Cisco Security Advisory

Cisco Small Business SPA3x/5x Series Denial of Service Vulnerability

Advisory ID: cisco-sa-20160831-spa
Published: 2016 August 31 16:00 GMT
Version1.0: Final
CVSS Score: Base - 7.8
Workarounds: No workarounds available
Cisco Bug IDs: CSCut67385

CVE-2016-1469
CWE-399

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.

Related Resources

IPS Cisco Small Business SPA3x and 5x Series Denial of Service

Subscribe to Cisco Security Notifications

Subscribe

Summary

A vulnerability in the HTTP framework of Cisco Small Business SPA300 Series IP Phones, Cisco Small Business SPA500 Series IP Phones, and Cisco SPA51x IP Phones could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device.

The vulnerability is due to incorrect handling of malformed HTTP traffic. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. An exploit could allow the attacker to deny service continually by sending crafted HTTP requests to a phone, resulting in a DoS condition.

Cisco has released software updates that address this vulnerability. Workarounds that address this vulnerability are not available.

This advisory is available at the following link:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-spa

Affected Products

Vulnerable Products

This vulnerability affects the following Cisco Small Business IP Phones running software release 7.5.7(6) or earlier:

- SPA300 Series IP Phones
- SPA500 Series IP Phones
- SPA51x IP Phones

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

Cisco has released free software updates that address the vulnerability described in this advisory. Customers may only install and expect support for software versions and feature sets for which they have purchased a license. By installing, downloading, accessing, or otherwise using such software upgrades, customers agree to follow the terms of the Cisco software license:
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html

Additionally, customers may only download software for which they have a valid license, procured from Cisco directly, or through a Cisco authorized reseller or partner. In most cases this will be a maintenance upgrade to software that was previously purchased. Free security software updates do not entitle customers to a new software license, additional software feature sets, or major revision upgrades.

When considering software upgrades, customers are advised to regularly consult the advisories for Cisco products, which are available from the Cisco Security Advisories and Alerts page, 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.

Customers Without Service Contracts

Customers who purchase directly from Cisco but do not hold a Cisco service contract and customers who make purchases through third-party vendors but are unsuccessful in obtaining fixed software through their point of sale should obtain upgrades by contacting the Cisco Technical Assistance Center (TAC):
http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

Customers should have the product serial number available and be prepared to provide the URL of this advisory as evidence of entitlement to a free upgrade.

Fixed Releases

This vulnerability has been fixed in software releases 7.6.2 and later for Cisco Small Business IP Phones.

Customers are advised to download the latest software release from the Software Center on Cisco.com.

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-20160831-spa

---

Revision History

Version	Description	Section	Status	Date
1.0	Initial public release.	-	Final	2016-August-31

Legal Disclaimer