

Cisco Security Advisory

# Cisco Unified Communications Manager Privilege Escalation Vulnerability



**Advisory ID:** Cisco-SA-20130717-CVE-2013-3433 CVE-2013-3433 [Download CVRF](#)  
**Published:** 2013 July 17 16:11 GMT CWE-264 [Download PDF](#)  
**Version 1.0:** Final [Email](#)  
**CVSS Score:** [Base - 6.8](#)  
**Workarounds:** [See below](#)  
**Cisco Bug IDs:** [CSCui02276](#)

## 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, local attacker to escalate privileges on the system.

The vulnerability is due to improper file permissions on a privileged system binary. An attacker could exploit this vulnerability by modifying a system script, which could allow the attacker to gain complete control of the affected system.

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 must authenticate to a targeted device. Authenticated access may require the attacker to access trusted, internal networks. These access requirements could limit the likelihood of a successful exploit.

## Affected Products

Cisco has released a security advisory for bug ID [CSCui02276](#) at the following link: [cisco-sa-20130717-cucm](#)

### Vulnerable Products

Cisco Unified CM versions 9.1(1a) 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.

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.

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 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-2013-3433>

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