

# Cisco Security Advisory: Multiple Vulnerabilities in 802.1X Supplicant

Document ID: 81676

Advisory ID: cisco-sa-20070221-supplicant

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

## Revision 1.1

Last Updated 2007 March 01 0100 UTC (GMT)

For Public Release 2007 February 21 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

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.

These products are affected by multiple vulnerabilities including privilege escalations and information disclosure.

Cisco Security Agent (CSA) 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. This vulnerability does not impact the the CSA client or server software.

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

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20070221-supplicant.shtml>.

Cisco Security Advisory: Multiple Vulnerabilities in 802.1X Supplicant

## Affected Products

This section provides details on affected products.

## 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)

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.

## 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

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 ( registered customers only)

Cisco Security Advisory: Multiple Vulnerabilities in 802.1X Supplicant

- 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 ( 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 ( 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 ( registered customers only) and 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 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 CSCsg34423 ( 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>.

CSCsf14120: Privilege escalation vulnerability via Help facility						
<b>Calculate the environmental score of CSCsf14120</b> 						
CVSS Base Score – 5.6						
Access Vector	Access	Authentication	Confidentiality	Integrity	Availability	Impact
Local	Complexity High	Not Required	Impact Complete	Impact Complete	Impact Complete	Bias Normal
CVSS Temporal Score – 4.6						
Exploitability	Remediation Level			Report Confidence		
Functional	Official Fix			Confirmed		

CSCsf15836: Privilege escalation vulnerability via web browser.						
<b>Calculate the environmental score of CSCsf15836</b> 						
CVSS Base Score – 7						
Access Vector	Access	Authentication	Confidentiality	Integrity	Availability	Impact
Local	Complexity Low	Not Required	Impact Complete	Impact Complete	Impact Complete	Bias Normal
CVSS Temporal Score – 5.8						
Exploitability	Remediation Level			Report Confidence		
Functional	Official Fix			Confirmed		

CSCsg20558: ConnectionClient.exe vulnerable to Local Privilege Escalation.						
<b>Calculate the environmental score of CSCsg20558</b> 						

CVSS Base Score – 7						
Access Vector	Access	Authentication	Confidentiality	Integrity	Availability	Impact
Local	Complexity Low	Not Required	Impact Complete	Impact Complete	Impact Complete	Bias Normal
CVSS Temporal Score – 5.8						
Exploitability	Remediation Level		Report Confidence			
Functional	Official Fix		Confirmed			

CSCsh30297: Security vulnerability while launching a process and CSCsh30624: Security vulnerability while launching a process.						
Calculate the environmental score of CSCsh30297 and CSCsh30624 <a href="#">↗</a>						
CVSS Base Score – 7						
Access Vector	Access	Authentication	Confidentiality	Integrity	Availability	Impact
Local	Complexity Low	Not Required	Impact Complete	Impact Complete	Impact Complete	Bias Normal
CVSS Temporal Score – 5.8						
Exploitability	Remediation Level		Report Confidence			
Functional	Official Fix		Confirmed			

CSCsg34423: User's password written to log file.						
Calculate the environmental score of CSCsg34423 <a href="#">↗</a>						
CVSS Base Score – 1.6						
Access Vector	Access	Authentication	Confidentiality	Integrity	Availability	Impact
Local	Complexity Low	Not Required	Impact Partial	Impact None	Impact None	Bias Normal
CVSS Temporal Score – 1.3						
Exploitability	Remediation Level		Report Confidence			
Functional	Official Fix		Confirmed			

## 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.

# 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 table below lists the first fixed releases for each specific vulnerability. Customers wishing to get all of the fixes may simply download CTA version 2.1.103.0 or CSSC version 4.0.51.5192.**

Category	BugID	Product	First Fixed Releases
Privilege Escalations	CSCsf14120	CTA	2.1.18.0
		CSSC	4.0.51.5192
	CSCsf15836	CTA	2.1.18.0
		CSSC	4.0.51.5192
	CSCsg20558	CTA	2.1.103.0
		CSSC	4.0.51.5192
CSCsh30297 and CSCsh30624	CTA	2.1.103.0	
	CSSC	4.0.51.5192	
Password Disclosures	CSCsg34423	CTA	2.1.103.0
		CSSC	4.0.51.5192

## 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.

## Obtaining Fixed Software

Cisco will make free software available to address these vulnerabilities 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.

Two of these vulnerabilities were reported to Cisco by a customer. The others were found internally.

## 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-20070221-supPLICANT.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 1.1	2007-March-01	Updated Cisco Security Agent (CSA) bundle versions 5.0 and 5.1 information in the Summary and Affected Products sections.
Revision 1.0	2007-February-21	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: Feb 28, 2007

Document ID: 81676

