

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:**

01/07/2016

**01/21/2016 - UPDATED**

**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.

**January 21 – UPDATED OVERVIEW:**

**Additional vulnerabilities have been discovered which could allow for remote code execution.**

**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 5.6 prior to 5.6.17
- PHP 5.5 prior to 5.5.31

**January 21 – UPDATED SYSTEM AFFECTED:**

- **PHP 7.0 prior to 7.0.2**

**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:

Prior to 5.6.17 and 5.5.31

- Bug 70661 - A vulnerability exists in the 'zval\_ptr\_dtor()' function of the 'wddx/wddx.c' source file. Exploit of this issue can be performed by sending specially crafted 'recordset'.
- Bug 70741 - A vulnerability exists in the 'php\_wddx\_deserialize\_ex()' function when performing deserialization on string-type 'ZVAL'.

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:

- Bug 66909 (configure fails utf8\_to\_mutf7 test).
- Bug 70958 (Invalid opcode while using ::class as trait method parameter default value).
- Bug 70957 (self::class can not be resolved with reflection for abstract class).
- Bug 70944 (try{ } finally{ }) can create infinite chains of exceptions).
- Bug 61751 (SAPI build problem on AIX: Undefined symbol: php\_register\_internal\_extensions).
- Bug 70755 (fpm\_log.c memory leak and buffer overflow).
- Bug 70976 (Memory Read via gdImageRotateInterpolated Array Index Out of Bounds). (emmanuel dot law at gmail dot com).
- Bug 68077 (LOAD DATA LOCAL INFILE / open\_basedir restriction).
- Bug 70900 (SoapClient systematic out of memory error).
- Bug 70960 (ReflectionFunction for array\_unique returns wrong number of parameters).
- Bug 60052 (Integer returned as a 64bit integer on X64\_86).
- Bug 70728 (Type Confusion Vulnerability in PHP\_to\_XMLRPC\_worker()).

**January 21 – UPDATED TECHNICAL SUMMARY:**

***Multiple heap-based buffer-overflow vulnerabilities occur in 'escapeshellarg' and 'escapeshellcmd' functions of the 'ext/standard/exec.c' file. Successful exploitation could allow for remote code execution. (CVE-2016-1904)***

***Prior to 7.0.2***

- ***Bug 71270 (Heap buffer-overflow in escapeshell functions).***

## **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#5.6.17>

<http://php.net/ChangeLog-5.php#5.5.31>

**January 21 – UPDATED REFERENCES**

**CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1904>

**PHP:**

<http://www.php.net/ChangeLog-7.php#7.0.2>

**TLP: WHITE**

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

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