

[NEWS] Netscape ?wp-html-rend Denial of Service Attack

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-01/0041.html>

From: support@securiteam.com

Date: 01/11/02

From: support@securiteam.com

To: list@securiteam.com

Date: Fri, 11 Jan 2002 11:29:25 +0100 (CET)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Netscape ?wp-html-rend Denial of Service Attack

SUMMARY

Remote attackers can easily disable unpatched Netscape Enterprise servers running on Windows NT/2000 with publishing enabled. By fetching the URL: <http://server/?wp-html-rend> multiple times (even with a standard web browser), an attacker can crash the service remotely.

DETAILS

Vulnerable systems:

Netscape Enterprise 4.0 SP2,SP6 to 4.1 SP8 (Under Windows NT/2000)

Consequences:

Remote attackers can easily perform a denial of service attack on Netscape Enterprise servers running with Windows NT.

Detailed description:

Netscape Enterprise has a selection of ?wp-* (Web publishing) commands built into the web server. Using the command ?wp-html-rend reliably performs a denial of service attack, by stopping the running Netscape Enterprise service (v4.0) Or the iWS service (v4.1)

Securiteam: [NEWS] Netscape ?wp-html-rend Denial of Service Attack

Publishing needs to be enabled for this to work. Netscape 4.0 SP6 seems to be less susceptible requiring multiple ?wp-html-rend requests to crash. The service has to be restarted manually for the server to function properly again.

?wp-html-rend is one of the wp command's, provided by Netscape's content_mgr.dll. To discover if publishing is enabled without crashing your NT/2000 servers, enter the following url <http://server/publisher> if publishing is enabled a page should appear.

Solution:

The ?wp-html-rend command is not useful in iWS 4.x. You can disable it by using the attached NSAPI SAF. To install the SAF, load the disrend.dll on your system and add the following lines to your obj.conf. The PathCheck line should be the first PathCheck listed.

```
Init fn="load-modules" funcs="disRend" shlib="/disrend.dll" PathCheck
fn="disRend"
```

Attached file:

Netscape has released the file disrend.dll, see:

<<http://knowledgebase.iplanet.com/ikb/kb/articles/7761.html>>
<http://knowledgebase.iplanet.com/ikb/kb/articles/7761.html>

ADDITIONAL INFORMATION

The information has been provided by <<mailto:weld@vulnwatch.org>> Chris Wysopal.

=====

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.

-
- **Previous message:** support@securiteam.com: "[REVS] Creating Arbitrary Shellcode in UNICODE Expanded Strings"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)