

Table of Contents

<u>Cisco Security Advisory: Cisco Call Manager Denial of Service</u>	1
<u>Document ID: 68791</u>	1
<u>Advisory ID: cisco-sa-20060118-ccmdos</u>	1
<u>http://www.cisco.com/warp/public/707/cisco-sa-20060118-ccmdos.shtml</u>	1
<u>Revision 1.0</u>	1
<u>For Public Release 2006 January 18 1600 UTC (GMT)</u>	1
<u>Please provide your feedback on this document</u>	1
<u>Summary</u>	1
<u>Affected Products</u>	1
<u>Vulnerable Products</u>	1
<u>Details</u>	2
<u>Impact</u>	2
<u>Software Versions and Fixes</u>	2
<u>Workarounds</u>	3
<u>Obtaining Fixed Software</u>	3
<u>Customers with Service Contracts</u>	3
<u>Customers using Third-party Support Organizations</u>	3
<u>Customers without Service Contracts</u>	3
<u>Exploitation and Public Announcements</u>	4
<u>Status of This Notice: FINAL</u>	4
<u>Distribution</u>	4
<u>Revision History</u>	5
<u>Cisco Security Procedures</u>	5

Cisco Security Advisory: Cisco Call Manager Denial of Service

Document ID: 68791

Advisory ID: cisco-sa-20060118-ccmdos

<http://www.cisco.com/warp/public/707/cisco-sa-20060118-ccmdos.shtml>

Revision 1.0

For Public Release 2006 January 18 1600 UTC (GMT)

Please provide your feedback on this document.

Summary
Affected Products
Details
Impact
Software Versions and Fixes
Workarounds
Obtaining Fixed Software
Exploitation and Public Announcements
Status of This Notice: FINAL
Distribution
Revision History
Cisco Security Procedures

Summary

Cisco CallManager (CCM) is the software-based call-processing component of the Cisco IP telephony solution which extends enterprise telephony features and functions to packet telephony network devices such as IP phones, media processing devices, voice-over-IP (VoIP) gateways, and multimedia applications. All Cisco CallManager versions are vulnerable to these Denial of Service (DoS) attacks, which may result in services being interrupted or servers rebooting.

Cisco has made free software available to address this vulnerability for affected customers. There are network-based workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20060118-ccmdos.shtml>.

Affected Products

Vulnerable Products

- Cisco CallManager 3.2 and earlier
- Cisco CallManager 3.3, versions earlier than 3.3(5)SR1a

- Cisco CallManager 4.0, versions earlier than 4.0(2a)SR2c
- Cisco CallManager 4.1, versions earlier than 4.1(3)SR2

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

Details

Vulnerable versions of Cisco Call Manager do not manage TCP connections and Windows messages aggressively, leaving some well-known, published ports vulnerable to Denial of Service attacks.

- **CSCea53907** CallManager does not time out TCP connections to port 2000 aggressively enough, leading to a scenario where memory and CPU resources are consumed with enough open connections. In specific scenarios, CallManager will leave the TCP connection open indefinitely until either the Call Manager service is restarted or the server is rebooted.
- **CSCsa86197, CSCsb16635, CSCsb64161** Multiple connections to ports 2001, 2002, or 7727 can fill up the Windows message queue. This prevents CCM from transacting with the Windows Service Manager, which restarts the CCM after a 30 second timeout.

Impact

Successful exploitation of these vulnerabilities may result in DoS attacks, which may result in high CPU utilization, services being interrupted, or servers rebooting. This may then lead to phones not responding, phones unregistering from the Cisco CallManager, or Cisco CallManager restarting..

Software Versions and Fixes

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.

Each row of the Cisco CallManager software table (below) describes a release train which will address all of the vulnerabilities mentioned in this advisory. If a given release train is vulnerable, then the earliest possible releases that contain the fixes (the "First Fixed Release") and the anticipated date of availability for each are listed in the "Engineering Special," "Service Release," and "Maintenance Release" columns. A device running a Cisco CallManager release in the given train that is earlier than the release in a specific column (less than the First Fixed Release listed in the Engineering Special or Special Release column) is known to be vulnerable to one or more issues. The Cisco CallManager should be upgraded at least to the indicated release or a later version (greater than or equal to the First Fixed Release label).

