Cisco Security Advisory

Cisco Unified Communications Manager SQL Injection Vulnerability

Advisory ID: Cisco-SA-20150505-CVE-2015-0715
Published: 2015 May 5 18:58 GMT
Version1.0: Final
CVSS Score: Base - 4.0
Workarounds: See below
Cisco Bug IDs: CSCut33447 CSCut33608

CVE-2015-0715
CWE-89

Download CVRF
Download PDF
Email

Cisco Security Vulnerability Policy

To learn about Cisco security vulnerability disclosure policies and publications, see the Security Vulnerability Policy. This document also contains instructions for obtaining fixed software and receiving security vulnerability information from Cisco.

Subscribe to Cisco Security Notifications

Subscribe

Summary

A vulnerability in Cisco Unified Communications Manager could allow an authenticated, remote attacker to perform SQL injection attacks.

The vulnerability is due to a failure to properly sanitize user-supplied input passed to the affected application. An attacker could exploit this vulnerability by logging in to the administrative web interface and submitting a crafted response to the affected pages. If successful, the attacker could access sensitive information stored in the database of the targeted device.

Cisco has confirmed the vulnerability and released software updates.

To exploit this vulnerability, an attacker must authenticate to the affected application on a targeted device. This access requirement decreases the likelihood of a successful exploit.

Cisco indicates through the CVSS score that functional exploit code exists; however, the code is not known to be publicly available.

Affected Products

Cisco has released bug IDs CSCut33447 and CSCut33608 for registered users, which contain additional details and up-to-date lists of affected product versions.

Vulnerable Products

At the time this alert was first published, Cisco Unified Communications Manager 11.0(0.98000.225) was vulnerable. Other releases of Cisco Unified Communications Manager may also be affected.

Products Confirmed Not Vulnerable

No other Cisco products are currently known to be affected by these vulnerabilities.

Workarounds

Administrators are advised to apply the appropriate updates.

Administrators are advised to allow only trusted users to have network access.

Administrators are advised to allow only privileged users to access administration or management systems.

For additional information about SQL injection attacks and defenses, see Understanding SQL Injection.

Administrators are advised to monitor affected systems.

Fixed Software

Cisco customers with active contracts can obtain updates through the Software Center at the following link: Cisco. Cisco customers without contracts can obtain upgrades by contacting the Cisco Technical Assistance Center at 1-800-553-2447 or 1-408-526-7209 or via email at *tac@cisco.com*.

Exploitation and Public Announcements

The Cisco Product Security Incident Response Team (PSIRT) is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SA-20150505-CVE-2015-0715

Revision History

Version	Description	Section	Status	Date
1.0	Initial Release	NA	Final	2015-May-05

Legal Disclaimer