

Cisco VPN Client can be used to gain local administrator rights (All Versions, patched or otherwise)

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2003-05/0051.html>

From: Nick Staff (*Nick.Staff_at_FOX.COM*)

Date: 05/22/03

Date: Thu, 22 May 2003 11:54:54 -0700

To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

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Systems VPN Client allows local logon with Elevated Privileges" was as Cisco's representative Sharad Ahlawat said, outdated and already addressed (see following link):

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

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

- Log on as a standard user.
- Browse to the C:\winnt directory, right click on explorer.exe and choose copy.
- Browse to C:\Program Files\Cisco Systems\VPN Client (the directory with ipsecdialer.exe) and paste a copy of explorer.exe into the folder.
- Double click on ipsecdialer.exe and select options > Windows logon properties.
- Click on the first box to "enable start before log on".
- Click OK and Close.
- Rename ipsecdialer.exe to ipsecdialer.ex_
- Rename the copy of explorer.exe to ipsecdialer.exe
- Close any open windows.
- log out.
- log back on as the same standard user.
- Click okay on any error messages that appear.
- DO NOT CLOSE THE EXPLORER WINDOW THAT IS OPEN.
- At this point you may see your desktop or you may not (have had it happen both ways), but whatever the case, that Explorer window is open as local system and anything else you see is opened as the standard user.
- In the open explorer window press the Up folder icon until you get to My computer.
- Double click on Control Panel, then Administrative Tools, then Computer Management

NT–Bugtraq: Cisco VPN Client can be used to gain local administrator rights (All Versions, patched or otherwise)

information assets. Experience it for yourself – just click below to begin
your FREE, NO OBLIGATION 14–day trial today!

<http://www.trusecure.com/offer/s0074/>

oo