

# Cisco Security Advisory: Cisco Security Agent for Linux Port Scan Denial of Service

Document ID: 71902

Advisory ID: cisco-sa-20061025-csa

<http://www.cisco.com/warp/public/707/cisco-sa-20061025-csa.shtml>

## Revision 1.0

For Public Release 2006 October 25 1600 UTC (GMT)

---

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

---

[Summary](#)

[Affected Products](#)

[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 Security Agent (CSA) for Linux contains a denial of service vulnerability involving port scans. By performing a port scan against a system running a vulnerable version of CSA, it is possible to cause the system to become unresponsive. Cisco Unified CallManager (CUCM) and Cisco Unified Presence Server (CUPS) ship with a vulnerable CSA version.

There are workarounds for this vulnerability. Cisco has made free software available to address this vulnerability for affected customers.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20061025-csa.shtml>.

## Affected Products

### Vulnerable Products

The following CSA versions are vulnerable to the port scanning issue:

- CSA version 4.5 for Linux (standalone and managed) prior to Hotfix 4.5.1.657
- CSA version 5.0 for Linux (standalone and managed) prior to Hotfix 5.0.0.193

The following Cisco products include a standalone CSA for Linux version which are also vulnerable to this issue:

- Cisco Unified CallManager (CUCM) 5.0 versions including 5.0(4) and 5.0(4a)
- Cisco Unified Presence Server (CUPS) 1.0 versions including 1.0(2)

## Products Confirmed Not Vulnerable

The following CSA Agent versions are not vulnerable to the port scanning issue:

- CSA version 5.1 (standalone and managed) for Linux
- All CSA versions (standalone and managed) for Windows
- All CSA versions (standalone and managed) for Solaris

No other Cisco products are currently known to be affected by this vulnerability.

## Details

Cisco Security Agent (CSA) provides threat protection for server and desktop computing systems. CSA for Linux is vulnerable to a denial of service attack that may be triggered during the identification of network port scans. By running a port scan with specific options, it is possible to cause excessive system resource consumption resulting in a denial of service. It is possible to mitigate this vulnerability by restricting network access to vulnerable systems to trusted networks. This issue is not a Linux operating system issue. CSA versions for other operating systems (Windows, Solaris) are not affected by this vulnerability. This issue is documented in Cisco Bug ID [CSCse98684](#) ([registered](#) customers only) .

Cisco Unified CallManager 5.0 versions, including 5.0(4) and 5.0(4a), ship with a vulnerable version of CSA. A new CallManager Options Package (COP) file is available to update the CSA version on CallManager 5.0(4). Future versions of CallManager will include the updated CSA version. This issue is documented in Cisco Bug ID [CSCse97601](#) ([registered](#) customers only) .

Cisco Unified Presence Server 1.0 versions, including 1.0(2), ship with a vulnerable version of CSA. A new COP file is available to update the CSA version on CUPS 1.0(2). Future versions of CUPS will include the updated CSA version. This issue is documented in Cisco Bug ID [CSCsg40052](#) ([registered](#) customers only) .

## Impact

Successful exploitation of the port scan vulnerability against a Linux system running a vulnerable version of CSA may cause the system to become unresponsive due to resource exhaustion while a port scan is underway. This may result in the failure of critical processes and remote network connectivity. Repeated port scans may result in a prolonged denial of service. If a CUCM or CUPS system running a vulnerable CSA version is scanned, voice operations may become unavailable for the duration of the port scan.

## 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.

## CSA for Linux

Affected Software Version	Fixed Software Version
CSA Hotfix prior to 4.5.1.657	CSA Hotfix 4.5.1.657
CSA Hotfix prior to 5.0.0.193	CSA Hotfix 5.0.0.194 *

\* CSA Hotfix 5.0.0.194 deprecates CSA Hotfix 5.0.0.193.

Fixed CSA software can be downloaded at

<http://www.cisco.com/cgi-bin/tablebuild.pl/csa-hf-crypto?psrtdcat20e2>.

## CUCM/CUPS

Affected Software Version	Fixed Software Version
CUCM 5.0 versions including 5.0(4) and 5.0(4a)	CUCM 5.0(4) and 5.0(4a) with CSA COP upgrade
CUPS 1.0 versions including 1.0(2)	CUPS 1.0(2) with CSA COP upgrade

The CUCM COP file (platform-csa-4.5.1-657.1.cop.sgn) and installation instructions can be downloaded at <http://www.cisco.com/cgi-bin/tablebuild.pl/cmva-3des?psrtdcat20e2>.

The CUPS COP file (CUPS-1.0.2-CSA-4.5.1-657.1.i386.cop.sgn) and installation instructions can be downloaded at <http://www.cisco.com/cgi-bin/tablebuild.pl/cups-10?psrtdcat20e2>.

## Workarounds

It is possible to workaround the Linux port scan vulnerability by disabling the Netshield rule in managed agents via the CSA Management Center (CSAMC) console (not possible for standalone and CUCM/CUPS agents). Administrators should exercise caution when employing this workaround because it may open a system to additional network denial of service attacks. With the Netshield rule disabled, CSA will still provide protection against buffer overflows and other malicious activities.

## 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.

## 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](mailto: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 vulnerabilities described in this advisory.

This vulnerability was 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-20061025-csa.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.

## Revision History

Revision 1.0	2006-October-25	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: Oct 25, 2006

Document ID: 71902

---