

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

Cisco Security Response: Cisco Unified MeetingPlace XSS Vulnerability

<http://www.cisco.com/warp/public/707/cisco-sr-20070808-mp.shtml>

Revision 1.1

Last Updated 2007 August 15 1500 UTC (GMT)

For Public Release 2007 August 08 1600 UTC (GMT)

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

Contents

[Cisco Response](#)

[Additional Information](#)

[Revision History](#)

[Cisco Security Procedures](#)

Cisco Response

This is the Cisco PSIRT response to an issue discovered and reported to Cisco by Roger Jefferiss and Rob Pope of SecureTest Ltd, UK regarding cross-site scripting (XSS) vulnerability in Cisco Unified MeetingPlace Web Conferencing.

The original report is available at the following link: <http://lists.grok.org.uk/pipermail/full-disclosure/2007-August/056073.html>.

We greatly appreciate the opportunity to work with researchers on security vulnerabilities, and welcome the opportunity to review and assist in product reports.

This vulnerability is documented in Cisco bug ID [CSCsi33940](#) ([registered](#) customers only) .

This Cisco Security Response is posted at the following link:
<http://www.cisco.com/warp/public/707/cisco-sr-20070808-mp.shtml>.

Additional Information

Cisco Unified MeetingPlace Web Conferencing (MP) 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.

Success Template (STPL) and Failure Template (FTPL) parameters are used to specify the return template of a user request. These should correspond to an actual template file that resides on the MP server's file system.

When MP servers running software versions 5.3.235.0 and earlier receive invalid input for the STPL or FTPL parameters, they return a HTML error template page. The returned HTML page contains the original inputted URL.

When this reflected XSS vulnerability is exploited, malicious code or a script is embedded within the URL and associated with either the STPL or FTPL parameter. The malicious code is usually in the form of a script embedded in the URL of a link or the code may be stored on the vulnerable server or malicious website. An unsuspecting user is enticed to follow a malicious link to a vulnerable MP server that injects (reflects) the malicious code back to the user's browser as the MP server does not have the requested template file associated with the STPL or FTPL parameter. Therefore, the MP server responds with the template used for error pages, which includes the requested URL with the malicious code, thus causing the target user's browser to execute it.

Software versions 5.3.333.0 and later of Cisco Unified MeetingPlace Web Conferencing will return an XML message with an embedded error code when receiving invalid input for the STPL and FTPL parameters. The error message is properly and securely formatted per the XML CDATA specification.

All 5.4 and 6.0 versions of Cisco Unified MeetingPlace Web Conferencing are unaffected by this vulnerability.

To determine the software version of a Cisco Unified MeetingPlace Web Conferencing server, access the MP server home page via an HTTP session; the version information is provided at the bottom of the home page. The following output shows an example of the text viewable when accessing the home page of a MeetingPlace Web Conferencing server running software version 5.3.447.4:

```
Copyright © 1992-2007 Cisco Systems, Inc. All Rights Reserved.  
Version: 5.3.447.4
```

Workarounds

For affected software releases of Cisco Unified MeetingPlace Web Conferencing, there are no known workarounds for this vulnerability.

Cisco recommends upgrading to a fixed release of Cisco Unified MeetingPlace Web Conferencing software.

Affected software versions:	5.3.235.0 and earlier.
-----------------------------	------------------------

Fixed software versions:	5.3.333.0 and later.
	All 5.4 and 6.0 versions.

For additional information on XSS attacks and the methods used to exploit these vulnerabilities, please refer to the Cisco Applied Intelligence Response "Understanding Cross-Site Scripting (XSS) Threat Vectors", which is available at the following link:

<http://www.cisco.com/warp/public/707/cisco-air-20060922-understanding-xss.shtml>

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.

Revision History

Revision 1.1	2007-August-15	Revised Workarounds section and added recommended software.
Revision 1.0	2007-August-08	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)

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.](#)