

Table of Contents

<u>Cisco Security Notice: Response to NTBugTraq – Cisco Systems VPN Client Allows Local Logon with Elevated Privileges</u>	1
<u>Revision 1.0</u>	1
<u>Last Updated 2003 May 14</u>	1
<u>Please provide your feedback on this document</u>	1
<u>Summary</u>	1
<u>Details</u>	1
<u>Cisco Security Procedures</u>	3

Cisco Security Notice: Response to NTBugTraq – Cisco Systems VPN Client Allows Local Logon with Elevated Privileges

Revision 1.0

Last Updated 2003 May 14

Please provide your feedback on this document.

Summary
Details
Cisco Security Procedures

Summary

This document is provided to simplify access to Cisco responses to possible product security vulnerability issues posted in public forums for Cisco customers. This does not imply that Cisco perceives each of these issues as an actual product security vulnerability. This notice is provided on an "as is" basis and does not imply any kind of guarantee or warranty. Your use of the information on the page or materials linked from this page are at your own risk. Cisco reserves the right to change or update this page without notice at any time.

Details

Original Report:

<http://www.ntbugtraq.com/default.asp?pid=36&sid=1&A2=ind0305&L=ntbugtraq&F=P&S=&P=4117> .

Cisco responded with the following, which is also archived at

<http://www.ntbugtraq.com/default.asp?pid=36&sid=1&A2=ind0305&L=ntbugtraq&F=P&S=&P=4605> .

```
To: NTBugTraq
Subject: Re: Cisco Systems VPN Client allows local logon with Elevated Privileges
Date: Wed, 14 May 2003 15:37:57 -0700
Author: Sharad Ahlawat <sahlawat@cisco.com>
In-Reply-To: <78C391165E0FA34090C8794E6BEB728611C7F7:nospam.ffep1w2exmb01.ffe.foxeg.com>
```

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

This is in response to the mail sent by Nick Staff. The original mail is available at [default.asp?pid=36&sid=1&A2=ind0305&L=ntbugtraq&F=P&S=&P=4117](http://www.ntbugtraq.com/default.asp?pid=36&sid=1&A2=ind0305&L=ntbugtraq&F=P&S=&P=4117)

Nick Staff writes:

=====

```
> The Cisco VPN client can be configured to start before the Windows log
> on in case a user needs to make a VPN connection before logging onto
> their domain. To that same effect the Cisco VPN client can also be
> configured to load a 3rd party application, like a dialer, to connect to
> an ISP. By default these settings are not locked to standard users
```

> because the configuration file responsible for holding these settings
> (vpnclient.ini) is installed to a non-restricted path
> (systemdrive%\program files\CiscoVPN).

Cisco Response:
=====

Hello Nick,

Thank you for your report. We always welcome the chance to work with people who wish to report product vulnerabilities to us.

To address this issue Cisco added a "Windows Logon Properties" dialog, under the "Options" menu, that allows the system administrator to enable/disable the "Allow launching of third party applications before logon" checkbox option. This checkbox option cannot be modified by a user with non-administrative privileges and is unchecked (disabled) by default. This option was added under Cisco Bug Id CSCdt76576.

This option was added in Cisco VPN Client release 3.1.24 and later for the 3.1.x releases and was also integrated in all 3.5.x, 3.6.x and 4.x. releases.

The last Cisco Security Advisory for the VPN Client posted at <http://www.cisco.com/warp/public/707/vpnclient-multiple2-vuln-pub.shtml> recommended that customers upgrade to versions of code later than the one which included this option.

As always, Cisco is interested in protecting our customers' networks and is continually striving to improve the security of our products. Vulnerabilities within any Cisco product should be reported directly to "psirt:nospam.cisco.com" or "security-alert:nospam.cisco.com".

Thank you.

Brgds,
/Sharad

On Wednesday 14 May 2003 10:09, Nick Staff wrote:

> Note: This is similar to the exploit where it's possible to log on to a
> Windows machine as local system by making a copy of cmd.exe and naming
> it logon.scr.
>
> The Cisco VPN client can be configured to start before the Windows log
> on in case a user needs to make a VPN connection before logging onto
> their domain. To that same effect the Cisco VPN client can also be
> configured to load a 3rd party application, like a dialer, to connect to
> an ISP. By default these settings are not locked to standard users
> because the configuration file responsible for holding these settings
> (vpnclient.ini) is installed to a non-restricted path
> (systemdrive%\program files\CiscoVPN).
>
> To log onto their workstation as the local system a standard user would
> simply need to configure their Cisco client to start up before windows
> log on and launch explorer.exe - this would bring them to the desktop
> where they could then do anything the local system could (add themselves
> to the local admins group, change file permissions, etc).
>
> Steps to Reproduce:
>
> - Install any 3.x version of the Cisco Systems VPN Client (could be
> other versions, but I've only tested using 3.x)
> - Open the VPN Dialer.
> - Select Options > Windows log on properties
> - Make sure all three boxes are selected (you must select the first box

```

> before the second box becomes active)
> - Click OK and then go to Options > Properties
> - Click on the connections tab and check the box next to 'Connect to the
> Internet via dial-up'
> - Select the radio button next to 3rd party dial-up application and
> enter the full path and file name of explorer.exe (i.e.
> c:\winnt\explorer.exe)
> - Click OK, Close, and then log out
>
> Note - if your desktop doesn't appear right away and instead you just
> get a 'welcome to windows' or 'configure you server' window, then close
> them, press ctrl-alt-del, and click connect when the Cisco client opens
> - then you will get the full desktop.
>
> Workarounds:
>
> Edit the ginadll value located in the registry key
> HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
> NT\CurrentVersion\Winlogon. Change the valuedata back to msgina.dll
> (Cisco client changes it to csgina.dll).
>
> or
>
> Set the security on the vpnclient.ini file to deny write permission for
> standard users (note this will prevent them from being able to import
> additional connection entries or configure any options from within the
> client).
>
> Thanks,
>
> Nick Staff

- --
Sharad Ahlawat
Cisco Product Security Incident Response Team (PSIRT)
http://www.cisco.com/go/psirt
Phone:+1 (408) 527-6087
PGP-key: http://pgp.mit.edu:11371/pks/lookup?op=get&search=0xC12A996C
-----BEGIN PGP SIGNATURE-----
Comment: PGP Signed by Sharad Ahlawat

iD8DBQE+wsVFGomMEqmWwRAoHPAKCzIehDFDOWNLXwf0Dxila7Jx5cAQCg/vFa
opJPwyG53VYhue5SUK/JJuI=
=jG9e
-----END PGP SIGNATURE-----

```

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/warp/public/707/sec_incident_response.shtml. 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 © 1992–2004 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.