

# Cisco Security Advisory: Cisco Unified Presence Denial of Service Vulnerabilities

Advisory ID: cisco-sa-20080514-cup

<http://www.cisco.com/warp/public/707/cisco-sa-20080514-cup.shtml>

## Revision 1.0

For Public Release 2008 May 14 1600 UTC (GMT)

---

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

---

## Contents

[Summary](#)

[Affected Products](#)

[Details](#)

[Vulnerability Scoring 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 Unified Presence contains three denial of service (DoS) vulnerabilities that may cause an interruption in presence services. These vulnerabilities were discovered internally by Cisco, and there are no workarounds.

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080514-cup.shtml>.

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

## ☐ Affected Products

### ☐ Vulnerable Products

Cisco Unified Presence versions prior to 6.0(3) are affected by the vulnerabilities described in this advisory.

Administrators of systems running all Cisco Unified Presence versions can determine the software version by viewing the main page of the Cisco Unified Presence Administration interface. The software version can be determined by running the command **show version active** via the Command Line Interface (CLI).

### ☐ Products Confirmed Not Vulnerable

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

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

## ☐ Details

Cisco Unified Presence collects information about a user's availability status and communications capabilities. Using information captured by Cisco Unified Presence, applications such as Cisco Unified Personal Communicator and Cisco Unified Communications Manager can improve productivity by helping users connect with colleagues more efficiently by determining the most effective means for collaborative communication.

The Presence Engine service of Cisco Unified Presence version 1.0 contains two vulnerabilities that occur when a series of malformed IP packets are received by a vulnerable Cisco Unified Presence system and may result in a DoS condition. There are no workarounds for these vulnerabilities. These vulnerabilities are fixed in Cisco Unified Presence version 6.0(1). Cisco Unified Presence version 6.0(1) is the upgrade path for Cisco Unified Presence version 1.0. The first vulnerability is documented in [CVE-2008-1158](#) and Cisco Bug ID CSCsh50164. The second vulnerability is documented in [CVE-2008-1740](#) and Cisco Bug ID [CSCsh20972](#) ( [registered](#) customers only) .

The SIP Proxy service of Cisco Unified Presence versions 6.0(1) and 6.0(2) contain a vulnerability that occurs when a TCP port scan is received by a vulnerable Cisco Unified Presence system and may result in a DoS condition. There is no workaround for this vulnerability. This vulnerability is fixed in Cisco Unified Presence version 6.0(3). This vulnerability is documented in [CVE-2008-1741](#) and Cisco Bug ID [CSCsj64533](#) ( [registered](#) customers only) .

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

## ☐ Vulnerability Scoring Details

Cisco has provided 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 2.0.

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

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

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>.

**CSCsh50164 - PE Service core dumps when it receives malformed packets**

( registered customers only)

Calculate the environmental score of CSCsh50164

CVSS Base Score - **7.8**

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete

CVSS Temporal Score - **6.4**

Exploitability	Remediation Level	Report Confidence
Functional	Official-Fix	Confirmed

**CSCsh20972 - PE Service core dumps under stress test ( registered**

**customers only)**

Calculate the environmental score of CSCsh20972

CVSS Base Score - **7.8**

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete

CVSS Temporal Score - **6.4**

Exploitability	Remediation Level	Report Confidence
Functional	Official-Fix	Confirmed

**CSCsj64533 - SIPD service core dumps during TCP port scan ( registered**

**customers only)**

Calculate the environmental score of CSCsj64533

CVSS Base Score - **7.8**

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
CVSS Temporal Score - <b>6.4</b>					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

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

## Impact

Successful exploitation of any of the vulnerabilities may result in the interruption of presence services.

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

## 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.

Fixes for all the vulnerabilities listed in this advisory are included in Cisco Unified Presence version 6.0(3) that is available at the following link:

<http://www.cisco.com/cgi-bin/tablebuild.pl/cup-60?psrtdcat20e2> ( [registered](#) customers only) .

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

## Workarounds

There are no workarounds for these vulnerabilities.

## ☐ **Obtaining Fixed Software**

Cisco has released free software updates that address these vulnerabilities. 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/en/US/docs/general/warranty/English/EU1KEN\\_.html](http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html), or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact [psirt@cisco.com](mailto:psirt@cisco.com) or [security-alert@cisco.com](mailto: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 agreements 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 do not hold a Cisco service contract, and customers who purchase through third-party vendors but are unsuccessful in obtaining fixed software through their point of sale should acquire 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

Customers should have their product serial number available and be prepared to give the URL of this notice as evidence of 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 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.

These vulnerabilities were internally discovered 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-20080514-cup.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)
- [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)
- [vulnwatch@vulnwatch.org](mailto:vulnwatch@vulnwatch.org)
- [cisco@spot.colorado.edu](mailto:cisco@spot.colorado.edu)
- [cisco-nsp@puck.nether.net](mailto:cisco-nsp@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.

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

## ☐ Revision History

Revision 1.0	2008-May-14	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](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](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 - 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)