Cisco Security Advisory

Cisco Unified Communications Manager Privilege Escalation Vulnerability

Advisory ID: Cisco-SA-20130717-CVE-2013-3433
Published: 2013 July 17 16:11 GMT
Version1.0: Final
CVSS Score: Base - 6.8
Workarounds: See below
Cisco Bug IDs: CSCui02276

CVE-2013-3433
CWE-264

Download CVRF
Download PDF
Email

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

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