

[NEWS] Cisco Unified MeetingPlace XSS Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-08/msg00009.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 13 Aug 2007 12:46:51 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

Cisco Unified MeetingPlace XSS Vulnerability

SUMMARY

There exists a cross site scripting issue in Cisco MeetingPlace Application. The result of this is that when a specially crafted web page with a hidden arbitrary code could be executed on the host accessing the application.

DETAILS

Affected Versions:

This vulnerability has been confirmed in the following versions:

- * 4.3.0.246
- * 4.3.0.246.5
- * 5.3.104.0
- * 5.3.104.3

The following versions have been tested and are unaffected due to the fact they return an xml template:

- * 5.3.333.0
- * 5.3.447
- * 5.3.447.4

[NEWS] Cisco Unified MeetingPlace XSS Vulnerability

- * 5.4.70.0
- * 6.0.170.0

Cisco MeetingPlace provides a web based application for online meetings. It was discovered that a specially crafted script could be executed on certain parameters with in MeetingPlace application.

The result is script code execution in the local user context in the host. Preliminary tests concluded the system is vulnerable with most popular web browsers such as Microsoft Internet Explorer 7.0 and Mozilla Firefox 2.0 fully patched.

User intervention (e.g. clicking on a malicious link) is necessary to trigger the exploit.

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.

[NEWS] Cisco Unified MeetingPlace XSS 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

There are no known workarounds for this vulnerability.

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

ADDITIONAL INFORMATION

The information has been provided by <mailto:Disclosure@xxxxxxxxxxxxxx>
Disclosure.

=====

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@xxxxxxxxxxxxxx
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxx

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind. In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.