Cisco Security Advisory

Cisco Unified Communications Manager Skinny Client Control Protocol Vulnerabilities

High

Advisory ID: cisco-sa-20120229-cucm
Last Updated: 2012 April 2 14:07 GMT
Published: 2012 February 29 16:00 GMT
Version1.1: Final
CVSS Score: Base - 7.8
Workarounds: See below
Cisco Bug IDs: CSCtu73538

CVE-2011-4486
CVE-2011-4487

Download CVRF
Download PDF
Email

Summary

Cisco Unified Communications Manager devices may allow a remote, unauthenticated attacker with the ability to send crafted Skinny Client Control Protocol (SCCP) messages to an affected device to cause a reload or execute attacker-controlled SQL code.

Cisco has released software updates that address these vulnerabilities.

Workarounds that mitigate these vulnerabilities are available.

This advisory is available at the following link:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120229-cucm

Affected Products

Vulnerable Products

The following products are affected by the vulnerabilities that are described in this advisory:

- Cisco Unified Communications Manager Software versions 6.x
- Cisco Unified Communications Manager Software versions 7.x
- Cisco Unified Communications Manager Software versions 8.x
- Cisco Business Edition 3000
- Cisco Business Edition 5000
- Cisco Business Edition 6000

Note: Cisco Unified Communications Manager version 6.1 reached the End of Software Maintenance on September 3, 2011. Customers using Cisco Unified Communications Manager Software versions 6.x, should contact their Cisco support team for assistance in upgrading to a supported version of Cisco Unified Communications Manager.

Products Confirmed Not Vulnerable

No other Cisco products are currently known to be affected by these vulnerabilities.

Details

Cisco Unified Communications Manager is the call processing component of the Cisco IP Telephony solution that extends enterprise telephony features and functions to packet telephony network devices, such as IP phones, media processing devices, VoIP gateways, and multimedia applications.

Cisco Unified Communications Manager contains two vulnerabilities that involve the processing of SCCP packets. These issues may allow a remote, unauthenticated attacker with the ability to send crafted SCCP messages to an affected device to cause a reload or execute attacker-controlled SQL code. Both SCCP ports (TCP ports 2000 and 2443) are affected.

Cisco Unified Communications Manager SCCP Registration may Cause Reload
Cisco Unified Communication Manager may reload when a specially crafted SCCP message is processed. Successful exploitation could cause a loss of all voice services that are being handled by the affected device. After the device restarts, voice services will be restored. This vulnerability is documented in Cisco bug ID CSCtu73538 (registered customers only) and has been assigned Common Vulnerabilities and Exposures (CVE) ID CVE-2011-4486.

Cisco Unified Communications Manager Vulnerable to Blind SQL Injection During Registration
Cisco Unified Communications Manager may allow the blind execution of attacker-controlled SQL code when processing a specially crafted SCCP message. Successful exploitation could allow the attacker to modify certain sections of the SQL database that are utilized by the device. This vulnerability is also documented in Cisco bug ID CSCtu73538 (registered customers only) and has been assigned CVE ID CVE-2011-4487.

Workarounds

Administrators can mitigate these vulnerabilities limiting access to TCP ports 2000 and 2443 to only allow traffic from networks that require SCCP access to Cisco Unified Communications Manager appliances.

Additional mitigation techniques that can be deployed on Cisco devices within the network are available in the Cisco Applied Mitigation Bulletin companion document for this advisory:

http://tools.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20120229-cucm

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.

Cisco Unified Communication Manager Version	First Fixed Release
6.x	Vulnerable; migrate to 7.1(5b)su5 or later
7.x	7.1(5b)su5; available April 6, 2012
8.0	8.0(3a)su3
8.5	Vulnerable; migrate to 8.6(2a)su1
8.6	8.6(2a)su1; available in March 2012
Cisco Business Edition 3000 Software	8.6.3
Cisco Business Edition 5000 Software	8.6(2a)su1; available in March 2012
Cisco Business Edition 6000 Software	8.6(2a)su1; available in March 2012

Cisco Unified Communications Manager Software can be downloaded at the following link:
http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=268439621

Cisco Business Edition Software can be downloaded at the following link:
http://www.cisco.com/cisco/software/navigator.html?mdfid=283661240i=rm

Exploitation and Public Announcements

These vulnerabilities were publicly disclosed on Bugtraq on November 8, 2011. The Cisco Product Security Incident Response Team (PSIRT) is not aware of any malicious use of the vulnerabilities described in this advisory.

These vulnerabilities were reported to Cisco by Felix Lindner of Recurity Labs GmbH and discovered by Sandro Gauci.

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120229-cucm

---

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

SA Cisco Unified Communications Manager Device Registration SQL Injection Vulnerability

IS Cisco Unified Communications Manager SCCP Message Processing Denial of Service Vulnerability

AMB Identifying and Mitigating Exploitation of the Cisco Unified Communications Manager Skinny Client Control Protocol Vulnerabilities

Subscribe to Cisco Security Notifications

Subscribe

Revision History

Revision 1.1	2012-April-02	Updated software release date.
Revision 1.0	2012-February-29	Initial public release.

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.