

# Cisco Security Advisory: Cisco CallManager Memory Handling Vulnerabilities

Document ID: 65529

Advisory ID: cisco-sa-20050712-ccm

<http://www.cisco.com/warp/public/707/cisco-sa-20050712-ccm.shtml>

## Revision 1.1

**Last Updated** 2005 July 18 2200 UTC (GMT)

For Public Release 2005 July 12 1500 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. Cisco CallManager 3.3 and earlier, 4.0, and 4.1 are vulnerable to Denial of Service (DoS) attacks, memory leaks, and memory corruption which may result in services being interrupted, servers rebooting, or arbitrary code being executed.

Cisco has made free software available to address these vulnerabilities.

This advisory will be posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050712-ccm.shtml>.

## Affected Products

This section provides details on affected products.

## Vulnerable Products

These products are vulnerable:

- Cisco CallManager 3.2 and earlier
- Cisco CallManager 3.3, versions earlier than 3.3(5)
- Cisco CallManager 4.0, versions earlier than 4.0(2a)SR2b
- Cisco CallManager 4.1, versions earlier than 4.1(3)SR1

## Products Confirmed Not Vulnerable

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

## Details

This section provides detailed information about these vulnerabilities.

- [CSCed37403](#) ([registered customers only](#)) — Resource leak with RISDC — CallManager does not time out RISDC (Realtime Information Server Data Collection) sockets aggressively enough, leading to a scenario where TaskManager indicates that RisDC.exe is using large amounts of non-paged pool memory and ports remain in the Close\_Wait state. Non-paged pool memory allocation can be checked by opening Microsoft Windows Task Manager, going to the View menu, choosing Select Columns and selecting Non-paged Pool. Open ports are listed in the output of the netstat -an command.
- [CSCee00116](#) ([registered customers only](#)) — Cisco CallManager CTI Manager may restart with greater than 1GB memory used — Repeated attacks with crafted packets can cause the CTI Manager to allocate greater than 1 gigabyte of virtual memory. Memory allocation of the ctimgr.exe process can be checked by viewing the Microsoft Windows Task Manager.
- [CSCee00118](#) ([registered customers only](#)) — CallManager may restart with repeated attacks — Crafted packets can cause the CallManager to inappropriately allocate 500MB to the ccm.exe process, which will return to the memory pool under normal conditions. Repeated attacks may cause a CallManager under load to exhaust memory resources and restart. Memory allocation of the ccm.exe process can be checked by viewing the Microsoft Windows Task Manager. Under attack, ccm.exe memory will jump repeatedly by 500MB.
- [CSCef47060](#) ([registered customers only](#)) — Failed logins create memory leak when MLA enabled — When MLA (Multi Level Admin) is enabled and there are repeated, failed logons for the AST (Admin Service Tool) a memory leak may occur. While under normal operations inetinfo.exe will use between 20Mb and 30Mb of memory, systems facing this issue showed up to 750Mb of memory used. Memory allocation of the inetinfo.exe process can be checked by viewing the Microsoft Windows Task Manager. MLA is not on by default and the enable status can be checked under CCM/User/Access Rights/MLA Parameters/Enable Multi Level Admin.
- [CSCsa75554](#) ([registered customers only](#)) — Vulnerability to DoS and remote execution in aupair service — Crafted packets directed at Cisco CallManager may cause a memory allocation failure and buffer overflow resulting in potential execution of arbitrary code, abnormal termination of the aupair process, or corruption of memory. The aupair.exe process is a database layer between ccm.exe and SQL which cannot be disabled for normal Cisco CallManager operation. When viewing Microsoft Windows Task Manager, the process is aupair.exe, but under the Service Control Manager it is called Cisco Database Layer Monitor. If the aupair.exe process terminates, a message will be logged to the events monitor and a drwatson report will be generated.

