

[Full-Disclosure] [GLSA 200411-32] phpBB: Remote command execution

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-11/1204.html>

From: Sune Kloppenborg Jeppesen (jaervosz_at_gentoo.org)

Date: 11/24/04

To: gentoo-announce@gentoo.org

Date: Wed, 24 Nov 2004 09:58:15 +0100

Gentoo Linux Security Advisory GLSA 200411-32

<http://security.gentoo.org/>

Severity: High

Title: phpBB: Remote command execution

Date: November 24, 2004

Bugs: #71681

ID: 200411-32

Synopsis
=====

phpBB contains a vulnerability which allows a remote attacker to execute arbitrary commands with the rights of the web server user.

Background
=====

phpBB is an Open Source bulletin board package.

Affected packages
=====

Package / Vulnerable / Unaffected

1 www-apps/phpbb < 2.0.10 >= 2.0.11

Description

=====

phpBB contains a vulnerability in the highlighting code and several vulnerabilities in the username handling code.

Impact

=====

An attacker can exploit the highlighting vulnerability to access the PHP `exec()` function without restriction, allowing them to run arbitrary commands with the rights of the web server user (for example the apache user). Furthermore, the username handling vulnerability might be abused to execute SQL statements on the phpBB database.

Workaround

=====

There is a one-line patch which will remediate the remote execution vulnerability.

Locate the following block of code in `viewtopic.php`:

```
//
// Was a highlight request part of the URI?
//
$highlight_match = $highlight = "";
if (isset($HTTP_GET_VARS['highlight']))
{
    // Split words and phrases
    $words = explode(' ',
trim(htmlspecialchars(urldecode($HTTP_GET_VARS['highlight']))));

    for($i = 0; $i < sizeof($words); $i++)
    {
```

Replace with the following:

```
//
// Was a highlight request part of the URI?
//
$highlight_match = $highlight = "";
if (isset($HTTP_GET_VARS['highlight']))
{
    // Split words and phrases
    $words = explode(' ',
trim(htmlspecialchars($HTTP_GET_VARS['highlight'])));

    for($i = 0; $i < sizeof($words); $i++)
    {
```

Resolution

=====

All phpBB users should upgrade to the latest version to fix all known vulnerabilities:

```
# emerge --sync
# emerge --ask --oneshot --verbose ">=www-apps/phpbb-2.0.11"
```

References

=====

[1] phpBB.com Announcement
<http://www.phpbb.com/phpBB/viewtopic.php?t=240513>

Availability

=====

This GLSA and any updates to it are available for viewing at the Gentoo Security Website:

<http://security.gentoo.org/glsa/glsa-200411-32.xml>

Concerns?

=====

Security is a primary focus of Gentoo Linux and ensuring the confidentiality and security of our users machines is of utmost importance to us. Any security concerns should be addressed to security@gentoo.org or alternatively, you may file a bug at <http://bugs.gentoo.org>.

License

=====

Copyright 2004 Gentoo Foundation, Inc; referenced text belongs to its owner(s).

The contents of this document are licensed under the Creative Commons – Attribution / Share Alike license.

<http://creativecommons.org/licenses/by-sa/2.0>

Full-Disclosure – We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>

Full-Disclosure: [Full-Disclosure] [GLSA 200411-32] phpBB: Remote command execution

- application/pgp-signature attachment: stored