Cisco Security Advisory

Cisco Unified IP Phones 9900 Series Denial of Service Vulnerability

Medium

Advisory ID: Cisco-SA-20150629-CVE-2015-4226
Published: 2015 June 29 18:05 GMT
Version1.0: Final
CVSS Score: Base - 4.3
Workarounds: See below
Cisco Bug IDs: CSCur39976

CVE-2015-4226
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.

Subscribe to Cisco Security Notifications

Subscribe

Summary

A vulnerability in the packet storing capabilities of Cisco 9900 Series IP Phones could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

The vulnerability is due to how the phone decoder handles certain real-time transport protocol (RTP) packets. An attacker could exploit this vulnerability by calling a registered phone, waiting for a user to answer, then send malformed RTP packets to the user's phone. A successful exploit could cause the phone to become unresponsive, resulting in a DoS condition.

Cisco has confirmed the vulnerability and released software updates.

To exploit this vulnerability, an attacker must first call a targeted phone and then rely on a user to answer the phone prior to sending malformed RTP packets. The attacker can not exploit this vulnerability without this requirement.

Cisco indicates through the CVSS score that functional exploit code exists; however, the code is not known to be publicly available.

Affected Products

Cisco has released bug ID CSCur39976 for registered users, which contains additional details and an up-to-date list of affected product versions.

Vulnerable Products

At the time this alert was first published, Cisco Unified IP Phones 9900 Series release 9.3(2) was vulnerable. Later releases of Cisco Unified IP Phones 9900 Series 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 monitor affected systems.

Fixed Software

Cisco customers with active contracts can obtain updates through the Software Center at the following link: Cisco. Cisco customers without contracts can obtain upgrades by contacting the Cisco Technical Assistance Center at 1-800-553-2447 or 1-408-526-7209 or via email at *tac@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.

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SA-20150629-CVE-2015-4226

Revision History

Version	Description	Section	Status	Date
1.0	Initial Release	NA	Final	2015-Jun-29

Legal Disclaimer

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

A stand-alone copy or paraphrase of the text of this document that omits the distribution URL is an uncontrolled copy, and may lack important information or contain factual errors. The information in this document is intended for end-users of Cisco products.