

# Cisco Security Response: Cisco Unified MeetingPlace XSS Vulnerability

Document ID: 99855

<http://www.cisco.com/warp/public/707/cisco-sr-20071107-mp.shtml>

## Revision 1.0

For Public Release 2007 November 07 1300 UTC (GMT)

---

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

---

[Cisco Response](#)

[Additional Information](#)

[Revision History](#)

[Cisco Security Procedures](#)

---

## Cisco Response

This is the Cisco PSIRT response to an issue that was discovered and reported to Cisco by Joren McReynolds regarding a cross-site scripting (XSS) vulnerability in Cisco Unified MeetingPlace Web Conferencing.

The original report is available at the following link: <http://secunia.com/advisories/26462/>

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 [CSCsk17122](#) ([registered](#) customers only) .

This Cisco Security Response is posted at the following link:

<http://www.cisco.com/warp/public/707/cisco-sr-20071107-mp.shtml>.

This vulnerability has been assigned CVE ID CVE-2007-5581.

## Additional Information

Cisco Unified MeetingPlace Web Conferencing (MeetingPlace) provides real-time collaboration functionality to an organization's intranet and extranet and integrates 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.

MeetingPlace is vulnerable to Cross Site Scripting (XSS) attacks from the login screen. When this XSS vulnerability is exploited, malicious code or script is embedded within the URL and associated with FirstName or LastName parameters.

The malicious code typically takes the form of a script that is embedded in the URL of a link. The malicious code may also be stored on the vulnerable server or a malicious website. An attacker could try to convince an unsuspecting user to follow a malicious link to a vulnerable MeetingPlace server that injects (reflects) the

malicious code back to the user's browser.

## Workarounds

There are no known workarounds for this vulnerability. Cisco recommends applying a hotfix to address the vulnerability.

Affected software versions	Hotfix
5.3 and prior versions	Affected, no hotfix available
5.4	5.4.156.2E
6.0	6.0.244.1A

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>

## Additional Information

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 1.0	2007–November–07	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](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>.

---

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. [Important Notices](#) and [Privacy Statement](#).

---

Updated: Nov 07, 2007

Document ID: 99855

---