Cisco Security Advisory

Cisco Unified IP Phone 8900/9900 Series Crafted SDP Packet Vulnerability

Advisory ID: Cisco-SA-20131010-CVE-2013-5526
Last Updated: 2013 October 11 16:41 GMT
Published: 2013 October 10 17:32 GMT
Version2.0: Final
CVSS Score: Base - 5.4
Workarounds: See below
Cisco Bug IDs: CSCuf06698

CVE-2013-5526
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 SDP negotiation logic of the Cisco Cisco Unified IP Phone 9951, Cisco Unified IP Phone 9971 and the Cisco Unified IP Phone 8961 could allow an unauthenticated, remote attacker to cause the phone to reboot.

The vulnerability is due to improper processing of crafted SDP packets. An attacker could exploit this vulnerability by sending crafted SDP packets to the phone to cause the phone to reload.

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

To exploit this vulnerability, an attacker must be able to send crafted SDP packets to the targeted device, which may reside on trusted, internal networks that the attacker may need access to. This access requirement decreases 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 CSCuf06698 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 releases of Cisco Unified IP Phones 9900 Series Firmware 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 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-20131010-CVE-2013-5526

Revision History

Version	Description	Section	Status	Date
1.0	Cisco fourth-generation RT style IP phones contain a vulnerability to could allow an unauthenticated, remote attacker to cause a denial of service condition. Updates are not available.	NA	Final	2013-Oct-10

Legal Disclaimer