Cisco Security Advisory

Cisco Unified Communications Manager Denial of Service Vulnerabilities

Advisory ID: cisco-sa-20100303-cucm
Published: 2010 March 3 16:00 GMT
Version1.0: Final
CVSS Score: Base - 8.5
Workarounds: See below

CVE-2010-0573

Download CVRF
Download PDF
Email

Summary

Cisco Unified Communications Manager (formerly Cisco CallManager) contains multiple denial of service (DoS) vulnerabilities that if exploited could cause an interruption of voice services. The Session Initiation Protocol (SIP), Skinny Client Control Protocol (SCCP) and Computer Telephony Integration (CTI) Manager services are affected by these vulnerabilities.

To address these vulnerabilities, Cisco has released free software updates for select Cisco Unified Communications Manager versions. There is a workaround for of one the vulnerabilities.

This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100303-cucm.

Affected Products

Vulnerable Products

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

- Cisco Unified Communications Manager 4.x
- Cisco Unified Communications Manager 5.x
- Cisco Unified Communications Manager 6.x
- Cisco Unified Communications Manager 7.x

Note: Cisco Unified Communications Manager version 5.1 reached the End of Software Maintenance on February 13, 2010. For customers using Cisco Unified Communications Manager 5.x versions, please contact your Cisco support team for assistance in upgrading to a supported version of Cisco Unified Communications Manager.

Products Confirmed Not Vulnerable

Cisco Unified Communications Manager version 8.0(1) and Cisco Unified Communications Manager Express are not affected by these vulnerabilities. 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.

Malformed SCCP Message Vulnerabilities

Cisco Unified Communications Manager contains two DoS vulnerabilities that involve the processing of SCCP packets. Each vulnerability is triggered by a malformed SCCP message that could cause a critical process to fail, which could result in the disruption of voice services. All SCCP ports (TCP ports 2000 and 2443) are affected.

The first SCCP DoS vulnerability is documented in Cisco Bug ID CSCtc38985 (registered customers only) and has been assigned the CVE identifier CVE-2010-0587. This vulnerability is fixed in Cisco Unified Communications Manager versions 4.3(2)SR2, 6.1(5), 7.1(3a)su1 and 8.0(1).

The second SCCP DoS vulnerability is documented in Cisco Bug ID CSCtc47823 (registered customers only) and has been assigned the CVE identifier CVE-2010-0588. This vulnerability is fixed in Cisco Unified Communications Manager versions 6.1(5), 7.1(3a)su1 and 8.0(1). Cisco Unified Communications Manager 4.x versions are not affected.

Malformed SIP Message Vulnerabilities

Cisco Unified Communications Manager contains two DoS vulnerabilities that involve the processing of SIP messages. Each vulnerability is triggered by a malformed SIP message that could cause a critical process to fail, which could result in the disruption of voice services. All SIP ports (TCP ports 5060 and 5061, UDP ports 5060 and 5061) are affected.

The first SIP DoS vulnerability is documented in Cisco Bug ID CSCtc37188 (registered customers only) and has been assigned the CVE identifier CVE-2010-0590. This vulnerability is fixed in Cisco Unified Communications Manager versions 7.1(3a)su1 and 8.0(1) . Cisco Unified Communications Manager 4.x and 6.x versions are not affected.

The second SIP DoS vulnerability is documented in Cisco Bug ID CSCtc62362 (registered customers only) and has been assigned the CVE identifier CVE-2010-0591. The second vulnerability is fixed in Cisco Unified Communications Manager versions 6.1(5), 7.1(3b)SU2 and 8.0(1). Cisco Unified Communications Manager 4.x versions are not affected.

Malformed CTI Manager Message Vulnerability

The CTI Manager service of Cisco Unified Communications Manager contains a DoS vulnerability. A malformed message sent to the CTI Manager service port (TCP 2748) could cause the CTI Manager service to fail, which could result in the interruption of CTI applications. The CTI Manager service is disabled by default.

