

Cisco Security Advisory: Cisco Unified Communications Manager and Presence Server Unauthorized Access Vulnerabilities

Advisory ID: [cisco-sa-20070711-voip](#)

<http://www.cisco.com/warp/public/707/cisco-sa-20070711-voip.shtml>

Revision 1.0

For Public Release 2007 July 11 1600 UTC (GMT)

Please provide your [feedback](#) on this document.

Contents

- [Summary](#)
- [Affected Products](#)
- [Details](#)
- [Vulnerability Scoring Details](#)
- [Impact](#)
- [Software Version and Fixes](#)
- [Workarounds](#)
- [Obtaining Fixed Software](#)
- [Exploitation and Public Announcements](#)
- [Status of this Notice: FINAL](#)
- [Distribution](#)
- [Revision History](#)
- [Cisco Security Procedures](#)

Summary

Cisco Unified Communications Manager (CUCM), formerly CallManager, and Cisco Unified Presence Server (CUPS) contain two vulnerabilities that could allow an unauthorized administrator to activate and terminate CUCM / CUPS system services and access SNMP configuration information. This may respectively result in a denial of service (DoS) condition affecting CUCM/CUPS cluster systems and the disclosure of sensitive SNMP details, including community strings.

There are no workarounds for these vulnerabilities.

Cisco has made free software available to address these vulnerabilities for affected customers.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20070711-voip.shtml>.

Affected Products

Note: Cisco Unified CallManager versions 4.2, 4.3, 5.1 and 6.0 have been renamed as Cisco Unified Communications Manager. CUCM versions 3.3, 4.0, 4.1 and 5.0 retain the Cisco Unified CallManager name.

Vulnerable Products

These products are vulnerable:

- Cisco Unified CallManager 5.0 and Communications Manager 5.1 versions up to and including 5.1(2)
- Cisco Unified Presence Server 1.0 versions up to and including 1.0(3)

Administrators of systems running CUCM version 5.x and CUPS version 1.x can determine the software version by viewing the main page of the CUCM/CUPS Administration interface. The software version can also be determined by running the command **show version active** via the Command Line Interface (CLI).

Products Confirmed Not Vulnerable

- Cisco Unified CallManager versions 3.3, 4.0, 4.1, 4.2
- Cisco Unified Communications Manager versions 4.3, 6.0
- Cisco Unified Presence Server version 6.0

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

Details

- **Unauthorized Administrator Can Activate/Terminate CUCM/CUPS System Services**
An unauthorized CUCM/CUPS administrator may be able to activate and terminate system services in a CUCM/CUPS cluster environment. This may result in a denial of critical voice services. The unauthorized administrator cannot make changes to or view the configuration of the vulnerable CUCM/CUPS system, with the exception of viewing SNMP settings, which is documented in the next vulnerability. The CUCM issue is documented by Cisco Bug ID CSCsj09859. The CUPS issue is documented by Cisco Bug ID CSCsj19985.
- **Unauthorized Administrator Can View CUCM/CUPS SNMP Settings**
An unauthorized CUCM/CUPS administrator may be able to view sensitive SNMP configuration information in a CUCM/CUPS cluster environment. This may result in the disclosure of sensitive information, including SNMP community strings. The CUCM issue is documented in Cisco Bug ID CSCsj20668. The CUPS issue is documented in Cisco Bug ID CSCsj25962.

Vulnerability Scoring Details

Cisco is providing scores for the vulnerabilities in this advisory based on the Common Vulnerability Scoring System (CVSS). The CVSS scoring in this Security Advisory is done in accordance with CVSS version 1.0.

Cisco will provide a base and temporal score. Customers can then compute environmental scores to assist in determining the impact of the vulnerability in individual networks.

Cisco PSIRT will set the bias in all cases to normal. Customers are encouraged to apply the bias parameter when determining the environmental impact of a particular vulnerability.

CVSS is a standards based scoring method that conveys vulnerability severity and helps determine urgency and priority of response.

Cisco has provided an FAQ to answer additional questions regarding CVSS at

<http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html>.

Cisco has also provided a CVSS calculator to help compute the environmental impact for individual networks at

<http://intellishield.cisco.com/security/alertmanager/cvss>.

