

[NEWS] 8e6 Technologies R3000 Internet Filter Bypass by Request Split

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-01/msg00056.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 25 Jan 2008 20:07:01 +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>

8e6 Technologies R3000 Internet Filter Bypass by Request Split

SUMMARY

"The <http://www.8e6.com/network-security/internet-filtering/internet-filtering.html>> 8e6 Professional Edition offers high-performance, enterprise-level filtering with the R3000 Internet Filter". The HTTP URL filtering function provided by the 8e6 Technologies R3000 Internet Filter can be bypassed by simply splitting the HTTP request line (which contains the URI) into multiple packets.

DETAILS

Vulnerable Systems:

* 8e6 version 2.0.05.33

Immune Systems:

* 8e6 version 2.0.11

Example:

packet 1: GE

packet 2: T / HTTP/1.0\r\n

This weakness is present regardless whether the site block is based on the

[NEWS] 8e6 Technologies R3000 Internet Filter Bypass by Request Split

DNS name or the IP address. For circumventing blocks based solely on the DNS name it is sufficient to arrange the HTTP request so that the request line and the Host header end up in separate packets.

Example:

packet 1: GET / HTTP/1.0

X-SomeHeader: ...

....

packet 2: X-SomeOtherHeader:

Host: www.blocked.com

...

Solution:

Use a filtering solution that performs an HTTP request reassembly.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:nnposter@xxxxxxxxxxxxxx>>
nnposter.

=====

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@xxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxx

=====

=====

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.