

[UNIX] Arbitrary File Disclosure and Unlink Vulnerabilities in phpBB

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-02/0107.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 02/24/05

To: list@securiteam.com

Date: 24 Feb 2005 17:04:49 +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>

Arbitrary File Disclosure and Unlink Vulnerabilities in phpBB

SUMMARY

" <<http://www.phpbb.com/>> phpBB is a high powered, fully scalable, and highly customizable Open Source bulletin board package. phpBB has a user-friendly interface, simple and straightforward administration panel, and helpful FAQ. Based on the powerful PHP server language and your choice of MySQL, MS-SQL, PostgreSQL or Access/ODBC database servers, phpBB is the ideal free community solution for all web sites."

Remote exploitation of an input validation vulnerability in the phpBB Group's phpBB2 bulletin board system allows attackers to read/unlink(delete) arbitrary system files under the privileges of the web server.

DETAILS

Vulnerable Systems:

* phpBB version 2.0.11 (prior versions suspected)

Immune Systems:

* phpBB version 2.0.12 (available for download)

<<http://www.phpbb.com/downloads.php>> here)

Arbitrary File Disclosure Vulnerability:

phpBB is an open-source web-based bulletin board system written in PHP. The problem specifically exists due to an input validation error that allows a remote attacker to control the arguments in a call to copy().

When a user requests to upload an avatar, the variable '\$user_avatar_upload' defaults to uploading from a remote URL and the variable '\$avatar_mode' defaults to uploading from the local computer. The variable '\$user_avatar_upload' contains either the remote URL or the temporary server name depending on whether the source of the avatar to upload is local or remote. In the event that both a local and remote upload are requested simultaneously, the temporary upload location is substituted with the remote server name. This will later be copied to the new location. By submitting a local path rather than a URL, an attacker is able to execute an arbitrary copy() command.

An attacker can exploit this input validation condition by selecting an avatar from the local machine that meets the board guidelines and can then fill the "Upload Avatar from a URL:" field with the path to an arbitrary file (ex: /etc/passwd). When the avatar is submitted, the destination image of the submitted avatar will contain the contents of the requested file.

Exploitation of this vulnerability allows remote attackers to view arbitrary system files under the privileges of the underlying web server. An attacker must have, or be able to create an account on the target system. Non-default settings must also be enabled for exploitation to be possible. Upon successful exploitation an attacker may be able to further compromise the system by gleaning system information that would otherwise be inaccessible to the attacker.

Workaround:

Disable remote avatars and remove avatar uploading. This can be done through the phpBB administrative interface under "General Admin -> Configuration -> Avatar Settings". Alternatively, enable the 'open_basedir' PHP security directive to lock file I/O operations to a specific directory.

Arbitrary File Unlink Vulnerability:

Remote exploitation of an input validation vulnerability in the phpBB Group's phpBB2 bulletin board system allows attackers to unlink (delete) arbitrary system files under the privileges of the web server.

phpBB is an open-source web-based bulletin board system written in PHP. The vulnerability specifically exists due to a combination of several flaws that allows a remote attacker to control the arguments in a call to unlink(). The first flaw occurs in the avatar gallery, where a user is permitted to specify part of the directory name for the desired avatar. Directory traversal modifiers (ex: "../") are not properly filtered out,

Securiteam: [UNIX] Arbitrary File Disclosure and Unlink Vulnerabilities in phpBB

allowing a user to break out of the default avatar directory. This issue is realized in lines 68–71 of `usercp_avatar.php`:

```
if ( file_exists(@phpbb_realpath($board_config['avatar_gallery_path']
    . '/' . $avatar_filename)) && ($mode == 'editprofile') )
{
    $return = ", user_avatar = " . str_replace("/", "",
        $avatar_filename) . ", user_avatar_type = " .
        USER_AVATAR_GALLERY;
}
```

Avatar's are then composed with the following code excerpt found in line 90 of `usercp_viewprofile.php`:

```
$avatar_img = ( $board_config['allow_avatar_local'] ) ? '' : "";
```

The abused calls to `unlink()` are made when an avatar is deleted. There is a guard around these functions requiring that the target avatar to unlink exist in the `avatar_path`. This routine is also vulnerable to a directory traversal attack. By issuing a large number of `"/../"` directory traversal modifiers, an attacker is able to delete arbitrary system files. The vulnerable segment of code shown here is from lines 473–478 of `usercp_register.php`:

```
if ( @file_exists(@phpbb_realpath('./' . $board_config['avatar_path']
    . '/' . $userdata['user_avatar'])) )
{
    @unlink(@phpbb_realpath('./' . $board_config['avatar_path'] . '/'
        . $userdata['user_avatar']));
}
```

Exploitation of this vulnerability allows remote attackers to unlink arbitrary system files under the privileges of the underlying web server. An attacker must have or be able to create an account on the target system. Non–default settings must be enabled for exploitation to be possible. An attacker can potentially further compromise the target system by erasing sensitive files such as `.htaccess` files that provide access control rules.

Workaround:

Disable gallery avatars. This can be done through the phpBB administrative interface under "General Admin → Configuration → Avatar Settings".

Disclosure Timeline:

- * 02/09/2005 Initial vendor notification
- * 02/11/2005 Initial vendor response
- * 02/22/2005 Public disclosure

Securiteam: [UNIX] Arbitrary File Disclosure and Unlink Vulnerabilities in phpBB

CVE Information:

File Disclosure:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0258>>

CAN-2005-0258

File Unlink:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0259>>

CAN-2005-0259

ADDITIONAL INFORMATION

The information has been provided by

<<mailto:idlabs-advisories@idefense.com>> iDEFENSE.

The original article can be found at:

<<http://www.idefense.com/application/poi/display?id=205&type=vulnerabilities>>

<http://www.idefense.com/application/poi/display?id=205&type=vulnerabilities>

=====

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.