

# Cisco Security Advisory: Vulnerability in Cisco Secure Access Control Server EAP-TLS Authentication

Document ID: 63178

Advisory ID: cisco-sa-20041102-acs-eap-tls

<http://www.cisco.com/warp/public/707/cisco-sa-20041102-acs-eap-tls.shtml>

## Revision 1.0

For Public Release 2004 November 2 1500 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

A Cisco Secure Access Control Server (ACS) that is configured to use Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) to authenticate users to the network will allow access to any user that uses a cryptographically correct certificate as long as the user name is valid. *Cryptographically correct* means that the certificate is in the appropriate format and contains valid fields. The certificate can be expired, or come from an untrusted Certificate Authority (CA) and still be cryptographically correct.

Only version 3.3.1 of the Cisco Secure ACS for Windows and Cisco Secure ACS Solution Engine is affected by this vulnerability. Cisco has made free software available to address this problem.

This vulnerability has no effect, that is, user authentication is not impacted, if EAP-TLS is configured in the Cisco Secure ACS with binary comparison of user certificates as the only comparison method *and* if the user entry in Lightweight Directory Access Protocol/Active Directory (LDAP/AD) contains only valid certificates.

No exploitations of this vulnerability have been reported.

This advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20041102-acs-eap-tls.shtml>.

# Affected Products

This section provides details on affected products.

## Vulnerable Products

Only version 3.3.1 of the Cisco Secure ACS for Windows and Cisco Secure ACS Solution Engine is affected by the vulnerability described in this document.

To determine your Cisco Secure ACS software version you can log into the Cisco Secure ACS. The first screen that is presented after a successful login will show the version number in the following format:

```
CiscoSecure ACS Release 3.3(1) Build 16..
```

ACS versions may also be displayed as 003.003(001.16), where "16" is the build number referenced on the ACS Administration Graphical User Interface (GUI).

## Products Confirmed Not Vulnerable

Cisco Secure ACS for Unix and versions of Cisco Secure ACS for Windows and Cisco Secure ACS Solution Engine prior to, and later than, 3.3.1 are **not affected** by this vulnerability. Version 3.3.1 is the first version in the 3.3.x series and version 3.3.2 is the first one that is not affected by this vulnerability. No other Cisco products are currently known to be affected by this vulnerability.

## Details

Cisco Secure Access Control Server provides centralized authentication, authorization, and accounting (AAA) services to network devices that function as AAA clients, such as a network access servers, PIX firewalls, routers and switches. With Cisco Secure ACS, network administrators can quickly administer accounts and globally change levels of service offerings for entire groups of users.

EAP is a general protocol for authentication that supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, public key authentication and smart cards.

TLS is a protocol that provides privacy and data integrity between client/server applications communicating over an unsecure network such as the Internet.

EAP and TLS are both IETF RFC standards. The EAP protocol carries initial authentication information, specifically EAPOL (the encapsulation of EAP over LANs as established by IEEE 802.1X). TLS uses certificates both for user authentication and for dynamic ephemeral session key generation. The EAP-TLS authentication protocol uses the certificates of Cisco Secure ACS and of the end-user client, enforcing mutual authentication of the client and of Cisco Secure ACS. More detailed information on EAP, TLS, and EAP-TLS can be found in the following IETF RFCs: RFC 2284 (PPP Extensible Authentication Protocol), RFC 2246 (The TLS Protocol), and RFC 2716 (PPP EAP TLS Authentication Protocol).

The vulnerability described in this document affects user authentication in the following way: when the EAP-TLS protocol is enabled in version 3.3.1 of Cisco Secure ACS for Windows or Cisco Secure ACS Solution Engine, and network devices and services are configured to authenticate users via the ACS, access will be granted to any user that uses a certificate that is cryptographically correct as long as the user name is valid and regardless of whether the certificate is from a trusted Certificate Authority or whether the certificate has expired. *Cryptographically correct* means that the certificate is in the appropriate format and contains valid fields.

If EAP–TLS is configured (through the ACS global authentication page) to perform binary comparison of user certificates as the only user certificate comparison method, user authentication is not affected by this vulnerability, as long as the user entry in LDAP/AD contains only valid certificates. The reason user authentication is not affected under this scenario is that when using the binary comparison method, the certificate that is sent by the user's machine during the EAP–TLS conversation is also compared to the user certificate that is stored in the user entry in the LDAP/AD.

The vulnerability described here is documented in the Cisco Bug ID [CSCef62913](#) ([registered](#) customers only) .

## Impact

Successful exploitation of this vulnerability could allow unauthorized access to the entire network, provided that the Cisco Secure ACS is being used to control network access.

## Software Versions and Fixes

The vulnerability described in this advisory is fixed in version 3.3.2 of the Cisco Secure ACS for Windows software and of the Cisco Secure ACS Solution Engine. If you are currently running the identified vulnerable software and are using EAP–TLS, you should obtain fixed software, as detailed below.

If you are running Cisco Secure ACS for Windows you can either upgrade to version 3.3.2 or just replace the current **CSCRL.dll** Windows Dynamic Link Library (DLL) in the Windows System32 folder with a fixed DLL and restart Cisco Secure ACS for Windows. Replacing the DLL fixes the problem and does not require a full upgrade.

The DLL fix can be downloaded from <http://www.cisco.com/cgi-bin/tablebuild.pl/cs-acs-win>. The file name is **CSCef62913-fix-ACSWIN-v3.3.1.16.zip**. The accompanying **Readme** file (available from the same location) contains detailed installation instructions.

If you are using the Cisco Secure ACS Solution Engine you can also upgrade to version 3.3.2 or run an upgrade package to replace the affected DLL (an upgrade package is needed because there is no access to the System32 directory when using the ACS Solution Engine.)

The upgrade package for the DLL fix can be downloaded from <http://www.cisco.com/cgi-bin/tablebuild.pl/acs-soleng-3des>. The file name is **CSCef62913-fix-ACSSE-v3.3.1.16.zip**. The accompanying **Readme** file (available from the same location) contains detailed installation instructions.

Either upgrade method, a full upgrade to version 3.3.2, or just an upgrade of the affected DLL, is provided free of charge.

## Workarounds

If the user account resides in an LDAP/AD server and the user certificate is stored in the user object in LDAP/AD, binary comparison of user certificates can be configured in the ACS Global Authentication page as the **only** allowed comparison method. This will work around the vulnerability described in this document provided that only valid certificates are stored in the user entry in LDAP/AD.

Please note that for this workaround to work, no other certificate comparison methods can be enabled, that is, SAN and CN certificate comparison must be disabled in the Global Authentication page.

## 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 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.

## 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 will be posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20041102-ac-s-eap-tls.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) (includes CERT/CC)
- [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.netsys.com](mailto:full-disclosure@lists.netsys.com)
- [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 1.0	2004-November-02	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>.

