

[NEWS] Vulnerability in 3Com OfficeConnect Remote 812 ADSL Router (PAT)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-05/0117.html>

From: support@securiteam.com

Date: 05/27/02

From: support@securiteam.com

To: list@securiteam.com

Date: Mon, 27 May 2002 20:04:59 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Vulnerability in 3Com OfficeConnect Remote 812 ADSL Router (PAT)

SUMMARY

There is a problem in PAT (Port Address Translation) that can be used to access all ports in the computer behind the router. This allows attackers to cause the OfficeConnect product to effectively scan the server residing behind the ADSL router, even though the PAT should have prevented this.

DETAILS

When we try to connect to a port that is not redirected to a computer behind the router using PAT, the router does not allow this connection (this as it should). However, if connect to a port redirected using PAT and then immediately try to connect to any port not redirected using PAT, the router will allow both connections to go through (this is not as it should). The problem exists with both IP stack implementations (TCP and UDP).

Affected versions:

Version 1.1.9 and version 1.1.7 for the OCR812. For customers of SKU's 3CP4144 (Telefónica S.A. (Spain) use this model for DSL)

Securiteam: [NEWS] Vulnerability in 3Com OfficeConnect Remote 812 ADSL Router (PAT)

Impact:

Allow access to all ports on the computer behind the router. If you find a port redirected using PAT, you can access any port you desire, scan the remote host for open services, etc.

Vendor status:

Insufficient contact information regarding this vendor, no contact has been made.

ADDITIONAL INFORMATION

The information has been provided by <mailto:ismael@el-mundo.net> Ismael Briones.

=====

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.

-
- *Previous message:* support@securiteam.com: "[\[NT\] Opera Allows Reading of Any Local File](#)"
 - *Messages sorted by:* [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)