

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.

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>

DATE ISSUED:

06/19/2015

SUBJECT:

Multiple Vulnerabilities in PHP Could Allow Remote Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in PHP which could allow an attacker to 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.

Successfully exploiting these issues may allow remote attackers to execute arbitrary code in the context of a webserver.

THREAT INTELLIGENCE:

There are currently no reports of these vulnerabilities being exploited in the wild. There are known proof-of-concept exploits for these vulnerabilities.

SYSTEM AFFECTED:

- PHP 5.4 prior to 5.4.42
- PHP 5.5 prior to 5.5.26
- PHP 5.6 prior to 5.6.10

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: Low

TECHNICAL SUMMARY:

Multiple remote code execution vulnerabilities were fixed in PHP versions 5.4.42, 5.5.26, and 5.6.10. These vulnerabilities include:

- PCRE Library heap overflow vulnerabilities. A carefully crafted regular expression may allow attackers to overflow heap variables, which could result in code execution. (CVE-2015-2325, CVE-2015-2326)
- OS command injection vulnerability in escapeshellarg() which could result in code execution. (CVE-2015-4642)

- The ftp_genlist() function of the ftp extension is prone to an integer overflow, which may result in remote code execution. (CVE-2015-4643)

Successful exploitation of these vulnerabilities may allow remote attackers to execute arbitrary code in the context of a webserver.

Other Bugs Fixed in the PHP Core for these versions may be found below.

Version 5.4.42

- Bug 69719 - Incorrect handling of paths with NULLs.

Versions 5.5.26

- Bug 69566 - Conditional jump or move depends on uninitialized value in extension trait.
- Bug 69048 - Temp directory is cached during multiple requests.
- Bug 69628 - Complex GLOB_BRACE fails on Windows.
- Bug 69719 - Incorrect handling of paths with NULLs.

Versions 5.6.10

- Bug 69048 - Temp directory is cached during multiple requests.
- Bug 69566 - Conditional jump or move depends on uninitialized value in extension trait.
- Bug 69599 - Strange generator exception variadic crash.
- Bug 69628 - Complex GLOB_BRACE fails on Windows
- Fixed POST data processing slowdown due to small input buffer size on Windows.

RECOMMENDATIONS:

The following actions should be taken:

- Upgrade to the latest version of PHP immediately, after appropriate testing.
- Apply the principle of Least Privilege to all systems and services.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.
- Do not open email attachments from unknown or untrusted sources.
- Limit user account privileges to only those required.

REFERENCES:

PHP:

<http://php.net/ChangeLog-5.php#5.4.42>

<http://php.net/ChangeLog-5.php#5.5.26>

<http://php.net/ChangeLog-5.php#5.6.10>

CVE:

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2325>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2326>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4642>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4643>

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>