Cisco Security Advisory

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

Advisory ID: cisco-sa-20070829-ccm
Published: 2007 August 29 16:00 GMT
Version1.2: Final
CVSS Score: Base - 5.0
Workarounds: See below

CVE-2007-4633
CWE-200
CWE-79

Download CVRF
Download PDF
Email

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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070829-ccm.

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.

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) .

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.

Fixed Software

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

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.

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070829-ccm

---

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
