

Cisco Security Advisory: SQL injection in Cisco Unified Communications Manager

Advisory ID: cisco-sa-20080213-cucmsql

<http://www.cisco.com/warp/public/707/cisco-sa-20080213-cucmsql.shtml>

Revision 1.2

Last Updated 2008 April 22 2000 UTC (GMT)

For Public Release 2008 February 13 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 Unified Communications Manager is vulnerable to a SQL Injection attack in the parameter *key* of the admin and user interface pages. A successful attack could allow an authenticated attacker to access information such as usernames and password hashes that are stored in the database.

Cisco has released free software updates that address this vulnerability.

Common Vulnerabilities and Exposures (CVE) identifier [CVE-2008-0026](#)  has been assigned to this vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080213-cucmsql.shtml>.

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

☐ Affected Products

☐ Vulnerable Products

Cisco Unified Communication Manager 5.0/5.1 versions prior to 5.1(3a) and 6.0/6.1 versions prior to 6.1(1a) are affected by this vulnerability.

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

☐ Products Confirmed Not Vulnerable

Cisco CallManager or Unified Communication Manager systems prior to 5.0 are not affected by this vulnerability. No 3.x and 4.x releases are vulnerable.

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

Details

Cisco Unified CallManager/Communications Manager (CUCM) is the call processing component of the Cisco IP telephony solution. This solution 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.

An attacker can trigger this SQL injection vulnerability by entering a specially crafted value is entered in the *key* parameter of either the admin or user interface page. Attacks against this vulnerability are conducted through the web interface and use the http or https protocol. A successful attack could terminate a SQL call and force a connection to the back-end database resulting in the disclosure of potentially sensitive information such as usernames and password hashes.

This vulnerability is documented as bug ID [CSCsk64286](#) ([registered](#) customers only) .

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

Vulnerability Scoring Details

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

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

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

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> .

SQL Injection Vulnerability in User And Admin Interface Pages

Calculate the environmental score of [CSCsk64286](#)

CVSS Base Score - 4

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	Single	Partial	None	None

CVSS Temporal Score - 3.3

Exploitability	Remediation Level	Report Confidence
Functional	Official-Fix	Confirmed

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

Impact

An authenticated attacker may be able to exploit this vulnerability to extract records from the Cisco Unified Communications Manager database. A successful attack might retrieve sensitive data such as user names, passwords hashes, and information from call records. An attacker cannot use this vulnerability 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 exercise caution to be certain the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly 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
---------	---------------	-------------------

5.1	5.1(3a)	http://www.cisco.com/cgi-bin/tablebuild.pl/callmgr-51?psrtdcat20e2 (registered customers only)
6.1	6.1(1a)	http://www.cisco.com/cgi-bin/tablebuild.pl/callmgr-61?psrtdcat20e2 (registered customers only)

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

☐ Workarounds

There are no workarounds for this vulnerability.

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

☐ Obtaining Fixed Software

Cisco has released free software updates that address these vulnerabilities. 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/en/US/docs/general/warranty/English/EU1KEN_.html , or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml> .

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

☐ 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>.

☐ Customers using Third Party Support Organizations

Customers whose Cisco products are provided or maintained through prior or existing agreements 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.

☐ Customers without Service Contracts

Customers who purchase direct from Cisco but do not hold a Cisco service contract, and customers who purchase through third-party vendors but are unsuccessful in obtaining fixed software through their point of sale should acquire 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

Customers should have their product serial number available and be prepared to give the URL of this notice as evidence of 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 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, the vulnerability has been discussed in public announcements. References include Secunia's original advisory available at <http://secunia.com/advisories/28932>  and Security Focus

posting available at <http://www.securityfocus.com/bid/27775> .

This vulnerability was reported to Cisco by Nico Leidecker and Tracey Parry at Portcullis Computer Security Limited. Cisco PSIRT would like to thank these two individuals for bringing this issue to our attention and for working with PSIRT toward coordinated disclosure of the issue. Cisco PSIRT greatly appreciates the opportunity to work with researchers on security vulnerabilities and welcomes 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-20080213-cucmsql.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-22	Updated URL of CVSS CSCsk64286 .
Revision 1.1	2008-April-03	Added links to Secunia and Security Focus references under Exploitation and Public Announcements
Revision 1.0	2008-February-13	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)

[Home](#)[How to Buy](#)[Login](#)[Profile](#)[Feedback](#)[Site Map](#)[Help](#)

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

© 2008 - 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) |

[Trademarks of Cisco Systems, Inc.](#)