

Cisco Security Advisory

Cisco Unified Call Manager Arbitrary File Retrieval Vulnerability



Advisory ID: Cisco-SA-20150327-CVE-2015-0680 CVE-2015-0680 [Download CVE](#)
Published: 2015 March 27 19:44 GMT CWE-264 [Download PDF](#)
Version 1.0: Final [Email](#)
CVSS Score: [Base - 4.0](#)
Workarounds: [See below](#)
Cisco Bug IDs: [CSCuq44439](#)

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 Call Manager (Cisco Unified CM) could allow an authenticated, remote attacker to retrieve arbitrary files.

The vulnerability is due to improper security restrictions by the affected application while handling requests for resources. An authenticated, remote attacker could exploit this vulnerability to retrieve arbitrary files from a targeted device. A successful exploit could be used to conduct further attacks.

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

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

There are known fixed releases that mitigate this vulnerability; however, at the time this alert was first published, the known fixed releases were not available for download on the Cisco software download page.

Affected Products

Cisco has released bug ID [CSCuq44439](#) for registered users that contains additional details and an up-to-date list of affected product versions.

Vulnerable Products

At the time this alert was first published, Cisco Unified CM 9.1(2.1000.28) was vulnerable. Later versions 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 are advised to allow only trusted users to have network access.

Administrators are advised to monitor affected systems.

Fixed Software

Software updates are currently 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-20150327-CVE-2015-0680>

Revision History

Version	Description	Section	Status	Date
1.0	Initial Release	NA	Final	2015-Mar-27

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
--	--	--	--