

Cisco Security Advisory: Local Privilege Escalation Vulnerabilities in Cisco VPN Client

Advisory ID: cisco-sa-20070815-vpnclient

<http://www.cisco.com/warp/public/707/cisco-sa-20070815-vpnclient.shtml>

Revision 1.2

Last Updated 2008 April 25 1400 UTC (GMT)

For Public Release 2007 August 15 1600 UTC (GMT)

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

Contents

[Summary](#)

[Affected Products](#)

[Details](#)

[Vulnerability Scoring 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

Two vulnerabilities exist in the Cisco VPN Client for Microsoft Windows that may allow unprivileged users to elevate their privileges to those of the LocalSystem account.

A workaround exists for one of the two vulnerabilities disclosed in this advisory.

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-20070815-vpnclient.shtml>.

[\[Expand all sections\]](#) [\[Collapse all sections\]](#)

☐ Affected Products

☐ Vulnerable Products

The vulnerabilities described in this document apply to the Cisco VPN Client on the Microsoft Windows platform. The affected versions are included in the following table:

Vulnerability Name	Versions affected	Cisco Bug ID
1. Local Privilege Escalation Through Microsoft Windows Dial-Up Networking Interface	All versions up to but not including 4.8.02.0010	CSCse89550 (registered customers only)
2. Local Privilege Escalation Through Default cvpnd.exe File Permissions	All versions up to but not including 5.0.01.0600	CSCsj00785 (registered customers only)

Note: The VPN Client for Windows software is distributed as both a Microsoft Installer (MSI) package and an InstallShield (IS) package. Only the MSI package for version 5.0.01.0600 of the VPN Client contains the fix for the "Local Privilege Escalation Through Default cvpnd.exe File Permissions" vulnerability. The IS package does **not** contain the fix for that vulnerability and has been removed from <http://www.cisco.com>. Customers who have downloaded and installed the IS package for version 5.0.01.0600 of the VPN Client will need to apply the workaround listed in the [Workarounds](#) section of this advisory or migrate to the MSI package to address these vulnerabilities.

☐ Products Confirmed Not Vulnerable

Versions of the Cisco VPN Client for platforms other than Microsoft Windows are **not affected** by these vulnerabilities. Specifically, the following versions of the Cisco VPN client are not affected:

- Cisco VPN Client for Solaris
- Cisco VPN Client for Linux
- Cisco VPN Client for Macintosh (Mac OS Classic and Mac OS X)

The Cisco AnyConnect VPN Client is not affected by these vulnerabilities.

No other Cisco products are known to be affected by the vulnerabilities described in this advisory.

Determining the Cisco VPN Client Version

To determine which version of the Cisco VPN Client is running on a Microsoft Windows machine, follow the following steps:

1. Select "Programs->Cisco Systems VPN Client->VPN Client" from the Start menu. This action will open the Cisco VPN Client graphical user interface.
2. Select the option "About VPN Client..." from the "Help" menu. This menu option will display a dialog box that contains text similar to "Cisco Systems VPN Client Version 4.8.01.0300."

Note: By default, the "Cisco Systems VPN Client" folder is located in the "Programs" sub-menu of the Windows Start menu. The system administrator may have chosen to use a different name or location.

Alternatively, the Cisco VPN Client version information can be obtained from a Microsoft Windows Command Prompt using the **vpnclient.exe version** command. For example:

```
C:\Program Files\Cisco Systems\VPN Client>vpnclient
version
4.8.01.0300
```

[Top of the section](#) [Close Section](#)

☐ Details

The Cisco VPN Client is a software solution for the Microsoft Windows, Sun Solaris, Linux, and Apple MacOS Classic and MacOS X operating systems. It allows users to establish IPsec VPN tunnels to Cisco VPN-capable devices, such as Cisco IOS routers, the PIX Security Appliance, the VPN 3000 Series Concentrators, and the ASA 5500 Series Adaptive Security Appliances.

Two vulnerabilities exist in the Cisco VPN Client for Microsoft Windows that may allow local, unprivileged users to elevate their privileges.

Note: The following vulnerabilities are different from the vulnerability that was detailed in the Cisco Security Advisory for the Cisco VPN Client for Windows available at <http://www.cisco.com/warp/public/707/cisco-sa-20060524-vpnclient.shtml>.

