

[Solutions](#) [Products](#) [Ordering](#) [Support](#) [Partners](#) [Training](#) [Corporate](#)[Security Advisories](#)

Cisco Security Advisory: Vulnerability in Cisco WebEx Meeting Manager ActiveX Control

Advisory ID: cisco-sa-20080814-webex

<http://www.cisco.com/warp/public/707/cisco-sa-20080814-webex.shtml>

Revision 1.3

Last Updated 2008 August 29 1530 UTC (GMT)

For Public Release 2008 August 14 2230 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

A buffer overflow vulnerability exists in an ActiveX control used by the WebEx Meeting Manager. Exploitation of this vulnerability could allow a remote attacker to execute arbitrary code on the user client machine. The WebEx Meeting Manager is a client-side program that is provided by the Cisco WebEx meeting service. The Cisco WebEx meeting service automatically downloads, installs, and configures Meeting Manager the first time a user begins or joins a meeting.

When users connect to the WebEx meeting service, the WebEx Meeting Manager is automatically

upgraded to the latest version. There is a manual workaround available for users who are not able to connect to the WebEx meeting service.

Cisco WebEx is in the process of upgrading the meeting service infrastructure with fixed versions of the affected file.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080814-webex.shtml>.

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

☐ Affected Products

☐ Vulnerable Products

The WebEx Meeting Manager downloads several components to meeting participants before they join a WebEx meeting. The vulnerability in this Security Advisory affects the *atucfobj.dll* library.

☐ Products Confirmed Not Vulnerable

No other Cisco products are currently known to be affected by this vulnerability.

[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. When a meeting participant connects to the WebEx meeting service through a web browser, the WebEx meeting service installs several components of the WebEx Meeting Manager browser plugin on the meeting participant's system.

WebEx Meeting Manager includes *atucfobj.dll*, a DLL that allows meeting participants to view Universal Communication Format (UCF) contents. This library contains a buffer overflow vulnerability that could allow an attacker to execute arbitrary code.

The WebEx meeting service currently maintains three different versions of software. WebEx meeting service servers run one of the following versions: WBS 23, WBS 25, or WBS 26.

Note: In addition to the three currently maintained versions of WebEx software, pre WBS 23 software versions may also be impacted by this vulnerability.

This vulnerability is documented in WebEx Bug IDs 292551 for WBS 26 and 306639 for WBS 25. This vulnerability has been assigned Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-3558.

Identifying WebEx Meeting Service Version

The following procedure will allow a meeting participant to identify the version of client software provided by a WebEx site. The procedure varies slightly depending on the software version. The URL in all the following examples is provided to meeting participants in the WebEx meeting invitation.

Client build numbers adhere to the format of **XX.YY.ZZ.WWWW**. The first number indicates the major version number of the software release. For example, a client build number of **26.49.9.2838** indicates a WBS 26-based software client.

For the WBS 26 version:

1. Browse to the WebEx meeting server at **https://<sitename>.webex.com/**.
2. Select **Support** from the left side of the web page.
3. Select **Downloads** from the left side of the web page.
4. The version of the client software that is provided by the server is listed next to **Client build**.

For WebEx servers that are running WBS 26, the first fixed version is 26.49.9.2838. Client build versions prior to 26.49.9.2838 are vulnerable.

For the WBS 25 version:

1. Browse to the WebEx meeting server at **https://<sitename>.webex.com/**.
2. Select **Assistant** on the left side of the page.
3. Select the **Support** link.
4. Select the **Version** link, which is displayed on the right side of the top of the page.
5. The **Client Build** version is displayed in a pop-up window.

There is currently no fixed version for the WBS 25-based WebEx meeting service. This section of the Security Advisory will be updated when fixed version information is available.

For the WBS 23 version:

Servers that run WBS 23-based WebEx meeting service display version information using the following URL format:

https://<sitename>.webex.com/version/wbxversionlist.do?siteurl=<sitename>

On the redisplayed page the **Client versions in files** field will indicate the **Client Build**.

For example: The 'T23' in **WBXclient-T23L10NSP33EP13-1092.txt** indicates a WBS 23-based system.

Cisco WebEx is not planning to repair WBS 23-based software. Affected WBS 23-based servers will be upgraded to fixed WBS 26-based software.

Attack Vector Details

This Security Advisory addresses a vulnerable ActiveX control (*atucfobj.dll*). If *atucfobj.dll* is present on a client's computer, it may be possible for an attacker to embed malicious code into HTML content that calls an affected function in *atucfobj.dll* via ActiveX.

Users could encounter the malicious HTML in several ways. The most common manners are:

- Browsing to a web-site that contains the malicious content
- HTML that is embedded in e-mail messages

- HTML that is delivered via instant messaging applications

WebEx Upgrade Timeline

Upgrades from WBS 23 versions to WBS 26 are expected to be complete by the end of September 2008.

