

[NT] Multiple OmniHTTPd Issues (CSS)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-08/0099.html>

From: support@securiteam.com

Date: 08/26/02

From: support@securiteam.com

To: list@securiteam.com

Date: Mon, 26 Aug 2002 21:30:42 +0200 (CEST)

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.

Multiple OmniHTTPd Issues (CSS)

SUMMARY

<<http://www.omnicron.ca/httpd/>> OmniHTTPd is a powerful all-purpose industry compliant web server built specifically for the Windows 95/98/NT4 platform. However, product has been found to contain multiple Cross-Site Scripting vulnerabilities allowing an attacker to cause the server to return 3rd-party data as if it were its own.

DETAILS

test.php Cross-Site Scripting Issue:

A vulnerability exists in the test.php script of OmniHTTPd. The script makes a classic coding error -- trusting un-sanitized user input. The query string and cookie values are returned unfiltered. Of most concern, of course, is the query string:

Example:

<http://localhost/test.php?%3CSCRIPT%3Ealert%28document.URL%29%3C%2FSCRIPT%3E=x>

The impact of this vulnerability will vary by site. A production site would most likely *not* have the sample scripts installed, but it would be wise to check.

Securiteam: [NT] Multiple OmniHTTPd Issues (CSS)

test.shtml Cross-Site Scripting Issue:
Test.shtml sample is also vulnerable to a similar issue:

Example:

[http://localhost/test.shtml?%3CSCRIPT%3Ealert\(document.URL\)%3C%2FSCRIPT%3E=x](http://localhost/test.shtml?%3CSCRIPT%3Ealert(document.URL)%3C%2FSCRIPT%3E=x)

Will pop up an alert containing the above URL. Of course, this has other uses (cookie theft, faking sources, etc.)

/cgi-bin/udir.exe Cross-Site Scripting Issue:

This /cgi-bin/udir.exe is vulnerable to a new line injection issue. The vulnerability occurs because the "URL" query parameter (case sensitive) is decoded and placed directly into the response as the "Location" header. If an attacker places URL encoded new lines ("%0D%0A") into the parameter, the headers following the "Location" header, as well as the resultant entity, can be controlled.

Matthew was able to exploit this vulnerability to produce the following output:

```
[Begin Server Response]
HTTP/1.0 302 Redirection
Content-Type: text/html
Date: Sun, 25 Aug 2002 16:36:39 GMT
Location: http://www.yahoo.com/
Server: OmniHTTPd/2.10
```

```
<script>alert(document.URL)</script>
[End Server Response]
```

This will pop up an alert, and then redirect to yahoo.com on browsers that display redirect entities (IE will not work for this)

Matthew was a bit puzzled by the "Server" header between the Location and the entity, but he figured out that OmniHTTPd was inserting the header after CGI processing was complete.

Example:

<http://localhost/cgi-bin/udir.exe?URL=http%3A%2F%2Fwww%2Eyahoo%2Ecom%2F%0D%0A%0D%0A%3CSCRIPT%3Ealert%28document%2EURL%29%3C%2FSCRIPT%3E>

ADDITIONAL INFORMATION

The information has been provided by <mailto:mattmurphy@kc.rr.com>
Matthew Murphy.

=====

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

Securiteam: [NT] Multiple OmniHTTPd Issues (CSS)

=====
=====

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: "[\[NT\] Unsafe Functions in Office Web Components](#)"
 - *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)