

# [NEWS] Cisco Call Manager DoS

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-01/msg00073.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxxx)>
  - *Date:* 19 Jan 2006 16:52:41 +0200
- 

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>  
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.  
<http://www.securiteam.com/maillinglist.html>

-----

Cisco Call Manager DoS

---

## 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".

Cisco CallManager has been found to be vulnerable to denial of service (DoS) attacks, which may result in services being interrupted or servers rebooting.

## DETAILS

### Vulnerable Systems:

- \* 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

Vulnerable versions of Cisco Call Manager do not manage TCP connections and Windows messages aggressively, leaving some well-known, published

[NEWS] Cisco Call Manager DoS

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.

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.

Workaround:

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>> <http://www.cisco.com/warp/public/779/largeent/it/ese/srnd.html>

ADDITIONAL INFORMATION

The original article can be found at: <<http://www.cisco.com/warp/public/707/cisco-sa-20060118-ccmdos.shtml>> <http://www.cisco.com/warp/public/707/cisco-sa-20060118-ccmdos.shtml>

=====

This bulletin is sent to members of the SecuriTeam mailing list.  
To unsubscribe from the list, send mail with an empty subject line and body to:  
list-unsubscribe@xxxxxxxxxxxxxxx  
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxx

=====  
=====

## [NEWS] Cisco Call Manager DoS

### DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

---

- Prev by Date: [\*\[NEWS\] Cisco IOS Stack Group Bidding Protocol Crafted Packet DoS\*](#)
- Next by Date: [\*\[NEWS\] Cisco Call Manager Privilege Escalation\*](#)
- Previous by thread: [\*\[NEWS\] Cisco IOS Stack Group Bidding Protocol Crafted Packet DoS\*](#)
- Next by thread: [\*\[NEWS\] Cisco Call Manager Privilege Escalation\*](#)
- Index(es):
  - ◆ [\*Date\*](#)
  - ◆ [\*Thread\*](#)