The CTI Manager vulnerability is documented in Cisco Bug ID CSCsu31800 (registered customers only) and has been assigned the CVE identifier CVE-2010-0592. This vulnerability is fixed in Cisco Unified Communications Manager versions 4.3(2)sr1a, 6.1(3), 7.0(2), 7.1(2) and 8.0(1).

Workarounds

Administrators can mitigate the SCCP- and SIP-related vulnerabilities by implementing filtering on screening devices to permit access to TCP ports 2000 and 2443, and TCP and UDP ports 5060 and 5061 only from networks that require SCCP and SIP access to Cisco Unified Communications Manager appliances.

It is possible to mitigate the CTI Manager vulnerability by disabling the CTI Manager service t is not necessary; however, this workaround will interrupt applications that reply on the CTI Manager service. Administrators can also mitigate the vulnerability by implementing filtering on screening devices to permit access to TCP port 2748 only from networks that require access to the CTI Manager service. Please consult the following documentation for details on disabling Cisco Unified Communications Manager services:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/service/6_0_1/admin/sasrvact.html#wp1048390

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-20100303-cucm

Fixed Software

When considering software upgrades, also consult http://www.cisco.com/go/psirt and any subsequent advisories to determine exposure and a complete upgrade solution.

In all cases, customers should exercise caution to be certain the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, contact the Cisco Technical Assistance Center (TAC) or your contracted maintenance provider for assistance.

Cisco Unified Communications Manager Version	Recommended Release
4.x	4.3(2)SR2
5.x	Cisco Unified Communications Manager version 5.1 reached the End of Software Maintenance on February 13, 2010.
6.x	6.1(5)
7.x	7.1(3b)SU2

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 Cisco Digital Media Player Remote Unauthorized Content Injection Vulnerability

Subscribe to Cisco Security Notifications

Subscribe

8.x	Cisco Unified Communications Manager version 8.0(1) was distributed with software fixes for all the vulnerabilities that are described in this advisory.

Cisco Unified Communications Manager software version 4.3(2)SR2 can be downloaded at the following link:

http://tools.cisco.com/support/downloads/go/PlatformList.x?sftType=Unified+Communications+Manager+Updates&mdfid=280771554&treeName=Voice+and+Unified+Communications&mdfLevel=Software%20Version/Option&url=null&modelName=Cisco+Unified+Communications+Manager+Version+4.3&isPlatform=N&treeMdfId=278875240&modifmdfid=null&imname=&hybrid=&Yimst=N

Cisco Unified Communications Manager software version 6.1(5) can be downloaded at the following link:

http://tools.cisco.com/support/downloads/go/ReleaseType.x?optPlat=&isPlatform=Y&mdfid=281023410&sftType=Unified+Communications+Manager+Updates&treeName=Voice+and+Unified+Communications&modelName=Cisco+Unified+Communications+Manager+Version+6.1&mdfLevel=Software%20Version/Option&treeMdfId=278875240&modifmdfid=null&limname=&hybrid=&Yimst=N

Cisco Unified Communications Manager software version 7.1(3b)SU2 can be downloaded at the following link:

http://tools.cisco.com/support/downloads/go/PlatformList.x?sftType=Unified+Communications+Manager+Updates&mdfid=282421166&treeName=Voice+and+Unified+Communications&mdfLevel=Software%20Version/Option&url=null&modelName=Cisco+Unified+Communications+Manager+Version+7.1&isPlatform=N&treeMdfId=278875240&modifmdfid=null&imname=&hybrid=&Yimst=N

Exploitation and Public Announcements

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerabilities described in this advisory.

The vulnerability documented in Cisco Bug ID CSCtc38985 (registered customers only) was reported to Cisco by the Sipera VIPER Lab. Cisco would like to thank Sipera VIPER Lab team for reporting this vulnerability to us and for working with us on a coordinated disclosure.

All other vulnerabilities described in this advisory were discovered as a result of internal testing conducted by Cisco.

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100303-cucm

---

Revision History

Revision 1.0	2010-March-03	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.