

[UNIX] phpBB Attachment Mod Directory Traversal HTTP POST Injection

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-12/0118.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 12/28/04

To: list@securiteam.com

Date: 28 Dec 2004 16:59:31 +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>

phpBB Attachment Mod Directory Traversal HTTP POST Injection

SUMMARY

<<http://www.phpBB.org>> 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."

An HTTP POST Injection vulnerability exists in the <<http://opentools.de>> Attachment Mod written by Meik Sievertsen AKA Acyd Burn that enables anyone to traverse directories on the web server.

DETAILS

Vulnerable Systems:

* phpBB's Attachment Module version 2.3.10 and prior

Immune Systems:

* phpBB's Attachment Module version 2.3.11 or newer

Securiteam: [UNIX] phpBB Attachment Mod Directory Traversal HTTP POST Injection

Due to insufficient sanitizing of the filename in the attachment mod user interface, a user can inject a filename via HTTP POST that includes a directory traversal vulnerability: "../.". This injection can be done via the "physical_filename" and/or "real_filename" fields.

Once the database table has a directory traversal filename stored in it, for example: "../.\$newfilename", you can use the download.php file to obtain files stored outside the UPLOAD_DIR location.

Impact:

With this an attacker could be able to add/remove/execute files outside of the UPLOAD_DIR directory.

Proof Of Concept:

- 1) Visit a website that has attachmod installed under phpBB
- 2) Start a new topic, attach a file via the "Add Attachment" input button
- 3) Prior to clicking "Submit", view the page source via your browser's "View Source"
- 4) Modify the <FORM> entry if required to send the POST back to the website
- 5) Modify the two values for the input names "attachment_list[]" and "filename_list[]" from "\$oldfilename" to "../.\$newfilename"
- 6) Save the page, load it in your browser, and click "Submit"

An un-patched attachmod site will now have "../.\$newfilename" in:
\$prefix_attachments_desc.physical_filename
\$prefix_attachments_desc.real_filename

And when a user accesses the file via the attachmod's download.php generated link, instead of serving "\$filename" from the UPLOAD_DIR location, it will serve the user the "../.\$newfilename" if it exists.

Disclosure Timeline:

- Dec 7 2004: Exploit discovered during an audit
- Dec 8 2004: Author was contacted with this advisory
- Dec 9 2004: Author developed a patch. Basic static test of the patch shows success in stopping the exploit
- Dec 12 2004: Author released version 2.3.11 to the public
- Dec 14 2004: Advisory released to the public

ADDITIONAL INFORMATION

The information has been provided by <mailto:zx@castlecops.com> Paul Laudanski.

The original article can be found at:

<<http://castlecops.com/postp393483.html>>
<http://castlecops.com/postp393483.html>

=====

Securiteam: [UNIX] phpBB Attachment Mod Directory Traversal HTTP POST Injection

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.