

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/>

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 are known proof-of-concept exploits for this vulnerability.

SYSTEMS AFFECTED:

- PHP 5.4 prior to 5.4.44
- PHP 5.5 prior to 5.5.28
- PHP 5.6 prior to 5.6.12

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 in the context of a webserver. These vulnerabilities include:

- Bug 70068 - A use-after-free vulnerability exists in the unserialization of ArrayObject items.
- Bug 70166 - A use-after-free vulnerability exists in the unserialization of the SPLArrayObject.
- Bug 70168 - A use-after-free vulnerability exists in the unserialization of SplObjectStorage.
- Bug 70169 - A use-after-free vulnerability exists in the unserialization of SplDoublyLinkedList.

Another bug fixed in PHP Phar may be found below:

- Bug 70019 - A vulnerability exists that allows extraction of archived files into the upper level directory.

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#5.4.44>

<http://php.net/ChangeLog-5.php#5.5.28>

<http://php.net/ChangeLog-5.php#5.6.12>

TLP: WHITE

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

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