

Table of Contents

<u>Cisco Security Notice: Response to NTBugTraq – Cisco VPN Client can be used to Gain Local Administrator Rights (All Versions, Patched or Otherwise)</u>	1
<u>Revision 1.0</u>	1
<u>Last Updated 2003 May 22</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 VPN Client can be used to Gain Local Administrator Rights (All Versions, Patched or Otherwise)

Revision 1.0

Last Updated 2003 May 22

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=6219> .
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=6392> .

To: NTBugTraq
Subject: Re: Cisco VPN Client can be used to gain local administrator rights (All Versions)
Date: Thu, 22 May 2003 19:30:37 -0700
Author: Sharad Ahlawat <sahlawat@cisco.com>
In-Reply-To: <78C391165E0FA34090C8794E6BEB7286136201:nospam.ffeplw2exmb01.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=6219](http://www.ntbugtraq.com/default.asp?pid=36&sid=1&A2=ind0305&L=ntbugtraq&F=P&S=&P=6219)

Physical access to the workstation and a valid user account are required to exploit this vulnerability which results in a person gaining local system administrative privileges. This vulnerability does not compromise the confidentiality of the data traversing the VPN tunnel established by the Cisco VPN Client.

Upon initial confirmation of the vulnerability, Cisco bug CSCeb12179 was opened to address the issue. Cisco continues to work on its resolution with due urgency and will announce an updated version to its customers as soon as one is tested and available.

The current workaround/mitigation technique is to make all the Cisco VPN client executable files read only for non administrative user groups.

Cisco confirmed the report of this new vulnerability on May 15, 2003 and had requested joint disclosure with the reporter once a fix was tested and available for our customers.

Cisco will continue to follow the guidelines of responsible disclosure with any reported vulnerabilities in its products. We welcome your reports and comments at psirt:nospam.cisco.com. For further information, please visit our web site at <http://www.cisco.com/go/psirt> .

/Sharad

On Thursday 22 May 2003 11:54, Nick Staff wrote:

NS>First, before getting into this exploit I think it's only fair to say
NS>that my last post, "Cisco Systems VPN Client allows local logon with
NS>Elevated Privileges" was as Cisco's representative Sharad Ahlawat said,
NS>outdated and already addressed (see following link):

NS>

NS><http://www.cisco.com/warp/public/707/vpnclient-multiple2-vuln-pub.shtml>
NS>

NS>That said, I was sufficiently enough embarrassed to see if I could get
NS>around their patched client, and here's how to do it:

NS>

NS>- Log on as a standard user.

NS>- Browse to the C:\winnt directory, right click on explorer.exe and
NS>choose copy.

NS>- Browse to C:\Program Files\Cisco Systems\VPN Client (the directory
NS>with ipsecdialer.exe) and paste a copy of explorer.exe into the folder.

NS>- Double click on ipsecdialer.exe and select options > Windows logon
NS>properties.

NS>- Click on the first box to "enable start before log on".

NS>- Click OK and Close.

NS>- Rename ipsecdialer.exe to ipsecdialer.ex_

NS>- Rename the copy of explorer.exe to ipsecdialer.exe

NS>- Close any open windows.

NS>- log out.

NS>- log back on as the same standard user.

NS>- Click okay on any error messages that appear.

NS>- DO NOT CLOSE THE EXPLORER WINDOW THAT IS OPEN.

NS>- At this point you may see your desktop or you may not (have had it
NS>happen both ways), but whatever the case, that Explorer window is open
NS>as local system and anything else you see is opened as the standard
NS>user.

NS>- In the open explorer window press the Up folder icon until you get to
NS>My computer.

NS>- Double click on Control Panel, then Administrative Tools, then
NS>Computer Management

NS>- Expand Local Users and Groups and add your Standard User account to
NS>the Local Administrators Group.

NS>

NS>The following steps are provided to return your machine to it's previous
NS>state (i.e. logging in without the client launching explorer)

NS>

NS>- Navigate to C:\Program Files\Cisco Systems\VPN Client and open the
NS>vpnclient.ini file

NS>- set runatlogon=0

NS>- Save the file and restart the machine (Ctrl-Alt-Del if no Start

```
NS>button)
NS>
NS>
NS>And to Verify the Changes took...
NS>
NS>Log on as the Standard user and do whatever you want.
NS>
NS>Cisco has been notified about this issue and has acknowledged it, but
NS>since asking for a week to test it further I have not heard from them
NS>again.
NS>
NS>Possible Issue/Workaround
NS>
NS>I can't code, but it would seem the file at fault is csgina.dll which is
NS>Cisco's replacement Gina that's installed automatically (and I assume is
NS>what allows the explorer window to be launched in the system process).
NS>Also, this exploit would be harder if not impossible were Cisco to
NS>secure their install folder, but unfortunately even if I have
NS>permissions set on the Program Files folder to only allow Users Read
NS>access the Cisco install creates a subfolder which grants the
NS>Interactive user Modify permissions. I think they do this because the
NS>program constantly re-encrypts the group authentication key which is
NS>stored in a text file in that directory.
NS>
NS>This has been Verified on Windows 2000 with SP3 and Windows 2003 Server
NS>with the newest version of the Cisco VPN client (as well as older
NS>versions too).
NS>
NS>Thanks,
NS>
NS>Nick Staff
NS>
NS>
```

--

```
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+zYfNGoGomMEqmWwRAnDBAKDTFL+75YhfAx87g8LkiVmbTlWclACfeyWN
9NIwGdso0VlaezbupA6j5XU=
=2pCG
-----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.