

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

05/07/12

SUBJECT:

An input vulnerability in PHP 5.4.1 Could Allow Remote Code Execution

OVERVIEW:

A vulnerability has been discovered in the PHP 5.4.1 and earlier which could allow an attacker to remotely disclose source code and potentially execute arbitrary code. PHP is a programming language originally designed for use in web-based applications with HTML content. PHP supports a wide variety of platforms and is used by numerous web-based software applications.

Successful exploitation could result in an attacker viewing the PHP source code of an web-based application or website and potentially execute arbitrary code.

SYSTEMS AFFECTED:

PHP versions 5.4.1 and prior

RISK:

Government:

Large and medium government entities: **High**

Small government entities: **High**

Businesses:

Large and medium business entities: **High**

Small business entities: **High**

Home users: N/A

DESCRIPTION:

A vulnerability exists within the PHP implementation of CGI, PHP-CGI that fails to properly escape command line arguments when run under a web context due to a missing validation check.

The Common Gateway Interface (CGI), defined in RFC3875, is a standard method for web server applications to assign web page generation tasks to executable files.

When a URL query string is being passed to a web application or website using PHP-CGI, the special characters space " " and dash "-" are not escaped, allowing command line arguments such as -s, -d or -c to be passed to the PHP-CGI binary. The space character allows an arbitrary number of arguments to be passed within a single query.

Special conditions required for exploitation is a mitigating factor for this vulnerability. At this time, the vulnerability has only been proven to be exploitable via Apache HTTP server with the mod_actions module enabled. Further, the non-default PHP-CGI is required to be installed on the system.

A Metasploit module is publicly available and capable of triggering the vulnerability by delivering a payload which spawns a command shell. This module has been tested and verified by a Trusted Third Party. Tests demonstrated that the module is effective against PHP-CGI 4.5.1 running on Apache HTTP server 2.2.14 and achieves remote code execution.

Websites potentially vulnerable to this issue may be tested with the following URL, which will cause vulnerable systems to display source code: `hxxp://website/index.php?-s`

The PHP Group, maintainers and chief developers of PHP, recommend users running PHP-CGI over Apache to add the following `mod_rewrite` condition and rule to completely mitigate against exploitation:

```
RewriteCond %{QUERY_STRING} ^(%2d|-)[^=]+$ [NC]
RewriteRule ^(.*) $1? [L]
```

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate fixes or patches provided by the PHP Group to vulnerable systems immediately after appropriate testing.
- Apply the principle of Least Privilege to all services.

REFERENCES:

PHP Group:

<http://www.php.net/archive/2012.php#id2012-05-03-1>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1823>

Security Focus:

<http://www.securityfocus.com/bid/53388>