

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:

09/08/2015

SUBJECT:

Multiple Vulnerabilities in PHP Could Allow Arbitrary 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 is known proof-of-concept code for these vulnerabilities.

SYSTEM AFFECTED:

- PHP 5.4 prior to 5.4.45
- PHP 5.5 prior to 5.5.29
- PHP 5.6 prior to 5.6.13

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:

PHP has released updates that address multiple vulnerabilities that could allow for arbitrary code execution. These vulnerabilities include:

- Bug 70172 - A vulnerability exists in the unserialize() function when trying to dereference memory that has already been freed.
- Bug 70219 - A vulnerability exists in the php_var_unserialize() function when trying to dereference memory that has already been freed.
- Bug 70345 - A vulnerability exists in the PCRE functions with regard to start and end offsets for subject strings.

- Bug 70365 - A vulnerability exists in the unserialize() function with SplObjectStorage when trying to dereference memory that has already been freed.
- Bug 70366 - A vulnerability exists in the unserialize() function with SplDoublyLinkedList when trying to dereference memory that has already been freed.
- Bug 70388 - A vulnerability exists in the SOAP serialize_function_call() function when trying to validate the input.

Successful exploitation of these vulnerabilities may allow remote attackers to execute arbitrary code in the context of the webserver. Other bugs fixed in the PHP Core for these versions may be found below:

Version 5.6.13

- Bug 69487 – Corrupted data as a result of SAPI failing to write POST data.
- Bug 69900 – fgets() function calls take 100ms.
- Bug 70198 – The Syscall recv doesn't set the errno value on success leading to failed if conditions.

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#5.4.45>

<http://php.net/ChangeLog-5.php#5.5.29>

<http://php.net/ChangeLog-5.php#5.6.13>

TLP: WHITE

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

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