

Cisco Security Advisory: XSS and SQL Injection in Cisco CallManager/Unified Communications Manager Logon Page

Advisory ID: cisco-sa-20070829-ccm

<http://www.cisco.com/warp/public/707/cisco-sa-20070829-ccm.shtml>

Revision 1.2

Last Updated 2008 April 25 1400 UTC (GMT)

For Public Release 2007 August 29 1600 UTC (GMT)

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

Contents

- [Summary](#)
- [Affected Products](#)
- [Details](#)
- [Vulnerability Scoring Details](#)
- [Impact](#)
- [Software Versions and Fixes](#)
- [Workarounds](#)
- [Obtaining Fixed Software](#)
- [Exploitation and Public Announcements](#)
- [Status of this Notice: FINAL](#)
- [Distribution](#)
- [Revision History](#)
- [Cisco Security Procedures](#)

Summary

Cisco CallManager and Unified Communications Manager are vulnerable to cross-site Scripting (XSS) and SQL Injection attacks in the lang variable of the admin and user logon pages. A successful attack

may allow an attacker to run JavaScript on computer systems connecting to CallManager or Unified Communications Manager servers, and has the potential to disclose information within the database.

Cisco has made free software available to address these vulnerabilities for affected customers.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20070829-ccm.shtml>.

[\[Expand all sections\]](#) [\[Collapse all sections\]](#)

☐ **Affected Products**

☐ **Vulnerable Products**

Cisco CallManager and Unified Communications Manager versions prior to the following are affected by these vulnerabilities:

- 3.3(5)sr2b
- 4.1(3)sr5
- 4.2(3)sr2
- 4.3(1)sr1

The software version of a CallManager or Unified Communications Manager system can be determined by navigating to **Show > Software** via the administration interface.

For Unified Communications Manager version 5.0, the software version can also be determined by running the command **show version active** in the Command Line Interface (CLI).

For CallManager and Unified Communications Manager version 3.x and 4.x systems, the software version can be determined by navigating to **Help > About Cisco Unified CallManager** and selecting the **Details** button via the administration interface.

Note: Cisco Unified CallManager versions 4.3, 5.1 and 6.0 have been renamed to Cisco Unified Communications Manager. Software versions 3.3, 4.0, 4.1, 4.2 and 5.0 retain the Cisco Unified CallManager name.

☐ **Products Confirmed Not Vulnerable**

No other Cisco products are known to be affected by this vulnerability.

No other versions of CallManager or Unified Communications Manager are vulnerable.

[Top of the section](#) [Close Section](#)

☐ **Details**

Cisco Unified CallManager/Communications Manager (CUCM) is the call processing component of the Cisco IP telephony solution which 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 cross-site scripting vulnerability and the SQL injection vulnerability are triggered when a specially crafted value is entered in the lang variable of either the admin or user logon pages. Attacks against these vulnerabilities are conducted through the web interface and use the http or https protocol. In the case of the cross-site scripting vulnerability, the malicious value includes scripting code enclosed by the <script> and </script> tags. In the case of the SQL injection vulnerability, the value terminates the SQL call and completes a call to the back-end database.

An attacker must be able to convince a user into following a specially crafted URL in order to successfully exploit the cross-site scripting vulnerability.

The cross-site scripting vulnerability is documented as bug ID [CSCsi10728](#) ([registered](#) customers only) .

The SQL injection vulnerability is documented as bug ID [CSCsi64265](#) ([registered](#) customers only) .

[Top of the section](#) [Close Section](#)

▣ Vulnerability Scoring Details

Cisco is providing scores for the vulnerabilities in this advisory based on the Common Vulnerability Scoring System (CVSS). The CVSS scoring in this Security Advisory is done in accordance with CVSS version 2.0.

Cisco will provide a base and temporal score. Customers can then compute environmental scores to assist in determining the impact of the vulnerability in individual networks.

