

Cisco Security Advisory: Multiple Vulnerabilities in Cisco Secure Desktop

Document ID: 72020

Advisory ID: cisco-sa-20061108-csd

<http://www.cisco.com/warp/public/707/cisco-sa-20061108-csd.shtml>

Revision 1.2

Last Updated 2007 February 20 2100 UTC (GMT)

For Public Release 2006 November 08 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

Cisco Secure Desktop (CSD) software is affected by three vulnerabilities that may:

- Cause information produced and accessed during an Internet browsing session to be left behind on a computer after an SSL VPN session terminates.
- Allow users to evade the system policy that prevents them from leaving the Secure Desktop while a VPN connection is active.
- Allow local users to elevate their privileges.

Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of some of these vulnerabilities.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20061108-csd.shtml>.

Affected Products

This section provides details on affected products.

Vulnerable Products

The vulnerabilities described in this document exist in versions 3.1.1.33 and earlier of Cisco Secure Desktop.

Products Confirmed Not Vulnerable

Versions 3.1.1.45 and later of the Cisco Secure Desktop are not affected by these vulnerabilities.

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

Details

The Cisco Secure Desktop (CSD) seeks to minimize data from being left behind after an SSL VPN session terminates. In particular, CSD works to reduce, via encryption, the risk that cookies, browser history, temporary files, and downloaded content remain on a system after a remote user logs out or an SSL VPN session times out.

CSD is affected by the following vulnerabilities:

Information Leakage via Spawnd Browser

This vulnerability occurs when the Internet browser that is automatically spawned to display a home page after an SSL VPN session is established uses a directory outside of the vault maintained by CSD to store its session information, i.e. browser cache (also known as "temporary Internet files"), history, cookies, etc. This also allows users to save files downloaded during this Internet browsing session to outside of the CSD vault, which would result in unencrypted files remaining in the system after the SSL VPN connection terminates.

Please note that this vulnerability only occurs when the Cisco SSL VPN Client is configured to spawn a home page after a successful connection. Spawning a home page after a successful connection is a configuration option of the VPN headend; that is, it is not a Cisco Secure Desktop configuration option and is not enabled by default.

This vulnerability is documented by Cisco Bug ID [CSCsg05935](#) ([registered](#) customers only) SVC's spawned browser saves to nonsecure desktop.

System Policy Evasion

This vulnerability allows users to switch between the Secure Desktop and the Local (nonsecure) Desktop when using certain applications that attempt to switch to the default desktop. This can occur even when the system administrator has configured CSD to prevent switching between the Secure Desktop and the Local Desktop.

This vulnerability is documented by Cisco Bug ID [CSCsg11636](#) ([registered](#) customers only) Applications that switch to the default desktop cause CSD to minimize.

Local Privilege Escalation

The default permissions of the directory where CSD is installed, and its parent directory, allow any user to modify the contents of a CSD installation, including renaming, deleting and overwriting files. Unprivileged users can make use of this to elevate their privilege and obtain LocalSystem–equivalent privileges by replacing certain CSD executables that are run as system services and with LocalSystem privileges.

CSD is installed by default into the directory %SystemDrive%\Program Files\Cisco Systems\Secure Desktop\.

Note: %SystemDrive% is a Microsoft Windows environment variable that holds the drive that Windows was installed to. Normally, Windows is installed in the first hard disk and therefore %SystemDrive% is usually C:.

Please note that there are other Cisco products that install their files in a directory under %SystemDrive%\Program Files\Cisco Systems\. When these products are installed they normally inherit the permissions from the parent directory (%SystemDrive%\Program Files\Cisco Systems\). Therefore, as a side effect of this vulnerability in CSD, other products may be affected if they are installed *after* a vulnerable version of CSD is installed.

This vulnerability is documented by Cisco Bug ID [CSCsg29650](#) ([registered](#) customers only) Insecure file and directory permissions in CSD installation.

