Cisco Security Advisory

Cisco Unified IP Phone 9900 Series Mobility Extension Availability Vulnerability

Advisory ID: Cisco-SA-20150204-CVE-2015-0600
Published: 2015 February 4 16:39 GMT
Version1.0: Final
CVSS Score: Base - 4.3
Workarounds: See below
Cisco Bug IDs: CSCuq12139

CVE-2015-0600
CWE-20

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 mobility extension support of Cisco Unified IP Phone 9900 Series could allow an unauthenticated, remote attacker to log off the mobility extension user.

The vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending crafted packets to an affected device. An exploit could allow the attacker to cause a denial of service (DoS) condition in which the user is no longer associated with the device and must log in again.

Cisco has confirmed the vulnerability in a security notice; however, software updates are not available.

To exploit this vulnerability, the attacker may need access to trusted, internal networks behind a firewall to send crafted packets to the targeted device. This access requirement may reduce 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 CSCuq12139 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 versions 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 contact the vendor regarding future updates and releases.

Administrators are advised to allow only trusted users to have network access.

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-20150204-CVE-2015-0600

Revision History

Version	Description	Section	Status	Date
1.0	Initial Release	NA	Final	2015-Feb-04

Legal Disclaimer