

[NT] Nortel Contivity VPN Client Privilege Escalation

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-08/0057.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 08/14/05

To: list@securiteam.com

Date: 14 Aug 2005 17:49:55 +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 Contivity VPN Client Privilege Escalation

SUMMARY

The Contivity VPN Client is a Windows application that lets you define and store connection information for accessing your corporate network through a Contivity Secure IP Services Gateway. When the Contivity client is running as a service it is possible to manipulate the interface of the client and escalate privileges to that of the LocalSystem account.

DETAILS

Vulnerable Systems:

* Nortel Contivity VPN Client version 05_01.030

By using the Digital Certificate Authentication Entrust attackers may receive console with the permission of LocalSystem account that will result in a privileges escalation, and will allow attackers to execute arbitrary programs, with that LocalSystem privilege.

Proof of Concept:

1. With the Contivity client open click on Options and select Authentication Options.

Securiteam: [NT] Nortel Contivity VPN Client Privilege Escalation

2. Select Digital Certificate Authentication Entrust and click OK.
3. To the right of the certificate box click the button icon and select open.
4. Change Files of type: to All Files, navigate to the system32 directory and locate cmd.exe. Right click cmd.exe and choose Open.

It should also be noted that this exploit can be carried out by running the connection wizard and following steps 2–4.

The result is a command prompt running under the context of the LocalSystem account.

Vendor Status:

The vendor was notified of the issue and an updated version has been released.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:jeff.peadro@gmail.com>> Jeff Peadro.

=====

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.