

Cisco Security Response: Cisco Unified MeetingPlace Stored Cross-Site Scripting Vulnerability

<http://www.cisco.com/warp/public/707/cisco-sr-20090226-mtgplace.shtml>

For Public Release 2009 February 26 1800 UTC (GMT)

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

Contents

[Cisco Response](#)

[Additional Information](#)

[Status of this Notice: FINAL](#)

[Revision History](#)

[Cisco Security Procedures](#)

Cisco Response

This is the Cisco PSIRT response to an issue discovered and reported to Cisco by the National Australia Bank Security Assurance team regarding a cross-site scripting vulnerability in Cisco Unified MeetingPlace Web Conferencing.

The original report is available at the following link:

<http://www.securityfocus.com/archive/1/501251/30/0/threaded> 

The Cisco PSIRT greatly appreciates the opportunity to work with researchers on security vulnerabilities, and welcomes the opportunity to review and assist in product reports.

This vulnerability is documented in Cisco bug ID [CSCsv66321](#) ([registered](#) customers only) .

This Cisco Security Response is posted at the following link:

<http://www.cisco.com/warp/public/707/cisco-sr-20090226-mtgplace.shtml>.

Additional Information

Cisco Unified MeetingPlace Web Conferencing provides real-time collaboration functionality to an organization's intranet and Extranet, and integrates Cisco Unified MeetingPlace with a web server, thus providing users with a browser-based interface. Web Conferencing enables users to schedule and attend conferences, access meeting materials, and collaborate on documents from common web browsers.

Cisco Unified MeetingPlace contains a stored cross-site scripting vulnerability that could allow a remote, authenticated attacker to perform a persistent cross-site scripting attack by injecting HTML or Script code by way of the edit account page. The malicious input is subsequently included within the Account Details page as well as within the Meeting Details pages of any meeting that is scheduled by the affected account.

This vulnerability exists within all versions of Cisco Unified MeetingPlace.

Additional information regarding cross-site scripting can be found in the following document: [Cisco Applied Mitigation Bulletin: Understanding Cross-Site Scripting \(XSS\) Threat Vectors](#).

To determine the software version of a Cisco Unified MeetingPlace Web Conferencing server, access the MeetingPlace server home page by means of an HTTP session; the version information is provided at the bottom of the home page. The following output shows an example of the text that is shown when accessing the home page of a MeetingPlace Web Conferencing server running software version 6.0.417.0:

```
Version: 6.0.417.0
Copyright © 1996-2009 Cisco Systems, Inc. All rights reserved.
```

Software Versions and Fixes

This vulnerability is fixed in Cisco Unified MeetingPlace Web Conferencing software version 6.0 (517.0), also known as Maintenance Release 4 (MR4) for the 6.0 release, and version 7.0(2), also known as Maintenance Release 1 (MR1) for the 7.0 release.

The latest versions of Cisco MeetingPlace software can be downloaded from <http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=278875240> ([registered](#) customers only) .

The Cisco Unified MeetingPlace Web Server software is available at: <http://tools.cisco.com/support/downloads/go/Model.x?mdfid=278816725&mdfLevel=Software%20Version/Option&treeName=Voice%20and%20Unified%20Communications&modelName=Cisco%20Unified%20MeetingPlace%20Web%20Conferencing&treeMdfId=278875240> ([registered](#) customers only) .

When considering software upgrades, also consult <http://www.cisco.com/go/psirt> and any subsequent advisories to determine exposure and a complete upgrade solution.

In all cases, customers should exercise caution to be certain the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, contact the Cisco Technical Assistance Center (TAC) or your contracted maintenance provider for assistance.

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.

Revision History

Revision 1.0	2009-February-26	Initial public release.
--------------	------------------	-------------------------

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>.

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](#)

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