## Impact

Successful exploitation of the vulnerabilities may result in severe issues with Cisco CallManager and related IP telephony services. Triggering a memory allocation and buffer overflow may allow remote code execution and breach of confidentiality. Excess memory allocation can cause resource starvation resulting in high CPU utilization, unresponsive terminal services, the inability to run CCM Admin, or map drives. 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, please also consult [http://www.cisco.com/en/US/products/products\\_security\\_advisories\\_listing.html](http://www.cisco.com/en/US/products/products_security_advisories_listing.html) 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") 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 columns) 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).

Train	Engineering Special	Service Release	Maintenance Release
3.2 and earlier			migrate to 3.3
3.3	3.3(3)ES61 3.3(4)ES25		or later 3.3(5)
4.0	4.0(2a)ES40	4.0(2a)SR2b	no release planned
4.1	4.1(2)ES33 4.1(3)ES07	4.1(3)SR1	no release planned

## Workarounds

The effectiveness of any workaround 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 is the most appropriate for use in the intended network before it is deployed.

While there are no workarounds available on the Cisco CallManager to eliminate 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 to restrict access to the Cisco CallManager, the risk of successful attack

is greatly reduced. Please refer to the SAFE: IP Telephony Security in Depth white paper located off the SAFE Blueprint <http://www.cisco.com/go/safe> introduction page. Also, Cisco provides Solution Reference Network Design (SRND) guides to help design and deploy networking solutions. <http://www.cisco.com/warp/public/779/largeent/it/ese/srnd.html>

The specific access list examples given below need to be tailored for each network's needs and added to the other access list entries in place. If you have gateways or other devices outside of the CallManager VLAN, you can configure specific ACL entries permitting access from those device IP addresses. See the list of CallManager ports used [http://www.cisco.com/en/US/products/sw/voicesw/ps556/products\\_tech\\_note09186a00801a62b9.shtml](http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_tech_note09186a00801a62b9.shtml)

- **CSCed37403** — To secure the Cisco CallManager cluster the following ports should be blocked between the CCM cluster and the rest of the network:  
Access-list 100 deny tcp any <CallManager IP subnet> <subnet wildcard> eq 2555  
Access-list 100 deny tcp any <CallManager IP subnet> <subnet wildcard> eq 2556
- **CSCee00116, CSCee00118** — To secure the Cisco CallManager cluster the following ports should be blocked between the CCM cluster and the rest of the network:  
UDP 1719 – H.323 RAS  
TCP 1720 – H.323 H.225  
TCP 2001 – SCCP  
TCP 2002 – SCCP  
TCP 2428 – MGCP  
TCP 2748 – TAPI/JTAPI Applications  
Access-list 100 deny tcp any <CallManager IP subnet> <subnet wildcard> eq 1719  
Access-list 100 deny tcp any <CallManager IP subnet> <subnet wildcard> eq 1720  
Access-list 100 deny tcp any <CallManager IP subnet> <subnet wildcard> eq 2001  
Access-list 100 deny tcp any <CallManager IP subnet> <subnet wildcard> eq 2002  
Access-list 100 deny tcp any <CallManager IP subnet> <subnet wildcard> eq 2428  
Access-list 100 deny tcp any <CallManager IP subnet> <subnet wildcard> eq 2748  
If there are devices that need to have access to any of these ports from outside the secured CallManager VLAN(s), permit those device IP's explicitly. Example devices include Voice Gateways, TAPI/JTAPI Softphones, as well as other Voice Application Servers such as IPCC Express, etc. Port 2000 is the last port that needs to be secured. Port 2000 is used by Skinny/SCCP IP Phones to communicate with the CallManager. Permit only traffic coming from the Voice VLAN s to access port 2000.  
Access-list 100 permit tcp <voice VLAN subnet> <subnet wildcard> <CallManager IP subnet> <subnet wildcard> eq 2000  
Note: If IP Communicator is used on the data VLAN, specific ACL entries can be added to allow IP Communicator operation.
- **CSCef47060** — This vulnerability is only applicable if you have enabled MLA (Multi Level Administration) and you are running Cisco CallManager 4.0(2) without SR1 (Service Release) or later. All other releases are not vulnerable. MLA is not on by default and the enable status can be checked under CCM/User/Access Rights/MLA Parameters/Enable Multi Level Admin. Disabling and re-enabling will release excess memory used, mitigating the effects of an attack. For a vulnerable server, TCP port 80 needs to be secured in order to limit access to the web pages. This can be done in two ways:
  - 1) Permit only trusted IP addresses access to this port until a patch can be applied. Users will not be able to access Phone Services, Directory & CCMUser pages. The following ACL will turn off web access completely.  
Access-list 100 deny tcp any <CallManager IP subnet> <subnet wildcard> eq 80
  - 2) Configure Windows IIS so that MLA related virtual directories permit access only to specific IP s, while other directories are left open for user access.  
How to enable Internet Information Services (IIS) IP Address Access Restrictions:
    1. Click Start > Programs > Administrative Tools > Internet Services Manager to open the IIS

