

Cisco Security Advisory: Multiple Cisco Unified CallManager and Presence Server Denial of Service Vulnerabilities

Advisory ID: cisco-sa-20070328-voip

<http://www.cisco.com/warp/public/707/cisco-sa-20070328-voip.shtml>

Revision 1.0

For Public Release 2007 March 28 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 CallManager (CUCM) and Cisco Unified Presence Server (CUPS) contain multiple vulnerabilities which may result in the failure of CUCM or CUPS functionality, resulting in a Denial of Service (DoS) condition. 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-20070328-voip.shtml>.

[\[Expand all sections\]](#) [\[Collapse all sections\]](#)

☐ Affected Products

☐ Vulnerable Products

These products are vulnerable:

- Cisco Unified CallManager 3.3 versions prior to 3.3(5)SR2a
- Cisco Unified CallManager 4.1 versions prior to 4.1(3)SR4
- Cisco Unified CallManager 4.2 versions prior to 4.2(3)SR1
- Cisco Unified CallManager 5.0 versions prior to 5.0(4a)SU1
- Cisco Unified Presence Server 1.0 versions prior to 1.0(3)

The software version of a CUCM / CUPS system can be determined by navigating to **Show > Software** via the administration interface.

For CUCM version 5.0 and CUPS version 1.0 systems, the software version can also be determined by running the command **show version active** in the Command Line Interface (CLI).

For CUCM version 3.x and 4.x systems, the software version can be determined by navigating to **Help > About Cisco Unified CallManager** and selecting the **Details** button via the administration interface.

☐ Products Confirmed Not Vulnerable

CUCM versions 4.3(1) and 5.1(1) are not affected by any of the vulnerabilities described in this advisory. No other Cisco products are currently known to be affected by these vulnerabilities.

[Top of the section](#) [Close Section](#)

☐ Details

Cisco Unified CallManager (CUCM) is the 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 Unified Presence Server (CUPS) is the identity tracking component of the Cisco IP telephony solution which collects information about a user's availability status, such as whether or not you are using a communications device such as a phone at a particular time. It also collects information regarding a user's communications capabilities, such as whether Web collaboration or video conferencing is enabled.

- **SCCP/SCCPS Port Scan Denial of Service**
Skinny Call Control Protocol (SCCP) is a Cisco proprietary voice protocol used to facilitate call management functions between CallManager systems and IP phones. SCCP uses TCP

port 2000 for communications. Secure SCCP (SCCPS) running on TCP port 2443 is also affected. By sending a series of specially-crafted packets to the SCCP service port, it may be possible to crash a CallManager system resulting in a denial of service affecting voice services. CUCM versions 3.x, 4.x and 5.0 are affected by this vulnerability. CUPS is not affected by this vulnerability. This issue is documented in Cisco Bug ID CSCsf10805.

- **ICMP Echo Request Flood Denial of Service**

By sending a large amount of ICMP Echo Requests (Ping) to a CUCM or CUPS system, it may be possible to cause various CUCM / CUPS services to crash resulting in a denial of service affecting voice services. CUCM versions 3.x and 4.x are not affected by this vulnerability, only CUCM version 5.0 is affected. The CUCM issue is documented in Cisco Bug ID CSCsf12698. The CUPS issue is documented in Cisco Bug ID CSCsg60930.

- **IPSec Manager Denial of Service**

The IPSec Manager Service of CUCM and CUPS is responsible for maintaining the connections between CUCM / CUPS systems deployed as a cluster. By sending a specific UDP packet to the IPSec Manager Service on UDP port 8500, it may be possible to cause the service to fail. This would impact advanced call features such as call forwarding and the ability to deploy configuration changes to CUCM / CUPS systems in a cluster. Standard call operations including the ability to place and receive calls will continue to function. Established calls will not be affected. CUCM versions 3.x and 4.x are not affected by this vulnerability, only CUCM version 5.0 is affected. The CUCM issue is documented in Cisco Bug ID CSCsg20143. The CUPS issue is documented in Cisco Bug ID CSCsg60949.

[Top of the section](#) [Close Section](#)

☐ **Vulnerability Scoring Details**

Cisco is providing scores for the vulnerabilities in this advisory based on the Common Vulnerability Scoring System (CVSS).

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>.

[CSCsf10805](#) ([registered](#) customers only) - Cisco Unified CallManager SCCP Port Scan Denial of Service

Calculate the environmental score of [CSCsf10805](#)

CVSS Base Score - **3.3**

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	Low	Not Required	None	None	Complete	Normal

CVSS Temporal Score - **2.7**

Exploitability	Remediation Level	Report Confidence
Functional	Official-Fix	Confirmed

[CSCsf12698](#) ([registered](#) customers only) - Cisco Unified CallManager ICMP Denial of Service

Calculate the environmental score of [CSCsf12698](#)

CVSS Base Score - **3.3**

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	Low	Not Required	None	None	Complete	Normal

CVSS Temporal Score - **2.7**

Exploitability	Remediation Level	Report Confidence
Functional	Official-Fix	Confirmed

[CSCsg60930](#) ([registered](#) customers only) - Cisco Unified Presence Server ICMP Denial of Service

Calculate the environmental score of [CSCsg60930](#)

CVSS Base Score - **3.3**

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	Low	Not Required	None	None	Complete	Normal