Cisco PSIRT will set the bias in all cases to normal. Customers are encouraged to apply the bias parameter when determining the environmental impact of a particular vulnerability.

CVSS is a standards based scoring method that conveys vulnerability severity and helps determine urgency and priority of response.

Cisco has provided an FAQ to answer additional questions regarding CVSS at:

<http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html>

Cisco has also provided a CVSS calculator to help compute the environmental impact for individual networks at:

<http://intellishield.cisco.com/security/alertmanager/cvss>

XSS in Cisco CallManager User Logon and Admin Page					
Calculate the environmental score of CSCsi10728					
CVSS Base Score - 4.3					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact

Network	Medium	None	Partial	None	None
CVSS Temporal Score - 3.6					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

SQL Injection in Cisco CallManager User Logon and Admin Page					
Calculate the environmental score of CSCsi64265					
CVSS Base Score - 5					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Partial	None	None
CVSS Temporal Score - 4.1					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

[Top of the section](#) [Close Section](#)

☐ Impact

An attacker could exploit the cross-site scripting vulnerability to steal account credentials or run unauthorized JavaScript on the client system.

An attacker could exploit the SQL injection vulnerability to read a single value from the database. Several successful attacks could disclose information about the database, information such as user names and passwords, and information from call records such as the time calls are placed and the numbers dialed. This vulnerability cannot be used to alter or delete call record information from the database.

[Top of the section](#) [Close Section](#)

☐ Software Versions and Fixes

When considering software upgrades, also consult <http://www.cisco.com/go/psirt> and any subsequent advisories to determine exposure and a complete upgrade solution.

In all cases, customers should be certain that the devices scheduled for upgrade contain sufficient memory and that current hardware and software configurations will continue to be properly supported by the new release. If the information is not clear, contact the Cisco Technical Assistance Center ("TAC") or your contracted maintenance provider for assistance.

Version	Fixed Release	Download Location
---------	---------------	-------------------

3.3	3.3(5) sr2b	http://www.cisco.com/cgi-bin/tablebuild.pl/callmgr-33?psrtdcat20e2 (registered customers only)
4.1	4.1(3)sr5	http://www.cisco.com/cgi-bin/tablebuild.pl/callmgr-41?psrtdcat20e2 (registered customers only)
4.2	4.2(3)sr2	http://www.cisco.com/cgi-bin/tablebuild.pl/callmgr-42?psrtdcat20e2 (registered customers only)
4.3	4.3(1)sr1	http://www.cisco.com/cgi-bin/tablebuild.pl/callmgr-43?psrtdcat20e2 (registered customers only)

[Top of the section](#) [Close Section](#)

☐ Workarounds

There are no workarounds for these vulnerabilities.

Cross-site scripting, also known as XSS, is a flaw within web applications that enables malicious users, vulnerable websites, or owners of malicious websites to send malicious code to the browsers of unsuspecting users. 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. The browser will execute the malicious script because the web content is assumed to be from a trusted site and the browser does not have a way to validate the URL or HTML content. A main source of XSS attacks is websites that do not properly validate user-submitted content for dynamically generated web pages.

Because of the nature of XSS vulnerabilities, network mitigation techniques are generally ineffective. To reduce the risk of users becoming victims of XSS attacks, users should be educated about the URL verification limitations of browsers. Countermeasures should also be implemented in the browser through scripting controls. Scripting controls do allow the ability to define policies to restrict code execution.

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

[Top of the section](#) [Close Section](#)

☐ Obtaining Fixed Software

Cisco will make free software available to address this vulnerability for affected customers. This advisory will be updated as fixed software becomes available. Prior to deploying software, customers should consult their maintenance provider or check the software for feature set compatibility and known issues specific to their environment.

Customers may only install and expect support for the feature sets they have purchased. By installing, downloading, accessing or otherwise using such software upgrades, customers agree to be bound by the terms of Cisco's software license terms found at <http://www.cisco.com/public/sw-license-agreement.html>, or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact either "psirt@cisco.com" or "security-alert@cisco.com" for software upgrades.

