

Cisco Security Response: Input Validation/Output Encoding Vulnerabilities in Cisco CallManager Allow Script Injection Attacks

Document ID: 70502

<http://www.cisco.com/warp/public/707/cisco-sr-20060619-ccmxss.shtml>

Revision 1.2

Last Updated 2007 January 23 0000 UTC (GMT)

For Public Release 2006 June 19 2100 UTC (GMT)

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

[Cisco Response](#)

[Additional Information](#)

[Revision History](#)

[Cisco Security Procedures](#)

[Related Information](#)

Cisco Response

This is the Cisco PSIRT response to the statements made by Jake Reynolds and FishNet Security in his advisory: Input Validation/Output Encoding Vulnerabilities in Cisco CallManager Allow Script Injection Attacks. The original email/advisory is available at <http://lists.grok.org.uk/pipermail/full-disclosure/2006-June/047015.html>.

This issue is being tracked by Cisco Bug ID CSCsb68657. We would like to thank Jake Reynolds of FishNet Security for reporting this issue to us.

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

Additional Information

The attacks described in the report manipulate a Cross Site Scripting (XSS) weakness in the web interface of the Cisco CallManager. XSS attacks of this nature rely on intervention of a privileged user and typically attempt to manipulate or trick such a user into clicking on an HTTP URL (typically embedded in an email or HTTP web page).

Cisco recommends that users take care when clicking on URLs and validate the URL being accessed is indeed the site you intend to browse. Checking the HTML source of a web page or email will reveal the true destination of a link.

There are no workarounds that will mitigate this vulnerability.

Cisco has released fixed software for the following supported CallManager trains:

- [4.2\(3\)](#)
- [4.1\(3\)SR4d](#)

Cisco is scheduled to release fixed software for the following supported CallManager trains:

- 4.3(1)
- 3.3(5)SR3

Additional Information

Revision History

Revision 1.2	2007–January–22	Added links to fixed software for 4.1(3)SR4 and 4.2(3).
Revision 1.1	2006–June–22	Changed the sentence: "Cisco has fixed this vulnerability and fixes will be forthcoming for all supported CallManager trains in the following versions:" to the following: "Cisco is scheduled to deliver resolution to mitigate this vulnerability and the fixes will be forthcoming for all supported CallManager trains in the following versions:"
Revision 1.0	2006–June–19	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>.

Related Information

[Security Advisories, Responses and Notices](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#) © 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)
