

[Solutions](#) [Products](#) [Ordering](#) [Support](#) [Partners](#) [Training](#) [Corporate](#)

Security Responses

Cisco Security Response: Cisco Trust Agent - Mac OS X Privilege Escalation Vulnerability

<http://www.cisco.com/warp/public/707/cisco-sr-20070611-cta.shtml>

Revision 1.1

Last Updated 2007 June 12 1400 UTC (GMT)

For Public Release 2007 June 11 1600 UTC (GMT)

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

Contents

[Cisco Response](#)
[Additional Information](#)
[Revision History](#)
[Cisco Security Procedures](#)

Cisco Response

This is the Cisco PSIRT response to an issue discovered and reported to Cisco by Adam Blake of Deloitte, UK regarding a vulnerability in Cisco Trust Agent (CTA) installations on Mac OS X. The original report is available at the following link:

<http://www.securityfocus.com/archive/1/471041/30/0/flat>.

We greatly appreciate the opportunity to work with researchers on security vulnerabilities, and welcome the opportunity to review and assist in product reports.

This vulnerability is documented in Cisco bug ID: [CSCsi58799](#) ([registered](#) customers only)

This Cisco Security Response is posted at the following link:

<http://www.cisco.com/warp/public/707/cisco-sr-20070611-cta.shtml>.

Additional Information

CTA installations on Mac OS X contain a vulnerability that can allow an unauthorized user to access the "System Preferences" window which can be used to change passwords of all non-root user accounts, including admin accounts. The "System Preferences" window becomes available to the unauthorized user because of the "user notifications" feature within CTA. These messages are sent from Cisco Secure Access Control Server (ACS) to CTA upon completion of initial posture validation or upon posture revalidation. These notifications are displayed as pop-up messages on the desktop, or login screen, of the system on which CTA is installed.

CTAs installed on Microsoft Windows or Linux operating systems are not affected.

The impact of the vulnerability varies slightly depending on whether an authorized user has authenticated on the host before a "user notification" message is received:

- **Prior to an Authorized User Being Authenticated**
On a Mac OS X host running CTA and performing posture assessment prior to a user logging in, the "user notifications" dialog window is displayed over the top of the login screen. An unauthorized user can "click" on the message dialog window, which displays a menu bar. From the menu bar, an unauthorized user can access the "System Preferences" window and then change the passwords of all non-root user accounts, including admin accounts, and also modify other system preferences. The changing of account passwords through this method of exploitation does **not** require previous knowledge of the existing password.
- **After an Authorized User Has Been Authenticated**
On a Mac OS X host running CTA and performing posture assessment after a user has logged in, and with an active screen saver with a password set, the "user notifications" dialog window is displayed over the screen saver unlock window. An unauthorized user can "click" on the message dialog window, which displays a menu bar. From the menu bar, an unauthorized user can access the "System Preferences" window and then change passwords of all non-root user accounts, including admin accounts, and also modify other system preferences. The changing of account passwords through this method of exploitation **does** require previous knowledge of the existing password.

Workarounds

CTA release 2.1.104.0 or later resolves this vulnerability and is available for download from the following location:

<http://www.cisco.com/cgi-bin/tablebuild.pl/cta> (registered customers only)

While upgrading to CTA release 2.1.104.0 or later is recommended, users can utilize either of the following mitigations prior to upgrading the version of CTA installed on a vulnerable host:

- **Set Mode to Presentation Mode**
Configure the mode to "Presentation Mode" by updating the Info.plist file. By default, the Info.plist file is located in the /opt/CiscoTrustAgent/sbin/CtaMsg.app/Content/ directory. To set up "Presentation Mode", open the Info.plist file and add the following two lines under the "<dict>" text:

```
<key>LSUIPresentationMode</key>
<integer>4</integer>
```

- **Disable User Notifications**

User notification pop-up windows can be disabled by updating the notification settings within the ctad.ini file. By default, the ctad.ini file is located in the /etc/opt/CiscoTrustAgent/ directory.

Note: Disabling this feature prevents the end user from receiving any configured messages from the ACS after posture validation.

Set the parameter "EnableNotifies" to 0, as demonstrated in the following example:

```
[UserNotifies]
;The EnableNotifies parameter enables or disables user
; notifications. This parameter applies to logged-in users.
; Default value: 1
; Range of values 0, 1
; 0 = User notifications are disabled.
; 1 = User notifications are enabled.

EnableNotifies=0
```

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.

Revision History

Revision 1.1	2007- June-11	Updated workaround section for availability of new software release
Revision 1.0	2007- JUNE-11	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. This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

Help us help you.

Please rate this document.

- Excellent
- Good
- Average
- Fair
- Poor

This document solved my problem.

- Yes
- No
- Just browsing

Suggestions for improvement:

(256 character limit)

Home	How to Buy	Login	Profile	Feedback	Site Map	Help
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

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