[Top of the section](#) [Close Section](#)

☐ Customers with Service Contracts

Customers with contracts should obtain upgraded software through their regular update channels. For most customers, this means that upgrades should be obtained through the Software Center on Cisco's worldwide website at <http://www.cisco.com>.

[Top of the section](#) [Close Section](#)

☐ Customers using Third Party Support Organizations

Customers whose Cisco products are provided or maintained through prior or existing agreement with third-party support organizations such as Cisco Partners, authorized resellers, or service providers should contact that support organization for guidance and assistance with the appropriate course of action in regards to this advisory.

The effectiveness of any workaround or fix is dependent on specific customer situations such as product mix, network topology, traffic behavior, and organizational mission. Due to the variety of affected products and releases, customers should consult with their service provider or support organization to ensure any applied workaround or fix is the most appropriate for use in the intended network before it is deployed.

[Top of the section](#) [Close Section](#)

☐ Customers without Service Contracts

Customers who purchase direct from Cisco but who do not hold a Cisco service contract and customers who purchase through third-party vendors but are unsuccessful at obtaining fixed software through their point of sale should get their upgrades by contacting the Cisco Technical Assistance Center (TAC). TAC contacts are as follows.

- +1 800 553 2447 (toll free from within North America)
- +1 408 526 7209 (toll call from anywhere in the world)
- e-mail: tac@cisco.com

Have your product serial number available and give the URL of this notice as evidence of your entitlement to a free upgrade. Free upgrades for non-contract customers must be requested through the TAC.

Refer to <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml> for additional TAC contact information, including special localized telephone numbers and instructions and e-mail addresses for use in various languages.

[Top of the section](#) [Close Section](#)

☐ **Exploitation and Public Announcements**

The Cisco PSIRT is not aware of any malicious use of the vulnerability described in this advisory; however, it has been discussed in public announcements. References include:

<http://packetstormsecurity.org/0708-exploits/cisco-sql.txt> 

This vulnerability was reported to Cisco independently by Gama SEC and Elliot Kendall from Brandeis University. We would like to thank Gama SEC and Elliot Kendall 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.

[Top of the section](#) [Close Section](#)

☐ **Status of this Notice: FINAL**

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.

A stand-alone copy or Paraphrase of the text of this document that omits the distribution URL in the following section is an uncontrolled copy, and may lack important information or contain factual errors.

[Top of the section](#) [Close Section](#)

☐ **Distribution**

This advisory is posted on Cisco's worldwide website at:

<http://www.cisco.com/warp/public/707/cisco-sa-20070829-ccm.shtml>

In addition to worldwide web posting, a text version of this notice is clear-signed with the Cisco PSIRT PGP key and is posted to the following e-mail and Usenet news recipients.

- cust-security-announce@cisco.com
- first-teams@first.org
- bugtraq@securityfocus.com

- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk
- comp.dcom.sys.cisco@newsgate.cisco.com

Future updates of this advisory, if any, will be placed on Cisco's worldwide website, but may or may not be actively announced on mailing lists or newsgroups. Users concerned about this problem are encouraged to check the above URL for any updates.

[Top of the section](#) [Close Section](#)

☐ Revision History

Revision 1.2	2008- April-25	Updated links to the CVSS scores for CSCsi10728 and CSCsi64265 .
Revision 1.1	2007- August-31	Under Exploitation and Public Announcements, changed verbiage and added a link.
Revision 1.0	2007- August-29	Initial public release

[Top of the section](#) [Close Section](#)

☐ 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>.

[Top of the section](#) [Close Section](#)

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)



Send

[Home](#)

[How to Buy](#)

[Login](#)

[Profile](#)

[Feedback](#)

[Site Map](#)

[Help](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2007 - 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)