CVSS Temporal Score - **2.7**

Exploitability	Remediation Level	Report Confidence
Functional	Official-Fix	Confirmed

[CSCsg20143](#) ([registered](#) customers only) - Cisco Unified CallManager IPSec_Mgr UDP Probe Denial of Service

Calculate the environmental score of [CSCsg20143](#)

CVSS Base Score - **4.7**

--	--	--	--	--	--	--

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	Low	Not Required	None	Partial	Partial	Normal
CVSS Temporal Score - 3.9						
Exploitability		Remediation Level		Report Confidence		
Functional		Official-Fix		Confirmed		

CSCsg60949 (registered customers only) - Cisco Unified Presence Server IPSec_Mgr UDP Probe Denial of Service						
Calculate the environmental score of CSCsg60949						
CVSS Base Score - 4.7						
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	Low	Not Required	None	Partial	Partial	Normal
CVSS Temporal Score - 3.9						
Exploitability		Remediation Level		Report Confidence		
Functional		Official-Fix		Confirmed		

[Top of the section](#) [Close Section](#)

☐ Impact

The section describes the impact of these vulnerabilities.

- SCCP/SCCPS Port Scan Denial of Service
Successful exploitation of this vulnerability may result in the failure of CUCM causing a disruption of voice services.
- ICMP Echo Request Flood Denial of Service
Successful exploitation of this vulnerability may result in the failure of CUCM / CUPS causing a disruption of voice services.
- IPSec Manager Denial of Service
Successful exploitation of this vulnerability may result in the failure of certain CUCM / CUPS cluster operations including the advanced phone services like call forwarding and the ability propagate configuration changes between cluster nodes. Standard voice services will continue to function normally.

[Top of the section](#) [Close Section](#)

☐ 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.

Fixed software for CUCM and CUPS can be obtained here:

CUCM Version	Fixed Release	Download Location
CUCM 3.3	CUCM 3.3(5) SR2a	http://www.cisco.com/cgi-bin/tablebuild.pl/callmgr-33?psrtdcat20e2
CUCM 4.1	CUCM 4.1(3)SR4	http://www.cisco.com/cgi-bin/tablebuild.pl/callmgr-41?psrtdcat20e2
CUCM 4.2	CUCM 4.2(3)SR1	http://www.cisco.com/cgi-bin/tablebuild.pl/callmgr-42?psrtdcat20e2
CUCM 5.0	CUCM 5.0(4a) SU1	http://www.cisco.com/cgi-bin/tablebuild.pl/callmgr-50?psrtdcat20e2
CUPS Version	Fixed Release	Download Location
CUPS 1.0	CUPS 1.0 (3)	http://www.cisco.com/cgi-bin/tablebuild.pl/cups-10?psrtdcat20e2

[Top of the section](#) [Close Section](#)

☐ Workarounds

There are no workarounds for these vulnerabilities.

Filtering traffic as follows for affected CUCM / CUPS systems can be used as a mitigation technique:

- Permit TCP port 2000 (SCCP) and TCP port 2443 (SCCPS) to CUCM systems only from VoIP endpoints.
- ICMP Echo Requests (type 8) should be blocked for CUCM and CUPS systems. This may affect network management applications and troubleshooting procedures.
- UDP Port 8500 (IPSec Manager) should only be permitted between CUCM / CUPS systems configured in a cluster deployment.

The ICMP Echo Request Flood Denial of Service and IPSec Manager Denial of Service vulnerabilities, described in this document may be exploited by spoofed attacks.

Transit Access Lists can also be deployed at your network edge as a potential mitigation technique. Refer to <http://www.cisco.com/warp/public/707/tacl.html> for examples on how to apply ACLs on Cisco routers and switches for protection.

Additional mitigations that can be deployed on Cisco devices within the network are available in the Cisco Applied Mitigation Bulletin companion document for this advisory: <http://www.cisco.com/warp/public/707/cisco-amb-20070328-voip.shtml>

[Top of the section](#) [Close Section](#)

☐ **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.

[Top of the section](#) [Close Section](#)

☐ **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>.

[Top of the section](#) [Close Section](#)

☐ **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.

[Top of the section](#) [Close Section](#)

☐ **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.

[Top of the section](#) [Close Section](#)

☐ **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 SCCP denial of service vulnerability was reported to Cisco by a customer. The ICMP Echo Request and IPSec Manager Service denial of service vulnerabilities were discovered internally by Cisco.

[Top of the section](#) [Close Section](#)

☐ **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.

[Top of the section](#) [Close Section](#)

☐ **Distribution**

This advisory is posted on Cisco's worldwide website at :
<http://www.cisco.com/warp/public/707/cisco-sa-20070328-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.

[Top of the section](#) [Close Section](#)

☐ **Revision History**

Revision 1.0	2007-March-28	Initial public release.
--------------	---------------	-------------------------

[Top of the section](#) [Close Section](#)

☐ **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>.

[Top of the section](#) [Close Section](#)

Help us help you.

Please rate this document.

- Excellent
- Good
- Average
- Fair
- Poor

This document solved my problem.

- Yes
- No
- Just browsing

Suggestions for improvement:

(256 character limit)

Home	How to Buy	Login	Profile	Feedback	Site Map	Help
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------