<u>CSCsj09859</u> (registered customers only) - Unauthorized administrators can start/stop CUCM services						
Calculate the environmental score of <u>CSCsj09859</u>						
CVSS Base Score - 7						
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	Low	Not Required	Partial	Partial	Partial	Normal
CVSS Temporal Score - 5.8						
Exploitability		Remediation Level		Report Confidence		
Functional		Official-Fix		Confirmed		

<u>CSCsj19985</u> (registered customers only) - Unauthorized administrators can start/stop CUPS services						
Calculate the environmental score of <u>CSCsj19985</u>						
CVSS Base Score - 7						
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	Low	Not Required	Partial	Partial	Partial	Normal
CVSS Temporal Score - 5.8						

Exploitability	Remediation Level	Report Confidence
Functional	Official-Fix	Confirmed

[CSCsj20668](#) ([registered](#) customers only) - Unauthorized administrators can view CUCM SNMP settings

Calculate the environmental score of [CSCsj20668](#)

CVSS Base Score - 2.3						
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	Low	Not Required	Partial	None	None	Normal
CVSS Temporal Score - 1.9						
Exploitability	Remediation Level	Report Confidence				
Functional	Official-Fix	Confirmed				

[CSCsj25962](#) ([registered](#) customers only) - Unauthorized administrators can view CUPS SNMP settings

Calculate the environmental score of [CSCsj25962](#)

CVSS Base Score - 2.3						
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	Low	Not Required	Partial	None	None	Normal
CVSS Temporal Score - 1.9						
Exploitability	Remediation Level	Report Confidence				
Functional	Official-Fix	Confirmed				

Impact

Successful exploitation of the service activation/termination vulnerability may result in a DoS condition affecting critical voice services. An attacker could disable central CUCM services, effectively causing the complete disruption of a CUCM cluster.

Successful exploitation of the SNMP settings vulnerability may result in the disclosure of sensitive network configuration information, including SNMP community strings. Using this information, an attacker may be able to leverage access to sensitive information on other systems in the network. It is a common practice in many enterprise environments to utilize standardized SNMP community strings. This may compound the severity of this vulnerability.

Software Version 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.

Workarounds

There are no workarounds for these vulnerabilities. It is possible to mitigate these vulnerabilities by permitting only trusted CUCM/CUPS cluster nodes and administrator workstations to access TCP port 8443 on a vulnerable CUCM/CUPS system.

Although it is often difficult to block traffic transiting your network, it is possible to identify traffic which should never be allowed to target your infrastructure devices and block that traffic at the border of your network. Infrastructure ACLs are considered a network security best practice and should be considered as a long-term addition to good network security, as well as a workaround for this specific vulnerability. The filters shown above should be included as part of an infrastructure access list, which will protect all devices with IP addresses in the infrastructure IP address range.

The white paper entitled "Protecting Your Core: Infrastructure Protection Access Control Lists" presents guidelines and recommended deployment techniques for infrastructure protection access lists. This document is available at the following link:

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml

Filters blocking access to TCP/8443 should be deployed at the network edge as part of a transit access list that will protect the router where the ACL is configured, as well as other devices behind it. Further information about transit ACLs is available in the white paper "Transit Access Control Lists: Filtering at Your Edge," which is available at the following link:

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801afc76.shtml

Additional mitigations that can be deployed on Cisco devices within the network are available in the Cisco Applied Intelligence companion document for this advisory:

<http://www.cisco.com/warp/customer/707/cisco-air-20070711-cucm.shtml>

Obtaining Fixed Software

Cisco will make free software available to address this vulnerability for affected customers. This advisory will be updated as fixed software becomes available. 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.

CUCM Version	Fixed Release	Download Location
CUCM 5.0 & 5.1	CUCM 5.1(2a)	http://www.cisco.com/cgi-bin/tablebuild.pl/callmgr-51?psrtdcat20e2
CUPS Version	Fixed Release	Download Location
CUPS 1.0	CUPS 6.0(1) *	http://www.cisco.com/cgi-bin/tablebuild.pl/cups-60?psrtdcat20e2

* Development of CUPS version 1.0 is discontinued. Users should upgrade to CUPS version 6.0 to obtain fixes for these vulnerabilities.

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.

- +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.

These vulnerabilities were discovered internally by Cisco.

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-20070711-voip.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-nsp@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	2007-July-11	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>.