

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:

07/21/2015

SUBJECT:

Multiple Vulnerabilities in PHP Could Allow Arbitrary Code Execution

OVERVIEW:

Multiple vulnerabilities has 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.

SYSTEM AFFECTED:

- PHP 5.4 prior to 5.4.43
- PHP 5.5 prior to 5.5.27
- PHP 5.6 prior to 5.6.11

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 69737 - A vulnerability exists in the `spl_heap_object_storage()` function when trying to deference memory that has already been freed.
- Bug 69970 - A vulnerability exists in the `spl_recursive_it_move_forward_ex ()` function when trying to deference memory that has already been freed.

Successful exploitation of this vulnerability 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 5.4.43

- Bug 69768—`escapeshell*()` does not handle “!” as a special character.
- Bug 69874 - cannot set empty `additional_headers` for `mail()` function.
- Bug 69669 - `mysqlnd` is vulnerable to BACKRONYM. (CVE-2015-3152)

Versions 5.5.27

- Bug 69768 - `escapeshell*()` does not handle “!” as a special character.
- Bug 69732 - Basic PHP code can induce a segmentation fault.
- Bug 69551 - `parse_ini_file()` function can crash with a segmentation fault.
- Bug 69669 - `mysqlnd` is vulnerable to BACKRONYM. (CVE-2015-3152)

Versions 5.6.11

- Bug 69768 - `escapeshell*()` does not handle “!” as a special character.
- Bug 69732 - Basic PHP code can induce a segmentation fault
- Bug 69551 - `parse_ini_file()` function can crash with a segmentation fault.
- Bug 69874 - cannot set empty `additional_headers` for `mail()` function.
- Bug 69669 - `mysqlnd` is vulnerable to BACKRONYM. (CVE-2015-3152)

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#5.4.43>

<http://php.net/ChangeLog-5.php#5.5.27>

<http://php.net/ChangeLog-5.php#5.6.11>

CVE:

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3152>

TLP: WHITE

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

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