Version	Engineering Special	Service Release	Maintenance Release
3.2 and earlier			migrate to 3.3 or later
3.3	3.3(5)ES24	3.3(5)SR1a	no release planned

4.0	4.0(2a)ES56	4.0(2a)SR2c	no release planned
4.1	4.1(2)ES50 4.1(3)ES24	4.1(3)SR2	no release planned

Workarounds

While there are no workarounds available on the Cisco CallManager to eliminate DoS attacks, securing the voice network with Cisco CallManager security best practices may lessen the risk or mitigate the effects of these vulnerabilities. By using access lists and rate limiting to control access to the Cisco CallManager, the risk of successful attack is greatly reduced. Cisco provides Solution Reference Network Design (SRND) guides to help design and deploy networking solutions, which can be found at <http://www.cisco.com/warp/public/779/largeent/it/ese/srnd.html>.

Obtaining Fixed Software

Cisco has made free software available to address this vulnerability for affected customers. Prior to deploying software, customers should consult their maintenance provider or check the software for feature set compatibility and known issues specific to their environment.

Customers may only install and expect support for the feature sets they have purchased. By installing, downloading, accessing or otherwise using such software upgrades, customers agree to be bound by the terms of Cisco's software license terms found at <http://www.cisco.com/public/sw-license-agreement.html>, or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact either "psirt@cisco.com" or "security-alert@cisco.com" for software upgrades.

Customers with Service Contracts

Customers with contracts should obtain upgraded software through their regular update channels. For most customers, this means that upgrades should be obtained through the Software Center on Cisco's worldwide website at <http://www.cisco.com>.

Customers using Third-party Support Organizations

Customers whose Cisco products are provided or maintained through prior or existing agreement with third-party support organizations such as Cisco Partners, authorized resellers, or service providers should contact that support organization for guidance and assistance with the appropriate course of action in regards to this advisory.

The effectiveness of any workaround or fix is dependent on specific customer situations such as product mix, network topology, traffic behavior, and organizational mission. Due to the variety of affected products and releases, customers should consult with their service provider or support organization to ensure any applied workaround or fix is the most appropriate for use in the intended network before it is deployed.

Customers without Service Contracts

Customers who purchase direct from Cisco but who do not hold a Cisco service contract and customers who purchase through third-party vendors but are unsuccessful at obtaining fixed software through their point of sale should get their upgrades by contacting the Cisco Technical Assistance Center (TAC). TAC contacts are as follows.

Cisco Security Advisory: Cisco Call Manager Denial of Service

- +1 800 553 2447 (toll free from within North America)
- +1 408 526 7209 (toll call from anywhere in the world)
- e-mail: tac@cisco.com

Have your product serial number available and give the URL of this notice as evidence of your entitlement to a free upgrade. Free upgrades for non-contract customers must be requested through the TAC.

Refer to <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml> for additional TAC contact information, including special localized telephone numbers and instructions and e-mail addresses for use in various languages.

Exploitation and Public Announcements

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

This vulnerability was reported to Cisco by a customer.

Status of This Notice: FINAL

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 in the following section is an uncontrolled copy, and may lack important information or contain factual errors.

Distribution

This advisory is posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20060118-ccmdos.shtml>.

In addition to worldwide web posting, a text version of this notice is clear-signed with the Cisco PSIRT PGP key and is posted to the following e-mail and Usenet news recipients.

- cust-security-announce@cisco.com
- first-teams@first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-voip@puck.nether.net
- full-disclosure@lists.grok.org.uk
- comp.dcom.sys.cisco@newsgate.cisco.com

Future updates of this advisory, if any, will be placed on Cisco's worldwide website, but may or may not be actively announced on mailing lists or newsgroups. Users concerned about this problem are encouraged to check the above URL for any updates.

Revision History

Revision 1.0	2006-January-18	Initial Public Release.
--------------	-----------------	-------------------------

Cisco Security Procedures

Complete information on reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information from Cisco, is available on Cisco's worldwide website at http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html. This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

All contents are Copyright © 1992–2006 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Jan 18, 2006

Document ID: 68791
