Cisco Security Advisory

Cisco Unified IP Phone 8900/9900 Series Insecure File Permissions Vulnerability

Advisory ID: Cisco-SA-20131113-CVE-2013-6685
Published: 2013 November 13 15:20 GMT
Version1.0: Final
CVSS Score: Base - 6.8
Workarounds: See below
Cisco Bug IDs: CSCui04382

CVE-2013-6685
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 Cisco Unified IP Phone 9951, Cisco Unified IP Phone 9971, and Cisco Unified IP Phone 8961 could allow an authenticated, local attacker to fully compromise the affected device.

The vulnerability is due to insecure file permissions on memory block devices. An attacker could exploit this vulnerability by mounting a malicious filesystem that contains an attacker-controlled SUID binary. An exploit could allow the attacker to take complete control of the affected device.

Cisco would like to thank Red Balloon Security for reporting this vulnerability.

Cisco has confirmed the vulnerability in a security notice and released software updates.

To exploit this vulnerability, an attacker must have local access to the targeted device. This 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

Customers are advised to consult Cisco bug ID CSCui04382 for a complete list of affected product versions.

Vulnerable Products

At the time this alert was first published, Cisco Unified IP Phone 9900 Series Firmware versions 9.4.1 and prior were vulnerable. Later releases of Cisco Unified IP Phone 9900 Series Firmware 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 apply the appropriate updates.

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

Administrators are advised to monitor affected systems.

Fixed Software

Cisco customers with active contracts should contact their Cisco support team for assistance in upgrading to a software version that includes fixes for this vulnerability. Cisco customers without contracts may contact the Cisco Technical Assistance Center at 1-800-553-2447 or 1-408-526-7209 or via email at *tac@cisco.com* for assistance.

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-20131113-CVE-2013-6685

Revision History

Version	Description	Section	Status	Date
1.0	Initial Release	NA	Final	2013-Nov-13

Legal Disclaimer