1. Local Privilege Escalation Through Microsoft Windows Dial-Up Networking Interface

Unprivileged users can elevate their privileges to those of the LocalSystem account by enabling the Start Before Logon (SBL) feature and configuring a VPN profile to use the Microsoft Dial-Up Networking interface. When these two settings are enabled and configured concurrently, the Cisco VPN Client Graphical User Interface (GUI) will be available in the Windows logon screen. It should be noted that configuring these two settings does **not** require the user to have administrative privileges.


From the Windows logon screen, users can leverage a VPN profile that is configured to utilize Microsoft dial-up networking to launch a dial-up networking dialog box. This action may allow users to elevate their privileges.

This vulnerability has been addressed by requiring that the configuration option "Allow launching of third party applications before logon," which is located in the "Windows Logon Properties" dialog box (available under **Options-> Windows Logon Properties...**), be enabled to use, from the Windows logon screen, a VPN profile that is configured for Microsoft Dial-Up Networking.

Note: Enabling "Allow launching of third party applications before logon" can itself raise some security issues; by design, only users with administrative rights can enable this option.

This vulnerability is documented in Cisco Bug ID [CSCse89550](#) ([registered](#) customers only) .

Additional information on the SBL feature can be found at http://www.cisco.com/en/US/docs/security/vpn_client/cisco_vpn_client/vpn_client46/win/user/guide/vc7.html#wp1301567

For information about the LocalSystem account and its privileges, please refer to <http://msdn2.microsoft.com/en-us/library/ms684190.aspx> .

2. Local Privilege Escalation Through Default cvpnd.exe File Permissions

Unprivileged users can execute arbitrary programs that run with the privileges of the LocalSystem account by replacing the Cisco VPN Service executable with arbitrary executables. This vulnerability exists because the default file permissions assigned during installation to **cvpnd.exe** (the executable for the Cisco VPN Service) allow unprivileged, interactive users to replace **cvpnd.exe** with any file.

Because the Cisco VPN Service is a Windows service running with LocalSystem privileges, unprivileged users can easily elevate their privileges.

It is possible to work around this vulnerability without a software upgrade. Please refer to the [Workarounds](#) section of this advisory.

This vulnerability is documented in Cisco Bug ID [CSCsj00785](#) ([registered](#) customers only) .

[Top of the section](#) [Close Section](#)

☐ Vulnerability Scoring Details

Cisco is providing scores for the vulnerabilities in this advisory based on the Common Vulnerability Scoring System (CVSS). The CVSS scoring in this Security Advisory is done in accordance with CVSS version 2.0.

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>

1. Local Privilege Escalation Through Microsoft Windows Dial-Up Networking Interface (CSCse89550 ([registered](#) customers only))

Calculate the environmental score of [CSCse89550](#) 

CVSS Base Score - **6.8**

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Local	Low	Single	Complete	Complete	Complete

CVSS Temporal Score - **5.9**

Exploitability	Remediation Level	Report Confidence
High	Official-Fix	Confirmed

2. Local Privilege Escalation Through Default cvpnd.exe File Permissions (CSCsj00785 ([registered](#) customers only))

Calculate the environmental score of [CSCsj00785](#) 

CVSS Base Score - **6.8**

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Local	Low	Single	Complete	Complete	Complete

CVSS Temporal Score - 5.9		
Exploitability	Remediation Level	Report Confidence
High	Official-Fix	Confirmed

[Top of the section](#) [Close Section](#)

[-] Impact

Successful exploitation of any the vulnerabilities described in this document may result in a valid, unprivileged user gaining full control of the system.

[Top of the section](#) [Close Section](#)

[-] 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.

Each row of the Cisco VPN Client software table (below) describes one of the vulnerabilities described in this document. For each vulnerability, the earliest possible release that contains the fix (the "First Fixed Release") and the anticipated date of availability for each are listed in the "First Fixed Release" column. A device running a release that is earlier than the release in a specific column (less than the First Fixed Release) is known to be vulnerable. The release should be upgraded at least to the indicated release or a later version (greater than or equal to the First Fixed Release label).

