

[NT] Internet Explorer Handling of %20 Allows Spoofing

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-01/0076.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 01/17/05

To: list@securiteam.com

Date: 17 Jan 2005 14:19:35 +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>

Internet Explorer Handling of %20 Allows Spoofing

SUMMARY

Internet Explorer supports two forms of URI (Universal Resource Identifiers), a full qualified domain name and dotted IP. Whenever Internet Explorer receives the dotted IP form, it will ignore any characters written after an escape space sign (%20). This opens the user to attack as he can be tricked into thinking he is connecting a certain server while in fact he is connected to another.

DETAILS

Vulnerable Systems:

- * Internet Explorer version 6.0 SP1
- * Internet Explorer version 6.0 SP2
- * Internet Explorer version 5.0
- * Internet Explorer version 5.5

Apparently IE handles IPs in URLs as something like (as you might expect):

<http://xxx.xxx.xxx.xxx/>

But the problem is if you put a %20 in the IP address like this, it will

Securiteam: [NT] Internet Explorer Handling of %20 Allows Spoofing

still render (assuming I am under 16 characters between the slashes):

<http://x.x.x.x%20/>

It is looking for 16 characters and ignores anything after the %20 (space). This becomes a problem is in the case of a short URL you can put in some data here, like so:

<http://x.x.x.x%20a.com/>

Further, if the real IP address is on a server that can handle this (IIS doesn't know how to handle it in all the cases I have tested, but Apache handles it fine by default) and you have either Earthlink's FraudEliminator or CoreStreet's SpooofStick, they give incorrect information. (Please don't hit this poor guy's IP, he just happened to have one short enough to test this):

<<http://www.shocking.com/~rsnake/images/rs/percenttwenty.jpg>>
<http://www.shocking.com/~rsnake/images/rs/percenttwenty.jpg>

ADDITIONAL INFORMATION

The information has been provided by <mailto:rsnake@shocking.com> RSnake.

=====

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.