Fixed versions of WBS 25 are expected to be deployed by the end of September 2008.

Deployed versions of WBS 26 are fixed.

[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>.

The CVSS scoring for WebEx bug IDs 292551 and 306639 are identical because they reference the same vulnerability. The below scoring applies to both 292551 and 306639.

ActiveX Vulnerability in WebEx Meeting Manager					
Calculate the environmental score of 292551					
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 - 8.4					
Exploitability		Remediation Level		Report Confidence	
Functional		Workaround		Confirmed	

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

☐ Impact

Successful exploitation of the vulnerability may result in execution of arbitrary code.

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

☐ Software Versions and Fixes

The following table contains information on the WebEx meeting service software releases:

Software release	First Fixed release
WBS19	Vulnerable. Migrate to WBS25
WBS20	Vulnerable. Migrate to WBS25
WBS23	Vulnerable. Migration to WBS25 expected to be completed by the end of September 2008.
WBS25	Fixed release expected to be deployed by the end of September 2008.
WBS26	26.49.9.2838

Clients will receive an upgrade automatically in accordance with the process that is outlined in the Obtaining Fixed Software section of this advisory within the time frame that is outlined in the WebEx Upgrade Timeline subsection of this advisory.

Cisco WebEx will not offer the modified *atucfobj.dll* as a separate download.

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

☐ Workarounds

WebEx meeting participants who join a WebEx meeting that is hosted by a server with fixed software will download a fixed version of *atucfobj.dll* prior to joining the meeting.

Several other workarounds are described below in the following subsections.

Additional mitigation techniques that can be deployed on Cisco devices within the network are available in the Cisco Applied Mitigation Bulletin companion document for this advisory: <http://www.cisco.com/warp/public/707/cisco-amb-20080814-webex.shtml>.

Manually Upgrading WebEx Meeting Manager

Users can verify that the WebEx meeting service server they are connecting to is running fixed code via the method that is described in the subsection entitled Identifying WebEx Version subsection of the Details section of this Security Advisory.

If the WebEx server is running a version of software that is fixed, users can manually download and install the Meeting Manager client to ensure their versions of *atucfobj.dll* are not vulnerable.

Removing WebEx Meeting Manager

It is possible to remove the WebEx Meeting Manager component from Microsoft Windows by using the **Add or Remove Programs** utility in the Windows Control Panel:

1. In Windows, choose **Start > Control Panel**.
2. Double-click **Add or Remove Programs**.
3. Double-click **WebEx**.
4. In the pop-up menu, check the **Meeting Manager** box and click **Uninstall**.
5. Follow the prompts to complete the uninstall process and restart the system.

NOTE: After uninstalling the WebEx Meeting Manager, users that join a WebEx meeting that is hosted by a vulnerable version will again download and install a vulnerable *atucfobj.dll*.

Disabling atucfobj.dll by Setting the Kill Bit

It is possible to disable the execution of *atucfobj.dll* by using a configuration setting in Microsoft Windows. This method is called *setting the kill bit* for the DLL. Once set, this method prevents *atucfobj.dll* from loading, which prevents exploitation of the vulnerability.

Instructions for setting the kill bit in Microsoft Windows are available at the following location:

<http://support.microsoft.com/kb/240797>

Setting the kill bit for *atucfobj.dll* will persist even after a fixed version of the DLL is installed. To re-enable the use of *atucfobj.dll*, the kill bit will need to be unset.

To disable *atucfobj.dll* users must know the CLSID for the DLL. The CLSID for *atucfobj.dll* is **{32E26FD9-F435-4A20-A561-35D4B987CFDC}**

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

☐ Obtaining Fixed Software

As outlined in WebEx Upgrade Timeline section, WebEx meeting participants who join a WebEx meeting that is hosted by a server with fixed software will automatically download a fixed version of *atucfobj.dll* prior to joining the meeting.

Clients can also upgrade manually by following the instructions in the Manually Upgrading WebEx Meeting Manager subsection of the Workarounds section of this advisory.

Clients can protect themselves without first accessing a WebEx server by following the instructions in the Removing WebEx Meeting Manager subsection of the Workarounds section of this advisory.

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**

This issue has been publicly announced on multiple external forums and mailing lists.

Exploit code has been made available.

[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-20080814-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 1.3	2008-August-29	Update to Software Fixes section and update to the software naming scheme.
Revision 1.2	2008-August-18	Updated CVE identifier.
Revision 1.1	2008-August-15	Addition of AMB link, adjustment of site terminology, and update of legacy software impact in Details section.
Revision 1.0	2008-August-14	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)



Send

Home	How to Buy	Login	Profile	Feedback	Site Map	Help
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

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

© 2007 - 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)