

[NT] Nortel VPN Client's Password Disclosure

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-03/0122.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 03/24/05

To: list@securiteam.com

Date: 24 Mar 2005 19:13:38 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Nortel VPN Client's Password Disclosure

SUMMARY

"The http://www.nortelnetworks.com/products/01/contivity/multi_os/ Nortel VPN Client provides user-side functionality for secure remote access over IP networks using Nortel VPN routers and VPN servers. http://www.nortelnetworks.com/products/01/contivity/multi_os/ Nortel VPN Client software works on virtually all user workstations access platforms, including Windows 2000, NT, ME, XP, Mobile (Pocket PC), IBM-AIX, SUN-Solaris, Linux and Macintosh operating systems."

Nortel VPN Client stores user and group passwords unencrypted in local memory, this makes it easy to retrieve them by simply dumping the memory of the VPN client.

DETAILS

Vulnerable Systems:

* Windows Contivity VPN client version 5.01.

While performing a VPN security test for a customer, NTA Monitor discovered that the VPN client that was being used stored the VPN password (pre-shared key) unencrypted in the memory of the process "Extranet.exe". It was possible to recover the password by dumping the process memory to a

Securiteam: [NT] Nortel VPN Client's Password Disclosure

file with <<http://ntsecurity.nu/toolbox/pmdump/>> PMDump or by crashing the system to obtain a physical memory dump with a crash-on-demand utility such as <<http://www.osronline.com/article.cfm?article=153>> Bang.

Both the user password and group password (if group authentication is being used) can be determined in this way. In the memory dump, the plain-text passwords appear near to the associated user name or group name, which makes them easy to locate. It would be simple to write a tool to extract the user name, group name and associated passwords from a memory dump file.

The vulnerability allows anyone with access to the client system to obtain the password. It may also allow anyone who has access to the obfuscated password in the client registry to use the VPN client to obtain the corresponding plain-text password, although this has not been tested.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:Roy.Hills@nta-monitor.com>> Roy Hills.

The original article can be found at:

<<http://www.nta-monitor.com/news/vpn-flaws/nortel/nortel-client/>>
<http://www.nta-monitor.com/news/vpn-flaws/nortel/nortel-client/>

=====

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@securiteam.com
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind. In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.