

[NEWS] Efficient Networks 5861 DSL Router (NMap DoS)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-01/0032.html>

From: support@securiteam.com

Date: 01/12/03

From: support@securiteam.com

To: list@securiteam.com

Date: 12 Jan 2003 18:38:28 +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

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit http://www.worldonline.co.za/services/work_ip.asp

Efficient Networks 5861 DSL Router (NMap DoS)

SUMMARY

<<http://www.efficient.com/ebz/5800.html>> Efficient Networks Business Class IDSL, ADSL, or SDSL Routers provide DSL access for up to 100 or more users with robust firewall and optional Secure Virtual Private Network (VPN) capabilities. Efficient Networks Business Class DSL Routers are Business Contingency Plan ready, with features such as Dial Backup and Virtual Router Redundancy Protocol (VRRP). A vulnerability in the product allows remote attackers to cause a denial of service attack against the product by simply port scanning the router's WAN interface.

DETAILS

Vulnerable systems:

* Efficient Networks 5861 DSL Router 5.3.80

When using the built-in IP filtering to block incoming TCP SYN flags, a simple port scan to the WAN interface of the router will cause it to lock up, and eventually restart.

Vendor response:

Greg has contacted Efficient Networks to inform them of the problem.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:greg@optionsinternet.com>>
Greg Bolshaw.

=====

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.