

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

Cisco Security Response: Cisco CallManager Input Validation Vulnerability

<http://www.cisco.com/warp/public/707/cisco-sr-20070523-ccm.shtml>

Revision 1.0

For Public Release 2007 May 23 1600 UTC (GMT)

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

Contents

[Cisco Response](#)
[Additional Information](#)
[Revision History](#)
[Cisco Security Procedures](#)

Cisco Response

This is Cisco PSIRT's response to the statements made by Marc Ruef and Stefan Friedi from scip AG in their message "Cisco CallManager 4.1 Input Validation Vulnerability," posted on 2007 May 23 at 1600 UTC (GMT).

The original emails were posted to BugTraq and Full-Disclosure.

In their postings, Marc Ruef and Stefan Friedi illustrate how to bypass the web application firewall used in Cisco CallManager. This means of bypass can be used to display graphics, scripts, or other information downloaded from an external web site. This technique may also be used to conduct cross-site scripting attacks. Cisco confirms that the example the authors Ruef and Friedi provided bypasses the web application firewall and that there may be other methods for bypassing the web application firewall.

Cisco has made improvements to the input validation mechanisms in CallManager that may mitigate the risks associated with this security vulnerability. These improvements have been incorporated into 4.2(3)sr2, 3.3(5)sr3, 4.1(3)sr5 and 4.3(1)sr1. This issue is being tracked by the following Cisco Bug ID:

- [CSCsi12374](#) ([registered](#) customers only) -Improvements in User Input Validation

Service releases of CallManager software are available at the following link:
<http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml> ([registered](#) customers only)

Additional Information

Cisco CallManager is the software-based call-processing component of the Cisco IP telephony solution that extends enterprise telephony features and functions to packet telephony network devices, such as IP phones, media processing devices, voice-over-IP (VoIP) gateways, and multimedia applications. The vulnerability described in this response exists in the web application firewall used in CallManager. This feature is designed to prevent users from entering malicious code into the input fields used in CallManager forms. The vulnerability exists because the web application firewall fails to properly sanitize some potentially malicious tags.

To exploit these issues an attacker must convince an authenticated user to follow a specially crafted, malicious URL. A successful attack may result in the execution of arbitrary script code in the user's web browser.

For additional information on cross-site scripting (XSS) attacks and the methods used to exploit such 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/en/US/products/products_applied_mitigation_bulletin09186a008073f7b3.html

The Cisco PSIRT is not aware of any malicious use of the vulnerability described in this document.

This issue was reported to Cisco by Marc Ruef and Stefan Friedi from scip AG. We would like to thank Marc Ruef and Stefan Friedi for bringing this issue to our attention and for working with us toward coordinated disclosure of the issue. We greatly appreciate the opportunity to work with researchers on security vulnerabilities, and welcome the opportunity to review and assist in product reports.

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-May-23	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>.

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

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