

*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:**

2/10/2015

**SUBJECT:**

A Vulnerability in PHP Could Allow Remote Code Execution

**EXECUTIVE SUMMARY:**

A vulnerability has been discovered in the PHP which could allow an attacker to remotely disclose source code and 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 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 these vulnerabilities being exploited in the wild.

**SYSTEM AFFECTED:**

- PHP versions 5.4.X prior to 5.4.37
- PHP versions 5.5.X prior to 5.5.21
- PHP versions 5.6.X prior to 5.6.5

**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: N/A**

**TECHNICAL SUMMARY:**

A use-after-free vulnerability has been discovered that could result in remote code execution. This vulnerability is due to a user-after-free error in the 'process\_nested\_data()' function of 'ext/standard/var\_unserializer.re' file. This occurs because of improper handling of duplicate keys within the serialized properties of an object.

An attacker may exploit this issue using a specially crafted input passed to the 'unserialized()' method.

This issue is the result of an incomplete fix for CVE-2014-8142 (PHP 'process\_nested\_data()' Function Use After Free Remote Code Execution Vulnerability) in PHP versions 5.4.36, 5.5.20, and 5.6.4

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.

**RECOMMENDATIONS:**

The following actions should be taken:

- Verify no unauthorized modifications occurred to the system before installing patches.
- 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.
- 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:

### Bugzilla:

[https://bugzilla.redhat.com/show\\_bug.cgi?id=1185397](https://bugzilla.redhat.com/show_bug.cgi?id=1185397)

### PHP Group:

<https://bugs.php.net/bug.php?id=68710>

### Security Focus:

<http://www.securityfocus.com/advisories/34780>

### CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0231>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8142>

### TLP: WHITE

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

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