management console.

2. Select Internet Information Services > [Computer Name] > Default Web Site.
  3. Right click the CCMAAdmin virtual directory and select Properties.
  4. Click the Directory Security tab.
  5. Click Edit for IP address and domain name restrictions.
  6. Select Denied Access.
  7. Click Add.
  8. Select Single Computer or Group of Computers.
  9. Type the IP Address or Network ID and Subnet Mask to be granted access.
  10. Click OK.
  11. Repeat Steps 7 – 10 until all desired IP Addresses or Networks have been granted access.
  12. Click OK.
  13. Return to Step 3 and repeat the steps for the following virtual directories: CCMService, CCMTraceAnalysis, AST, RTMTReports, SOAP.
  14. Click OK out of all the open windows.
  15. Test connectivity from an allowed and denied IP address to confirm the filter is in place.
- **CSCsa75554** --- To secure the Cisco CallManager cluster block port 8001 between the CCM cluster and the rest of the network:  
Access-list 100 deny tcp any <CallManager IP subnet> <subnet wildcard> eq 8001  
If there are Cisco CallManagers that need access to this service from outside the secured CallManager VLAN, permit those device IP addresses explicitly.

## 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 assistance with the upgrade, which should be free of charge.

## 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.

- +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](mailto:tac@cisco.com)

Please 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.

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

If you need assistance with the implementation of the workarounds, or have questions on the workarounds, please contact the Cisco Technical Assistance Center (TAC).

- +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](mailto:tac@cisco.com)

See <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.

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>.

## Exploitation and Public Announcements

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

The aupair service vulnerability (CSCsa75554) was reported to Cisco by Internet Security Systems who will also be making public announcements regarding this issue.

Jeff Fay from PatchAdvisor will issue a report on his findings of CSCee00116 on their vulnerability alert service.

## 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 will be posted on Cisco's worldwide website at

<http://www.cisco.com/warp/public/707/cisco-sa-20050712-ccm.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](mailto:cust-security-announce@cisco.com)
- [first-teams@first.org](mailto:first-teams@first.org) (includes CERT/CC)
- [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)
- [cisco@spot.colorado.edu](mailto:cisco@spot.colorado.edu)
- [cisco-nsp@puck.nether.net](mailto:cisco-nsp@puck.nether.net)
- [cisco-voip@puck.nether.net](mailto:cisco-voip@puck.nether.net)
- [full-disclosure@lists.grok.org.uk](mailto:full-disclosure@lists.grok.org.uk)
- [comp.dcom.sys.cisco@newsgate.cisco.com](mailto: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 1.1	2005-July-18	Workaround section added example of restricting access to the Cisco Call Manager.
Revision 1.0	2005-July-12	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](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 © 2006–2007 Cisco Systems, Inc. All rights reserved. [Important Notices](#) and [Privacy Statement](#).

---

Updated: Jul 18, 2005

Document ID: 65529

---