Vulnerability	First Fixed Release

1. Local Privilege Escalation Through Microsoft Windows Dial-Up Networking Interface (CSCse89550 (registered customers only))	4.8.02.0010 (MSI and IS packages)
2. Local Privilege Escalation Through Default cvpnd.exe File Permissions (CSCsj00785 (registered customers only))	5.0.01.0600 (MSI package only)

Note: The VPN Client for Windows software is distributed as both a Microsoft Installer (MSI) package and an InstallShield (IS) package. Only the MSI package for version 5.0.01.0600 of the VPN Client contains the fix for the "Local Privilege Escalation Through Default cvpnd.exe File Permissions" vulnerability. The IS package does **not** contain the fix for that vulnerability and has been removed from <http://www.cisco.com>. Customers who have downloaded and installed the IS package for version 5.0.01.0600 of the VPN Client will need to apply the workaround listed in the [Workarounds](#) section of this advisory or migrate to the MSI package to address these vulnerabilities.

Note: Customers who want to deploy a software version containing fixes for the two vulnerabilities disclosed in this advisory should deploy the MSI package for v5.0.01.0600 of the VPN Client.

The Cisco VPN Client for Windows is available for download from the following location on cisco.com:

<http://www.cisco.com/cgi-bin/tablebuild.pl/windows?psrtdcat20e2>

Please note that security fixes are **not** applied to older versions of the Cisco VPN Client for Windows software. Customers looking for a version containing fixes for all published vulnerabilities affecting the Cisco VPN Client for Windows should download and install the latest MSI package available from the previously listed URL.

Note: It has been reported that upgrades to version 5.0.01.0600 of the Cisco VPN Client in non-English versions of Microsoft Windows may fail. This issue is being tracked by Cisco Bug ID CSCsj89801, and Cisco has made available a workaround in the form of an MSI transform, which is available from <http://www.cisco.com/pcgi-bin/tablebuild.pl/windows?psrtdcat20e2> ([registered](#) customers only) (file name vpnclient-international-transform-5.0.01.0600.zip). Future versions of the Cisco VPN Client for Windows will not require this workaround.

Workarounds

1. Local Privilege Escalation Through Microsoft Windows Dial-Up Networking Interface

There are no workarounds for this vulnerability.

2. Local Privilege Escalation Through Default cvpnd.exe File Permissions

An effective workaround for this vulnerability is to revoke access rights for NT AUTHORITY \INTERACTIVE from **cvpnd.exe**. For example:

```
C:\Program Files\Cisco Systems\VPN Client>cacls cvpnd.exe /E /R "NT AUTHORITY\INTERACTIVE"
```

Note: Windows Vista includes **icacls**, an updated partial replacement for cacls. More information about **icacls** can be found at <http://www.microsoft.com/technet/technetmag/issues/2007/07/SecurityWatch/default.aspx> .

[Top of the section](#) [Close Section](#)

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/en/US/docs/general/warranty/English/EU1KEN_.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.

[Top of the section](#) [Close Section](#)

☐ **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>.

[Top of the section](#) [Close Section](#)

☐ **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.

[Top of the section](#) [Close Section](#)

☐ **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.

[Top of the section](#) [Close Section](#)

☐ **Exploitation and Public Announcements**

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerabilities described in this advisory.

The "Local Privilege Escalation Through Microsoft Windows Dial-Up Networking Interface" vulnerability (CSCse89550) was reported to Cisco by a customer.

The "Local Privilege Escalation Through Default cvpnd.exe File Permissions" vulnerability (CSCsj00785) was reported to Cisco by Dominic Beecher of Next Generation Security Software Ltd. Dominic also provided a viable workaround for this vulnerability. Cisco would like to thank Dominic Beecher and Next Generation Security Software Ltd. for reporting this vulnerability and for working with us towards a coordinated disclosure of the vulnerability.

[Top of the section](#) [Close Section](#)

☐ **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.

[Top of the section](#) [Close Section](#)

☐ **Distribution**

This advisory is posted on Cisco's worldwide website at:

<http://www.cisco.com/warp/public/707/cisco-sa-20070815-vpnclient.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.

[Top of the section](#) [Close Section](#)

☐ Revision History

Revision 1.2	2008-April-25	Updated the links to the CVSS scores for CSCse89550  and CSCsj00785  .
Revision 1.1	2007-September-12	Added information about failing upgrade in non-English versions of Microsoft Windows and the published workaround.
Revision 1.0	2007-August-15	Initial public release

[Top of the section](#) [Close Section](#)

☐ 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>.

[Top of the section](#) [Close Section](#)

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](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 - 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)