users will need to manually install a new version of the player after downloading the latest version from www.webex.com .

[Top of the section](#) [Close Section](#)

☐ Workarounds

There are no workarounds for the vulnerabilities disclosed in this advisory.

[Top of the section](#) [Close Section](#)

☐ Obtaining Fixed Software

Cisco has released free software updates that address these vulnerabilities. Prior to deploying software, customers should consult their maintenance provider or check the software for feature set compatibility and known issues specific to their environment.

Customers may only install and expect support for the feature sets they have purchased. By installing, downloading, accessing or otherwise using such software upgrades, customers agree to be bound by the terms of Cisco's software license terms found at http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html , or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml> .

Do not contact psirt@cisco.com or security-alert@cisco.com for software upgrades.


Customers that need additional information can contact WebEx Global Support Services and Technical Support. WebEx Global Support Services and Technical Support can be reached through the WebEx support site at <http://support.webex.com/support/support-overview.html> or by phone at +1-866-229-3239 or +1-408-435-7088.

Customers outside of the United States can reference the following link for local support numbers: <http://support.webex.com/support/phone-numbers.html>.

[Top of the section](#) [Close Section](#)

☐ **Exploitation and Public Announcements**

The Cisco PSIRT is not aware of malicious use of the vulnerabilities described in this advisory.

These vulnerabilities were discovered and reported to Cisco by Xiaopeng Zhang and Zhenhua Liu of Fortinet's FortiGuard Labs. The FortiGuard Labs advisory is available at <http://www.fortiguard.com> . Cisco would like to thank FortiGuard Labs for reporting these vulnerabilities to us and for working with us on a coordinated disclosure.

[Top of the section](#) [Close Section](#)

☐ **Status of this Notice: FINAL**

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

A stand-alone copy or Paraphrase of the text of this document that omits the distribution URL in the following section is an uncontrolled copy, and may lack important information or contain factual errors.

[Top of the section](#) [Close Section](#)

☐ Distribution

This advisory is posted on Cisco's worldwide website at:

<http://www.cisco.com/warp/public/707/cisco-sa-20091216-webex.shtml>

In addition to worldwide web posting, a text version of this notice is clear-signed with the Cisco PSIRT PGP key and is posted to the following e-mail and Usenet news recipients.

- cust-security-announce@cisco.com
- first-bulletins@lists.first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk
- comp.dcom.sys.cisco@newsgate.cisco.com

Future updates of this advisory, if any, will be placed on Cisco's worldwide website, but may or may not be actively announced on mailing lists or newsgroups. Users concerned about this problem are encouraged to check the above URL for any updates.

[Top of the section](#) [Close Section](#)

☐ Revision History

Revision 1.1	2009-December-23	Revised the Vulnerable Products section
Revision 1.0	2009-December-16	Initial public release

[Top of the section](#) [Close Section](#)

☐ Cisco Security Procedures

Complete information on reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information from Cisco, is available on Cisco's worldwide website at <http://www.cisco.com/en/US/products/>

[products_security_vulnerability_policy.html](#). This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

[Top of the section](#) [Close Section](#)

Help us help you.



Please rate this document.

- Excellent
- Good
- Average
- Fair
- Poor



This document solved my problem.

- Yes
- No
- Just browsing



Suggestions for improvement:

(256 character limit)



[Home](#)

[How to Buy](#)

[Login](#)

[Profile](#)

[Feedback](#)

[Site Map](#)

[Help](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 - 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)