Cisco Security Advisory

Cisco Unified Communications Manager root Shell Access Local Privilege Escalation Vulnerability

Advisory ID: Cisco-SA-20150508-CVE-2015-0717
Last Updated: 2015 June 2 13:41 GMT
Published: 2015 May 8 21:01 GMT
Version2.0: Final
CVSS Score: Base - 6.3
Workarounds: See below
Cisco Bug IDs: CSCut19546

CVE-2015-0717
CWE-264

Download CVRF
Download PDF
Email

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 local read file of the Cisco Unified Communications Manager could allow an authenticated, local attacker to execute commands and obtain an interactive Linux shell as the *root* user if the attacker has already obtained sensitive information from the system.

The vulnerability is due to a failure to properly sanitize user input. An attacker could exploit this vulnerability by inserting Linux shell commands into a parameter using common techniques. A successful exploit could allow the attacker to execute any command on the Linux shell as the *root* user, which could result in a complete system compromise.

Cisco has confirmed the vulnerability and released software updates.

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

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

Affected Products

Cisco has released bug ID CSCut19546 for registered users, which 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 Communications Manager 10.0(1.10000.12) was vulnerable. Other releases of Cisco Unified Communications Manager may also be affected.

Products Confirmed Not Vulnerable

No other Cisco products are currently known to be affected by these vulnerabilities.

Workarounds

Administrators are advised to apply the appropriate updates.

Administrators are advised to allow only trusted users to access local systems.

Administrators are advised to allow only privileged users to access administration or management systems.

Administrators are advised to monitor affected systems.

Fixed Software

Cisco customers with active contracts can obtain updates through the Software Center at the following link: Cisco. Cisco customers without contracts can obtain upgrades by contacting the Cisco Technical Assistance Center at 1-800-553-2447 or 1-408-526-7209 or via email at *tac@cisco.com*.

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-20150508-CVE-2015-0717

Revision History

Version	Description	Section	Status	Date
1.0	Cisco Unified Communications Manager contains a vulnerability that could allow an authenticated, local attacker to execute arbitrary commands as the *root* user. Updates are available.	NA	Final	2015-May-08

Legal Disclaimer