

Cisco Security Advisory

Cisco Unified Communications Manager CAPF Unauthenticated Blind SQL Injection Vulnerability



Advisory ID: Cisco-SA-20140219-CVE-2014-0734 CVE-2014-0734 [Download CVRF](#)
Published: 2014 February 19 20:20 GMT CWE-89 [Download PDF](#)
Version 1.0: Final [Email](#)
CVSS Score: [Base - 4.3](#)
Workarounds: [See below](#)
Cisco Bug IDs: [CSCum46483](#)

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 Certificate Authority Proxy Function (CAPF) of Cisco Unified Communications Manager (Cisco Unified CM) could allow an unauthenticated, remote attacker to impact the integrity of the system by executing arbitrary SQL queries.

The vulnerability is due to a failure to validate user-supplied input used in SQL queries. An attacker could exploit this vulnerability by sending crafted URLs that include SQL statements. An exploit could allow the attacker to determine the presence of certain values in the database.

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

To exploit the vulnerability, the attacker may provide a link that directs a user to a malicious site and use misleading language or instructions to persuade the user to follow the provided link.

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

Affected Products

Customers are advised to consult Cisco bug ID [CSCum46483](#) for a complete list of affected product versions.

Vulnerable Products

At the time this alert was first published, Cisco Unified CM versions 10.0(1) and prior were vulnerable. Later releases of Cisco Unified CM may also be vulnerable.

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.

Administrators may consider using IP-based access control lists (ACLs) to allow only trusted systems to access the affected 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-20140219-CVE-2014-0734>

Revision History

Version	Description	Section	Status	Date
1.0	Initial Release	NA	Final	2014-Feb-19

Legal Disclaimer

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 is an uncontrolled copy, and may lack important information or contain factual errors. The information in this document is intended for end-users of Cisco products.

<p>Information For</p> <ul style="list-style-type: none"> Small Business Midsize Business Service Provider Executives <p>Industries ></p> <p>Marketplace</p> <p>Contacts</p> <ul style="list-style-type: none"> Contact Cisco Find a Reseller 	<p>News & Alerts</p> <ul style="list-style-type: none"> Newsroom Blogs Field Notices Security Advisories <p>Technology Trends</p> <ul style="list-style-type: none"> Cloud Internet of Things (IoT) Mobility Software Defined Networking (SDN) 	<p>Support</p> <ul style="list-style-type: none"> Downloads Documentation <p>Communities</p> <ul style="list-style-type: none"> DevNet Learning Network Support Community <p>Video Portal ></p>	<p>About Cisco</p> <ul style="list-style-type: none"> Investor Relations Corporate Social Responsibility Environmental Sustainability Tomorrow Starts Here Our People <p>Careers</p> <ul style="list-style-type: none"> Search Jobs Life at Cisco <p>Programs</p> <ul style="list-style-type: none"> Cisco Designated VIP Program Cisco Powered Financing Options
--	--	--	--