

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

Cisco Security Response: CiscoWorks Server XSS Vulnerability

<http://www.cisco.com/warp/public/707/cisco-sr-20071205-cw.shtml>

Revision 1.0

For Public Release 2007 December 05 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 that was discovered and reported to Cisco by David Lewis of Liquidmatrix.org regarding a cross-site scripting (XSS) vulnerability in CiscoWorks Server login page.

The original report is available at the following link:

<http://www.liquidmatrix.org/blog/2007/12/05/advisory-cross-site-scripting-in-ciscoverks/>.

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 [CSCsk69289](#) ([registered](#) customers only) .

This Cisco Security Response is posted at the following link:

<http://www.cisco.com/warp/public/707/cisco-sr-20071205-cw.shtml>.

This vulnerability has been assigned CVE ID CVE-2007-5582.

Additional Information

CiscoWorks Common Services (CS) provides the foundation of application infrastructure for all existing CiscoWorks network management solutions to share a common model for data storage, user login, user role definitions, user access privileges, and security protocols.

CS is vulnerable to Cross Site Scripting (XSS) attacks from the CiscoWorks Server login page, `http://server-name:portnumber`. In both Windows and Solaris, the port numbers are 1741 for normal access, and the secure port number is 443. Both the Windows and Solaris versions of the Cisco Works Server login page are affected.

When this XSS vulnerability is exploited, malicious code or script is embedded within the URL and associated with an unsuccessful login attempt page refresh.

The malicious code typically takes the form of a script that is embedded within 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 CiscoWorks server that injects (reflects) the malicious code into the user's browser.

The following versions of CiscoWorks Common Services for both Solaris and Windows operating systems are affected by this vulnerability:

- CiscoWorks Common Services 3.0.x
- CiscoWorks Common Services 3.1

Prior to CiscoWorks Common Services 3.0, the product was titled CiscoWorks Common Management Foundation (CMF). CMF is not affected by this vulnerability.

CiscoWorks products that do not use CiscoWorks Common Services are not affected by this vulnerability.

Workarounds

There are no known workarounds for this vulnerability. Cisco recommends applying a point patch to address the vulnerability. The point patch can be downloaded from Cisco.com for both Solaris and Windows Operating Systems at: <http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-cd-one> ([registered](#) customers only) .

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

<http://www.cisco.com/warp/public/707/cisco-amb-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 1.0	2007-December-05	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](#)

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