Cisco Security Advisory

Cisco Unified Communications Manager Interactive Voice Response Interface SQL Injection Vulnerability

Advisory ID:	Cisco-SA-20150414-CVE-2015-0699
Last Updated:	2015 April 17 21:17 GMT
Published:	2015 April 14 21:23 GMT
Version2.0:	Final
CVSS Score:	Base - 5.0
Workarounds:	See below
Cisco Bug IDs:	CSCut21563

CVE-2015-0699
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 the Interactive Voice Response (IVR) interface of Cisco Unified Communications Manager (UCM) could allow an unauthenticated, remote attacker to conduct SQL injection attacks.

The vulnerability is due to a lack of input validation on user-supplied input within SQL queries. An attacker could exploit this vulnerability by sending crafted URLs that contain malicious SQL statements to the affected system. A successful exploit could allow the attacker to determine the presence of certain values in the database, which could be leveraged to conduct further attacks.

Cisco has confirmed the vulnerability; however, software updates are not available.

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 ID CSCut21563 for registered users that contains additional details and an up-to-date list of affected product versions.

Vulnerable Products

Cisco UCM version 10.5(1.98991.13) is affected. Other versions of Cisco UCM 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 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

Software updates are not available.

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-20150414-CVE-2015-0699

Revision History

Version	Description	Section	Status	Date
1.0	Cisco Unified Communications Manager contains a vulnerability that could allow an unauthenticated, remote attacker to conduct SQL injection attacks. Updates are not available.	NA	Final	2015-Apr-14

Legal Disclaimer