Cisco Security Advisory

Cisco 9900 Series Phone Arbitrary File Download Vulnerability

Advisory ID: Cisco-SA-20130717-CVE-2013-3426
Published: 2013 July 17 14:39 GMT
Version1.0: Final
CVSS Score: Base - 5.0
Workarounds: See below
Cisco Bug IDs: CSCuh52810

CVE-2013-3426
CWE-200

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 Serviceability servlet of fourth-generation Cisco IP phones could allow an unauthenticated, remote attacker to download arbitrary files from the phone's file system.

The vulnerability is due to incomplete filtering of path values. An attacker could exploit this vulnerability by passing a valid path in a file request in the URL passed to the phone. An exploit could allow the attacker to retrieve an arbitrary file from the IP phone.

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

To exploit this vulnerability, an attacker may need access to trusted, internal networks to submit a request to a targeted device. This access requirement decreases the likelihood of a successful exploit.

Affected Products

Customers should refer to Cisco bug ID CSCuh52810 for the most complete list of affected product versions.

Vulnerable Products

At the time this alert was first published, Cisco Unified IP Phones 9900 Series firmware versions 9.3.2 SR1 and prior were vulnerable. Later versions of Cisco Unified IP Phones 9900 Series firmware 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 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

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-20130717-CVE-2013-3426

Revision History

Version	Description	Section	Status	Date
1.0	Initial Release	NA	Final	2013-Jul-17

Legal Disclaimer