Cisco Security Advisory

Cisco Unified Communications Manager Blind SQL Injection Vulnerability

Medium

Advisory ID:	Cisco-SA-20130717-CVE-2013-3412
Published:	2013 July 17 16:20 GMT
Version1.0:	Final
CVSS Score:	Base - 5.5
Workarounds:	See below
Cisco Bug IDs:	CSCuh81766

CVE-2013-3412
CWE-89

Download CVRF

Download PDF

Email

Related Resources

SA Multiple Vulnerabilities in Cisco Unified Communications Manager

Subscribe to Cisco Security Notifications

Subscribe

Summary

A vulnerability in Cisco Unified Communication Manager (Unified CM) could allow an authenticated, remote attacker to execute a blind Structured Query Language (SQL) injection.

The vulnerability is due to improper validation of user-supplied requests by the Cisco Unified CM. An attacker could exploit this vulnerability by injecting SQL commands, which could allow the attacker to insert rows within the database.

Proof-of-concept code that demonstrates an exploit of this vulnerability is publicly available.

Cisco has confirmed the vulnerability in a security advisory; however, software updates are not yet available.

To exploit this vulnerability, an attacker requires authenticated access to the targeted system. Authenticated access may require the attacker to access trusted, internal networks. These access requirements could limit the likelihood of a successful exploit.

Cisco Unified CM version 8.0 reached the End of Software Maintenance on October 23, 2012. Customers using Cisco Unified CM 8.0(x) versions should contact their Cisco support team for assistance in upgrading to a supported version of Cisco Unified CM.

Cisco Unified CM is the only product confirmed to be vulnerable. Additional voice products may be affected by one or more of the individual vulnerabilities that are described in the advisory. The following products are being investigated but have not yet been confirmed as vulnerable:

- Cisco Emergency Responder
- Cisco Unified Contact Center Express
- Cisco Unified Customer Voice Portal
- Cisco Unified Presence Server/Cisco IM and Presence Service
- Cisco Unity Connection

This vulnerability can be exploited over the default management ports, TCP port 8080 or 8443.

Affected Products

Cisco has released a security advisory for bug ID CSCuh81766 at the following link: cisco-sa-20130717-cucm

Vulnerable Products

Cisco Unified CM versions 9.1(2) and prior are affected.

Products Confirmed Not Vulnerable

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

Workarounds

Administrators are advised to contact the vendor regarding future updates and releases.

The Cisco Applied Intelligence team has created the following companion document to guide administrators in identifying and mitigating attempts to exploit this vulnerability prior to applying updated software: Identifying and Mitigating Exploitation of the Multiple Vulnerabilities in Cisco Unified Communications Manager

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

Administrators are advised to allow only trusted users to access local systems.

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.

Administrators may consider using IP-based access control lists (ACLs) to allow only trusted systems to access the affected systems.

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-20130717-CVE-2013-3412

Revision History

Version	Description	Section	Status	Date
1.0	Initial Release	NA	Final	2013-Jul-17

Legal Disclaimer

Information For
Small Business
Midsize Business
Service Provider
Executives
Industries >
Marketplace
Contacts
Contact Cisco
Find a Reseller

News & Alerts
Newsroom
Blogs
Field Notices
Security Advisories
Technology Trends
Cloud
Internet of Things (IoT)
Mobility
Software Defined Networking (SDN)

Support
Downloads
Documentation
Communities
DevNet
Learning Network
Support Community
Video Portal >

About Cisco
Investor Relations
Corporate Social Responsibility
Environmental Sustainability
Tomorrow Starts Here
Our People
Careers
Search Jobs
Life at Cisco
Programs
Cisco Designated VIP Program
Cisco Powered
Financing Options

Contacts | Feedback | Help | Site Map | Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks