Cisco Security Advisory

Unauthorized Access Vulnerability in Cisco Unified SIP Phone 3905

Advisory ID: cisco-sa-20140219-phone
Published: 2014 February 19 16:00 GMT
Version1.0: Final
CVSS Score: Base - 10.0
Workarounds: See below
Cisco Bug IDs: CSCuh75574

CVE-2014-0721
CWE-264

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

IS Unauthorized Access Vulnerability in Cisco Unified SIP Phone 3905

AMB Mitigation and Identification of the Unauthorized Access Vulnerability in Cisco Unified SIP Phone 3905

IPS Cisco IP Phone Unauthorized Access

Subscribe to Cisco Security Notifications

Subscribe

Summary

A vulnerability in the Cisco Unified SIP Phone 3905 could allow an unauthenticated, remote attacker to gain *root*-level access to an affected device.

Cisco has released software updates that address this vulnerability. Workarounds that mitigate this vulnerability are not available. This advisory is available at the following link:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140219-phone

Affected Products

Vulnerable Products

Only the Cisco Unified 3905 Phone is affected by this vulnerability.

Products Confirmed Not Vulnerable

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

Details

A vulnerability in the Cisco Unified SIP Phone 3905 could allow an unauthenticated, remote attacker to gain *root*-level access to an affected device.

Note: Only the Cisco Unified 3905 Phone is affected by this vulnerability.

This vulnerability is due to an undocumented test interface in the TCP service listening on port 7870 of the affected device.

This vulnerability is documented in Cisco bug ID CSCuh75574 (registered customers only) and has been assigned Common Vulnerabilities and Exposures (CVE) ID CVE-2014-0721.

Workarounds

Workarounds that mitigate this vulnerability are not available.

Mitigations that can be deployed on Cisco devices within the network are available in the Applied Mitigation Bulletin at the following link: Mitigation and Identification of the Unauthorized Access Vulnerability in Cisco Unified SIP Phone 3905.

Fixed Software

When considering software upgrades, customers are advised to consult the Cisco Security Advisories, Responses, and Notices 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.

This vulnerability has been fixed in Cisco Unified SIP Phone 3905 Firmware Release 9.4(1) or later.

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.

This vulnerability was reported to Cisco by a customer.

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140219-phone

---

Revision History

Revision 1.0	2014-February-19	Initial public release

Legal Disclaimer