

Cisco Security Advisory

Cisco Unified Communications Manager Command Injection Vulnerability



Advisory ID: Cisco-SA-20130717-CVE-2013-3402 CVE-2013-3402 [Download CVRF](#)
Published: 2013 July 17 16:20 GMT CWE-20 [Download PDF](#)
Version 1.0: Final [Email](#)
CVSS Score: [Base - 6.5](#)
Workarounds: [See below](#)
Cisco Bug IDs: [CSCuh73440](#)

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.

Related Resources

SA [Multiple Vulnerabilities in Cisco Unified Communications Manager](#)

Subscribe to Cisco Security Notifications

[Subscribe](#)

Summary

A vulnerability in Cisco Unified Communications Manager (Unified CM) could allow an authenticated, remote attacker to execute commands on the underlying operating system with the privileges of the database user.

The vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by submitting malicious input to the affected function.

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 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

Affected Products

Cisco has released a security advisory for bug ID [CSCuh73440](#) 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](#)

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-2013-3402>

Revision History

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

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 Midsized 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
---	--	--	--