

# Cisco Security Advisory: Multiple Vulnerabilities in Cisco Clean Access

Advisory ID: cisco-sa-20070103-CleanAccess

<http://www.cisco.com/warp/public/707/cisco-sa-20070103-CleanAccess.shtml>

## Revision 1.0

For Public Release 2007 January 03 1600 UTC (GMT)

---

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

---

## Contents

[Summary](#)

[Affected Products](#)

[Details](#)

[Impact](#)

[Software Version and Fixes](#)

[Workarounds](#)

[Obtaining Fixed Software](#)

[Customers using Third Party Support Organizations](#)

[Customers without Service Contracts](#)

[Exploitation and Public Announcements](#)

[Status of this Notice:FINAL](#)

[Distribution](#)

[Revision History](#)

[Cisco Security Procedures](#)

---

## Summary

Cisco Clean Access (CCA) is a software solution that can automatically detect, isolate, and clean infected or vulnerable devices that attempt to access your network. It consists of Cisco Clean Access Manager (CAM) and Cisco Clean Access Server (CAS) devices that work in tandem.

Cisco Clean Access is affected by the following vulnerabilities:

- Unchangeable shared secret
- Readable snapshot files

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20070103-CleanAccess.shtml>.

## Affected Products

### Vulnerable Products

The following software releases are vulnerable.

#### Unchangeable Shared Secret

- CCA releases 3.6.x - 3.6.4.2
- CCA releases 4.0.x - 4.0.3.2

#### Readable Snapshots

- CCA releases 3.5.x - 3.5.9
- CCA releases 3.6.x - 3.6.1.1

### Products Confirmed Not Vulnerable

No other Cisco products are known to be affected by the vulnerabilities described in this Advisory.

## Details

### Unchangeable Shared Secret

In order for Cisco Clean Access Manager (CAM) to authenticate to a Cisco Clean Access Server (CAS), both CAM and CAS must have the same shared secret. The shared secret is configured during the initial CAM and CAS setup. Due to this vulnerability the shared secret can not be properly set nor be changed, and it will be the same across all affected devices. In order to exploit this vulnerability the adversary must be able to establish a TCP connection to CAS.

This vulnerability is documented in Cisco Bug ID [CSCsg24153](#) ( [registered](#) customers only ) .

### Readable Snapshots

Manual backups of the database ('snapshots') taken on CAM are susceptible to brute force download attacks. A malicious user can guess the file name and download it without authentication. The file itself is not encrypted or otherwise protected.

This vulnerability is documented in Cisco Bug ID [CSCsd48626](#) ( [registered](#) customers only ) .

## 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>.

<a href="#">CSCsg24153 - Unchangeable shared secret</a> ( <a href="#">registered</a> customers only)						
CVSS Base Score - <b>8</b>						
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	High	Not Required	Complete	Complete	Complete	Normal
CVSS Temporal Score - <b>6.3</b>						
Exploitability		Remediation Level		Report Confidence		
Proof of Concept		Official Fix		Confirmed		

<a href="#">CSCsd48626 - Readable snapshot files</a> ( <a href="#">registered</a> customers only)						
CVSS Base Score - <b>10</b>						
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	Low	Not Required	Complete	Complete	Complete	Normal
CVSS Temporal Score - <b>8.3</b>						
Exploitability		Remediation Level		Report Confidence		
Functional		Official Fix		Confirmed		

## Impact

### Unchangeable Shared Secret

Successful exploitation of the vulnerability may enable a malicious user to effectively take administrative control of a CAS. After that, every aspect of CAS can be changed including its configuration and setup.

## Readable Snapshots

The snapshot contains sensitive information that can aid in the attempts, or be used to compromise the CAM. Among other things, the snapshot can contain passwords in cleartext. Starting with the release 3.6.0, passwords are no longer stored in cleartext in the snapshot files.

## 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.

The following CCA software releases contain the fixes.

## Unchangeable Shared Secret

The following software releases contain the fix for this vulnerability: 3.6.4.3, 4.0.4 and 4.1.0. All subsequent releases will contain the fix.

The alternative is to install the patch Patch-CSCsg24153.tar.gz which is available at <http://www.cisco.com/cgi-bin/tablebuild.pl/cca-patches>. This patch provides the fix only for the Unchangeable Shared Secret issue and does not address any other vulnerability.

## Readable Snapshots

The following software releases contain the fix for this vulnerability: 3.5.10 and 3.6.2. All subsequent releases will contain the fix.

## Workarounds

There are no workarounds for these vulnerabilities.

Possible mitigation of threat posed by readable snapshot files is to remove them from the device shortly after they were created. If the snapshot file needs to be preserved then it can be moved to a different computer or archived on a secondary storage. Alternately, the snapshot file can be deleted from the device.

## 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 vulnerability described in this advisory.

The readable snapshot issue was reported to Cisco by Chris Hartley from Ohio State University. The unchangeable shared secret was discovered while working on a customer's case and is unrelated to the Mr. Hartley's report.

## 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-20070103-CleanAccess.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

1.0	2007-Jan-03	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>.

---

<a href="#">Home</a>	<a href="#">How to Buy</a>	<a href="#">Login</a>	<a href="#">Profile</a>	<a href="#">Feedback</a>	<a href="#">Site Map</a>	<a href="#">Help</a>
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

All contents are Copyright © 1992-2006 Cisco Systems, Inc. All rights reserved. [Important Notices](#) and [Privacy Statement](#).