Cisco Security Advisory

Multiple Cisco IP Phones Firmware Image Upload Vulnerability

Advisory ID: cisco-sa-20151209-ipp
Published: 2015 December 9 00:00 GMT
Version1.0: Final
CVSS Score: Base - 4.9
Workarounds: No workarounds available
Cisco Bug IDs: CSCut67400

CVE-2015-6403
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 TFTP implementation of the Cisco Small Business SPA30X and SPA50X IP Phones could allow an unauthenticated, local attacker to load arbitrary firmware images onto the affected device.

The vulnerability is due to insufficient file integrity checks of the firmware image. An attacker could exploit this vulnerability by gaining access to the local shell of the device and loading an arbitrary firmware image onto the device.

Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

This advisory is available at the following link:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151209-ipp

Affected Products

Vulnerable Products

Cisco SPA30X Series IP Phones, Cisco SPA50X Series IP Phones, and Cisco SPA51X Series IP Phones are vulnerable.

Products Confirmed Not Vulnerable

No other Cisco products are currently known to be affected by this vulnerability.

Workarounds

There are no workarounds that address this vulnerability.

Fixed Software

When considering software upgrades, customers are advised to consult the Cisco Security Advisories and Responses archive at http://www.cisco.com/go/psirt and review subsequent advisories to determine exposure and a complete upgrade solution.

In all cases, customers should ensure that the devices to be upgraded contain sufficient memory and confirm that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, customers are advised to contact the Cisco Technical Assistance Center (TAC) or their contracted maintenance providers.

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.

Source

Cisco would like to thank security researcher Chris Watts for discovering and reporting this vulnerability.

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151209-ipp

---

Revision History

Version	Description	Section	Status	Date
1.0	Initial public release	-	Final	2015-December-09

Legal Disclaimer