

[UNIX] MoniWiki Arbitrary File Uploading

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-12/0042.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 12/16/04

To: list@securiteam.com

Date: 16 Dec 2004 14:04:07 +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>

MoniWiki Arbitrary File Uploading

SUMMARY

<<http://kldp.net/projects/moniwiki/>> MoniWiki is "a wiki web application used by many Korean Linux users. However, an input validation flaw can cause malicious attackers to run arbitrary commands with the privilege of the HTTPD process, which is typically run as the nobody user".

Due to improper testing of incoming files, MoniWiki's files upload mechanism can be used to execute arbitrary code on the remote server (by uploading a PHP file, Perl scripts, etc).

DETAILS

Vulnerable Systems:

* MoniWiki version 1.0.9.2 and prior

MoniWiki doesn't implemented in "UploadFile.php" a check for multiple extensions in the files it receives as uploads (e.g. attack.php.hwp).

Therefore a malicious attacker can upload an arbitrary script files (with the extension of PHP, PL, CGI, etc) to a web server.

This vulnerability allows an attacker to cause the execution of arbitrary code whenever the Apache's MIME module (mod_mime) is in use. As Appache's

Securiteam: [UNIX] MoniWiki Arbitrary File Uploading

MIME module regards attack.php.hwp as a normal PHP file and execute the file through mod_php module with the privilege of the HTTPD process.

Solution:

A patch is available for the UploadFile.php file from:

<http://kldp.net/forum/forum.php?forum_id=2085>

http://kldp.net/forum/forum.php?forum_id=2085

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.