For information about local system level privileges, please refer to:

- LocalSystem Account
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dllproc/base/localsystem_account.asp

Impact

The "Information Leakage via Spawned Browser" vulnerability may cause information produced and accessed during an Internet browsing session to be left behind on a computer after an SSL VPN session terminates and after CSD has attempted to clean up all traces of the data.

The "System Policy Evasion" vulnerability may allow users to access the nonsecure desktop while the VPN connection is active, which is something that the system administrator may have chosen to prevent via a configuration option.

Successful exploitation of the "Local Privilege Escalation" vulnerability may result in a normal user or attacker gaining full control of the system, evading any controls put in place by the Windows system administrator.

Software Version and Fixes

The vulnerabilities described in this document are fixed in version 3.1.1.45 of the Cisco Secure Desktop software.

Cisco Secure Desktop software can be downloaded from the following location:

<http://www.cisco.com/cgi-bin/tablebuild.pl/securedesktop?psrtdcat20e2> ([registered](#) customers only)

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.

Workarounds

This section describes workarounds for these vulnerabilities.

Information Leakage via Spawnd Browser

A workaround for this vulnerability is to disable the spawning of a home page after a successful VPN connection. This setting is disabled by default and is a VPN headend configuration setting, not a Cisco Secure Desktop configuration setting.

To disable the spawning of a home page after a successful VPN connection on the Cisco VPN 3000 Series Concentrators, log into the web administration interface of the concentrator via the URL:

https://<IP address of concentrator>/admin/

and then clear the Homepage URL under "Configuration | User Management | Groups | Modify {groupname}"

For more information on setting a home page for the Cisco VPN 3000 Series Concentrators, visit the following URL:

http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_configuration_guide_chapter09186a00803ee1f01.html

To disable the spawning of a home page on the PIX and ASA security appliances, modify the "homepage" attribute under WebVPN Group Policy and User Attributes.

For more information on setting a home page for the Cisco PIX and ASA security appliances, visit the following URL:

http://www.cisco.com/en/US/products/ps6120/products_configuration_guide_chapter09186a008063b194.html#wp104

System Policy Evasion

There are no workarounds for this vulnerability.

Local Privilege Escalation

A workaround for this vulnerability is to change the permissions of the directory where CSD is installed, and all files under it, so only users with administrative privileges can modify the contents of the CSD installation. CSD is installed by default into the directory %SystemDrive%\Program Files\Cisco Systems\Secure Desktop\.

The actual permissions that need to be set can be inherited from the directory %SystemDrive%\Program Files\, which *by default*, have secure permissions.

Changing directory permissions can be accomplished using the Windows Explorer or using the CAcls.EXE command-line utility distributed with modern versions of the Microsoft Windows operating system.

As mentioned in the [Details](#) section, if another Cisco product that installs its files to its own directory under %SystemDrive%\Program Files\Cisco Systems\ is installed *after* a vulnerable version of CSD is installed, that other product may become affected as a side effect of the CSD vulnerability. Therefore, it is recommended to also fix permissions of directory and files of other Cisco products that have been installed after the installation of a vulnerable CSD version.

Please note that uninstalling CSD will remove the %SystemDrive%\Program Files\Cisco Systems\Secure Desktop\ directory, but will not remove nor change the permissions of the parent directory, i.e. %SystemDrive%\Program Files\Cisco Systems\.

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

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 vulnerabilities and limitations described in this advisory.

The "Information Leakage Via Spawned Browser" and the "System Policy Evasion" vulnerabilities were reported to Cisco by customers.

The "Local Privilege Escalation" vulnerability was reported to Cisco by iDefense. iDefense's advisory is available at <http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=442>.

Cisco would like to thank them for working with us towards coordinated disclosure of these vulnerabilities.

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-20061108-csd.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
- first-teams@first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk
- 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 1.2	2007-February-21	Clarified workaround for the "Information Leakage via Spawned Browser" vulnerability (CSCsg05935).
-----------------	------------------	--

Revision 1.1	2006–November–08	Included link to iDefense advisory.
Revision 1.0	2006–November–08	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>.

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

Updated: Feb 20, 2007

Document ID: 72020
