

[UNIX] Multiple Extensions Vulnerability in phpBB Attachment Mod

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-12/0116.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 12/28/04

To: list@securiteam.com

Date: 28 Dec 2004 16:45:44 +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>

Multiple Extensions Vulnerability in phpBB Attachment Mod

SUMMARY

The <<http://www.opentools.de/>> phpBB Attachment Mod is a "file upload module for phpBB". However, an input validation flaw in phpBB's Attachment Mod allows a malicious attackers to run arbitrary commands with the privileges of the HTTPD process, which is typically run as the nobody user.

DETAILS

Vulnerable Systems:

* phpBB's Attachment Mod version 2.3.10 and prior

Immune Systems:

* phpBB's Attachment Mod version 2.3.11 or newer

phpBB's Attachment Mod doesn't implemented any type of check for multiple extensions of uploaded files, e.g. `attack.php.rar`. Therefore, malicious attackers can upload arbitrary script files (PHP, pl, CGI, etc) to a web server. This is vulnerability is caused by Apache's MIME module (`mod_mime`), which regards `attack.php.rar` as a normal PHP file and execute

Securiteam: [UNIX] Multiple Extensions Vulnerability in phpBB Attachment Mod

the file through mod_php module with the privilege of the HTTPD process.

Disclosure Timeline:

- 2004-12-08 Vulnerability found
- 2004-12-08 Attachment Mod developer notified
- 2004-12-13 Update version released
- 2004-12-15 Official release

ADDITIONAL INFORMATION

The information has been provided by <mailto:advisory@stgsecurity.com>
SSR Team.

=====

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.