

*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(S) ISSUED:**

4/24/2015

**SUBJECT:**

A vulnerability in PHP could allow for remote code execution

**OVERVIEW:**

A vulnerability has been identified in PHP which could allow for remote code execution. 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 this issue may allow remote attackers to execute arbitrary code in the context of a webserver. Failed attempts will likely result in denial-of-service conditions.

**THREAT INTELLIGENCE:**

There are currently no reports of this vulnerability being exploited in the wild.

**SYSTEM AFFECTED:**

- PHP 5.6 prior to 5.6.8
- PHP 5.5 prior to 5.5.24
- PHP 5.4 prior to 5.4.40

**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:**

A vulnerability has been discovered in PHP versions prior to 5.6.8, 5.5.24, and 5.4.40 which could lead to remote code execution. Specifically, the vulnerability occurs when a maliciously crafted request is submitted to a web server running Apache 2.4 with the apache2handler configuration enabled. When this packet is processed by the application, it results in a segmentation fault in 'sapi/apache2handler/sapi\_apache2.c'. Successful exploitation of this vulnerability could result in remote code execution, allowing an attacker to run code in the context of the user running the affected application, failed attempts may result in denial of service conditions.

**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 systems and services.
- Limit user account privileges to only those required.

**REFERENCES:****PHP:**

<https://bugs.php.net/bug.php?id=69221>

**CVE:**

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3330>

**TLP: WHITE**

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

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