Cisco Security Advisory

Cisco Unified IP Phone 9900 Series Arbitrary File Upload Vulnerability

Medium

Advisory ID:	Cisco-SA-20150204-CVE-2015-0604
Published:	2015 February 4 20:36 GMT
Version1.0:	Final
CVSS Score:	Base - 5.0
Workarounds:	See below
Cisco Bug IDs:	CSCup90424

CVE-2015-0604
CWE-20

Download CVRF

Download PDF

Email

Summary

A vulnerability in the web framework of Cisco Unified IP Phone 9900 Series could allow an unauthenticated, remote attacker to upload arbitrary files to the phone.

The vulnerability is due to insufficient validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted request to the server. An exploit could allow the attacker to upload arbitrary files to arbitrary locations on an affected device.

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

To exploit this vulnerability, an attacker may need access to trusted, internal networks behind a firewall to send crafted HTTP requests 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 CSCup90424 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 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 can help protect affected systems from external attacks by using a solid firewall strategy.

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-20150204-CVE-2015-0604

Revision History

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

Legal Disclaimer

Information For
Small Business
Midsize Business
Service Provider
Executives

Industries ›

Marketplace

Contacts
Contact Cisco
Find a Reseller

News & Alerts
Newsroom
Blogs
Field Notices
Security Advisories

Technology Trends
Cloud
Internet of Things (IoT)
Mobility
Software Defined Networking (SDN)

Support
Downloads
Documentation

Communities
DevNet
Learning Network
Support Community

Video Portal ›

About Cisco
Investor Relations
Corporate Social Responsibility
Environmental Sustainability
Tomorrow Starts Here
Our People

Careers
Search Jobs
Life at Cisco

Programs
Cisco Designated VIP Program
Cisco Powered
Financing Options

Contacts | [–] Feedback | Help | Site Map | Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks