

[NEWS] Cisco API Privileges Escalation

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-08/0075.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/18/05

To: list@securiteam.com

Date: 18 Aug 2005 15:02:45 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Cisco API Privileges Escalation

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."

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.

DETAILS

Vulnerable Systems:

- * 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

Immune Systems:

- * Any CCA release prior to 3.3.0
- * CCA release 3.5.4 or later

As part of the solution, the CCA Manager offers a documented way to access

Securiteam: [NEWS] Cisco API Privileges Escalation

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
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.

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.

Vendor Status:

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.

ADDITIONAL INFORMATION

The information has been provided by <mailto:psirt@cisco.com> Cisco Systems Product Security Incident Response Team.

The original article can be found at:

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

Securiteam: [NEWS] Cisco API Privileges Escalation

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.