

[UNIX] Multiple Vulnerabilities in PHP (Information Discloser, File Access, Negative Reference, Integer Handling Bug, Buffer Overflow, Directory Traversal, Arbitrary File Upload)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-03/0092.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 03/22/05

To: list@securiteam.com

Date: 22 Mar 2005 10:21:44 +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 Vulnerabilities in PHP (Information Discloser, File Access, Negative Reference, Integer Handling Bug, Buffer Overflow, Directory Traversal, Arbitrary File Upload)

SUMMARY

<<http://www.php.net/>> PHP "is a widely-used general-purpose scripting language that is especially suited for Web development and can be embedded into HTML".

PHP has been found to contain multiple vulnerabilities that allow malicious users to execute arbitrary code on the server side, information traversal, access arbitrary files on the server side, and uploading arbitrary files to the server.

DETAILS

Vulnerable Systems:

* PHP version 4.3.9 and prior

* PHP version 5.0.1 and prior

Immune Systems:

- * PHP version 4.3.10
- * PHP version 5.0.2 or newer

Information Disclosure:

An information disclosure was discovered in the parsing of "GPC" variables in PHP (query strings or cookies, and POST form data). If particular scripts used the values of the GPC variables, portions of the memory space of an HTTPD child process could be revealed to the client.

Arbitrary File Uploading:

An arbitrary file access was discovered in the parsing of "multipart/form-data" forms, used by PHP scripts which allow file uploads. In particular configurations, some scripts could allow a malicious client to upload files to an arbitrary directory where the "apache" user has write access.

Integer Handling Bug:

Multiple integer handling in PHP allow attackers to bypass the safe mode restrictions, cause a denial of service, or execute arbitrary code via a negative offset value to the shmop_write function. An "integer overflow/underflow" in the pack function, or an "integer overflow/underflow" in the unpack function.

Negative Reference:

Flaws including possible information disclosure, double free, and negative reference index array underflow were found in the deserialization code of PHP. PHP applications may use the unserialize function on untrusted user data, which could allow a remote attacker to gain access to memory or potentially execute arbitrary code.

Directory Traversal:

A flaw in the PHP cURL functions allows remote attackers to bypass the open_basedir setting and read arbitrary files via a file: URL argument to the curl_init function.

Buffer Overflow:

A flaw in the exif extension of PHP was found which lead to a stack overflow. An attacker could create a carefully crafted image file in such a way that if parsed by a PHP script using the exif extension it could cause a crash or potentially execute arbitrary code.

CVE Information:

<<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0958>>
CAN-2004-0958
<<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0959>>
CAN-2004-0959
<<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1018>>
CAN-2004-1018
<<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1019>>
CAN-2004-1019

ulnerabilities in PHP (Information Discloser, File Access, Negative Reference, Integer Handeling Bug, Buffer Overflow, Dire

<<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1065>>

CAN-2004-1065

<<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1392>>

CAN-2004-1392

ADDITIONAL INFORMATION

The information has been provided by
<<mailto:marcdeslauriers@videotron.ca>> Marc Deslauriers.

=====

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.