

Cisco Security Advisory: Cisco Clean Access Unauthenticated API Access

Document ID: 66068

Advisory ID: cisco-sa-20050817-cca

<http://www.cisco.com/warp/public/707/cisco-sa-20050817-cca.shtml>

Revision 1.0

For Public Release 2005 August 17 1600 UTC (GMT)

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

[Summary](#)

[Affected Products](#)

[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 Clean Access (CCA) is a software solution that can automatically detect, isolate, and clean infected or vulnerable devices that attempt to access your network.

CCA includes as part of the architecture an Application Program Interface (API). Lack of authentication while invoking API methods can allow an attacker to bypass security posture checking, change the assigned role for a user, disconnect users and can also lead to information disclosure on configured users.

Cisco has made free software patches available to address this vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050817-cca.shtml>.

Affected Products

This section provides details on affected products.

Vulnerable Products

- CCA releases 3.3.0 to 3.3.9
- CCA releases 3.4.0 to 3.4.5

- CCA releases 3.5.0 to 3.5.3

Products Confirmed Not Vulnerable

The following products are confirmed not vulnerable:

- Any CCA release previous to 3.3.0
- CCA release 3.5.4 or later

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

Details

The CCA solution comprises three main components:

- One or more CCA Servers
- A CCA Manager
- Optional CCA Agents

Customers configure the solution using a Web-based interface on the CCA Manager and the CCA Manager distributes that configuration to the CCA Servers.

As part of the solution, the CCA Manager offers a documented way to access the CCA Manager API using the Hypertext Transfer Protocol (HTTP) over TLS (HTTPS) protocol. The API provides methods to allow customer-written scripts to do the following:

- Modify the list of clean machines
- Change user roles
- Get user information
- Query a given user login time
- Modify timeout values for established user sessions
- Perform some additional functions

A complete list of methods that can be invoked in this way can be found in the CCA Manager Installation and Administration Guide, page 13–21, available at

http://www.cisco.com/en/US/products/ps6128/products_user_guide_list.html

An attacker with access to the network where the CCA Manager is located can use a custom script to invoke the API without being required to provide authentication credentials.

This vulnerability is documented in the Cisco Bug Toolkit as Bug ID [CSCsb48572](#) ([registered](#) customers only)

Impact

Successful exploitation of the vulnerability may result in one or more of the following:

- Machines being added to the CCA clean list, bypassing CCA checks and being allowed access to the network regardless of their state
- Machines being removed from the CCA clean list, preventing those machines from accessing the network
- Users being assigned to different roles than those configured by the CCA administrator, possibly granting access to parts of the network that they should not been allowed to access

- Information disclosure – by using the API to query the CCA Manager an attacker could collect user names and properties of users configured in the CCA Manager

Software Versions and Fixes

When considering software upgrades, please also consult http://www.cisco.com/en/US/products/products_security_advisories_listing.html 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") for assistance.

Cisco has developed a software fix for this vulnerability for all affected versions. Once the fix is applied to a CCA Manager running an affected release, any attempt to access the API by a custom script will be authenticated against the user database.

In order to get the fix, customers should access the CCA [software patches download](#) page. The fix consists of two files:

- Patch–CSCsb48572.tar.gz – this file contains the fix for all affected software versions. It will determine at runtime the CCA software version in use and apply the appropriate fix.
- Readme–Patch–CSCsb48572.txt – this file contains instructions on how to apply the fix to a vulnerable CCA Manager server.

Workarounds

The effectiveness of any workaround 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 is the most appropriate for use in the intended network before it is deployed.

No specific workaround has been identified for this vulnerability. However, this vulnerability can be mitigated by restricting access to the CCA Manager to known, trusted IP addresses. A sample access–list would be as follows (**Note:** ACL entries have been wrapped for easier reading) :

```
access-list 101 permit tcp <management network address> <management network mask> \  
    host <CCA Manager server address> eq 443  
access-list 101 permit tcp host <management host> \  
    host <CCA Manager server address> eq 443  
access-list 101 deny tcp any host <CCA Manager server address> eq 443  
access-list 101 permit ip any any  
  
interface type/number  
    ip access-group 101 in
```

Refer to the SAFE Security Blueprint for Enterprise Networks (available at <http://www.cisco.com/go/safe>) for additional information about how to secure your network management infrastructure.

Obtaining Fixed Software

Cisco has made free software available to address this vulnerability for affected customers. 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 assistance with the upgrade, which should be free of charge.

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

Please 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.

Please do not contact either "psirt@cisco.com" or "security-alert@cisco.com" for software upgrades.

See <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.

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>.

Exploitation and Public Announcements

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerability described in this advisory.

Cisco would like to thank Troy Holder from the North Carolina State University for bringing this to our attention.

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-20050817-cca.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 (includes CERT/CC)
- 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	2005 August 17	Initial 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>.

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. [Important Notices](#) and [Privacy Statement](#).

