

# [NT] Multiple Vulnerabilities in Cisco 802.1X Supplicant

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-02/msg00077.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxxx)>
  - *Date:* 22 Feb 2007 13:44:06 +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>

-----

Multiple Vulnerabilities in Cisco 802.1X Supplicant

---

## SUMMARY

The Cisco Secure Services Client (CSSC) is a software client that enables customers to deploy a single authentication framework using the 802.1X authentication standard across multiple device types to access both wired and wireless networks. A lightweight version of the CSSC client is also a component of the Cisco Trust Agent (CTA) within the Cisco Network Admission Control (NAC) Framework solution.

Cisco Secure Services Client (CSSC), Cisco Trust Agent (CTA) and Cisco Network Admission Control (NAC) are affected by multiple vulnerabilities including privilege escalations and information disclosure.

Cisco has made free software available to address these vulnerabilities for affected customers.

## DETAILS

Affected Products:

This section provides details on affected products.

## [NT] Multiple Vulnerabilities in Cisco 802.1X Supplicant

### Vulnerable Products

Any version of the following software clients, prior to the versions which are listed in the Software Versions and Fixes section below, may be vulnerable.

- \* Cisco Secure Services Client 4.x versions
- \* Cisco Trust Agent 1.x and 2.x versions
- \* Meetinghouse AEGIS SecureConnect Client (Windows platform versions)
- \* Cisco Security Agent (CSA) bundle versions 5.0 and 5.1

To determine the version of the Cisco Trust Agent installed, the `ctastat` command found in the

`\Program Files\Cisco Systems\CiscoTrustAgent`

directory will provide output similar to:

Cisco Trust Agent Statistics

Current Time: Tue Sep 27 19:11:18 2005

CTA Version: 2.0.0.26

To determine the version of the Cisco Secure Services Client installed, the software version information may be found in "About" dialog window which may be launched underneath the Help tab within the client.

Cisco Security Agent bundle versions 5.0 and 5.1 included Cisco Trust Agent software within the bundle. Customers who have deployed CTA as part of their CSA client package may be vulnerable if the version of CTA included is a version which is affected.

### Products Confirmed Not Vulnerable

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

### Details:

The Cisco Secure Services Client (CSSC) is a software client that enables customers to deploy a single authentication framework using the 802.1X authentication standard across multiple device types to access both wired and wireless networks. Previously this product was marketed as the Meetinghouse AEGIS SecureConnect client.

Cisco Trust Agent (CTA) installed on end-hosts is a core component of the Cisco Network Admission Control (NAC) Framework solution. CTA optionally includes a lightweight version of CSSC to provide authentication as part of the NAC Framework solution, using the network infrastructure to enforce security policy compliance on all devices seeking to access network computing resources.

Both products are affected by multiple vulnerabilities including privilege escalations and password disclosure.

### Privilege Escalations

## [NT] Multiple Vulnerabilities in Cisco 802.1X Supplicant

Four privilege escalation vulnerabilities exist in both products.

- \* It is possible for an unprivileged user who is logged into the computer to increase their privileges to the local system user via the help facility within the supplicant Graphical User Interface (GUI). This vulnerability is documented by Cisco Bug ID [CSCsf14120](http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsf14120) ( registered customers only)
- \* An unprivileged user who is logged into the computer is able to launch any program on a system to run with SYSTEM privileges from within the supplicant application. This vulnerability is documented by Cisco Bug ID [CSCsf15836](http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsf15836) ( registered customers only)
- \* Insecure default Discretionary Access Control Lists (DACL) for the connection client GUI (ConnectionClient.exe) allows an unprivileged user to inject a thread under ConnectionClient.exe running with SYSTEM level privileges. This vulnerability is documented by Cisco Bug ID [CSCsg20558](http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsg20558) ( registered customers only)
- \* Due to the method used in parsing commands, it is possible that an unprivileged user who is logged into the computer could launch a process as the local system user. This vulnerability is documented by Cisco Bug IDs [CSCsh30297](http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsh30297) ( registered customers only) and [CSCsh30624](http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsh30624) ( registered customers only) .

### Password Disclosure

With authentication methods which convey a password in a protected tunnel the users password will be logged in cleartext in the application log files described below (assuming default installation paths). This will occur with the following methods:

- \* TTLS CHAP
- \* TTLS MSCHAP
- \* TTLS MSCHAPv2
- \* TTLS PAP
- \* MD5
- \* GTC
- \* LEAP
- \* PEAP MSCHAPv2
- \* PEAP GTC
- \* FAST

### CTA Wired Client:

- \* \Program Files\Cisco Systems\Cisco Trust Agent 802\_1x Wired Client\system\log\apiDebug\_current.txt
- \* \Program Files\Cisco Systems\Cisco Trust Agent 802\_1x Wired Client\system\log\apiDebug\_1.txt
- \* \Program Files\Cisco Systems\Cisco Trust Agent 802\_1x Wired

## [NT] Multiple Vulnerabilities in Cisco 802.1X Supplicant

Client\system\log\apiDebug\_2.txt

Cisco Secure Services Client:

- \* \Program Files\Cisco System\Cisco Secure Services Client\system\log\apiDebug\_current.txt
- \* \Program Files\Cisco System\Cisco Secure Services Client\system\log\apiDebug\_1.txt
- \* \Program Files\Cisco System\Cisco Secure Services Client\system\log\apiDebug\_2.txt

AEGIS Secure Connect:

- \* \Program Files\Meetinghouse\AEGIS SecureConnect\System\log\apiDebug\_current.txt
- \* \Program Files\Meetinghouse\AEGIS SecureConnect\System\log\apiDebug\_1.txt
- \* \Program Files\Meetinghouse\AEGIS SecureConnect\System\log\apiDebug\_2.txt

This log file is rotated on a regular basis and will be recreated if the file has been deleted.

This vulnerability is documented by Cisco Bug ID

<<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsg34423>>  
CSCsg34423 ( registered customers only)

Impact:

Successful exploitation of any one of the four privilege escalation vulnerabilities may result in a user gaining privilege to run programs, read or modify files, or otherwise damage the integrity, confidentiality, and availability of the system.

If any of the authentication methods described earlier is employed, then a user who can access the apiDebug\_current.txt file or previous copies of this file created via normal log rotation may see passwords of other users in cleartext, enabling them to impersonate and authenticate as those users gaining the privilege and identity of the compromised user account.

Workarounds:

There are no workarounds available for the privilege escalation vulnerabilities.

The password disclosure vulnerability may be temporarily mitigated by deleting the current apidebug\_current.txt file and previous versions of the file. This workaround is only temporary as those files will be automatically recreated by the application.

### ADDITIONAL INFORMATION

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

[NT] Multiple Vulnerabilities in Cisco 802.1X Supplicant

The original article can be found at:

<<http://www.cisco.com/warp/public/707/cisco-sa-20070221-supplicant.shtml>>

<http://www.cisco.com/warp/public/707/cisco-sa-20070221-supplicant.shtml>

=====

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@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====

=====

**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.