

*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:**

10/17/2016

**SUBJECT:**

Multiple Vulnerabilities in PHP Could Allow For Arbitrary Code Execution

**OVERVIEW:**

Multiple vulnerabilities have been discovered in PHP, the most severe of which could allow an attacker to execute arbitrary code, with failed exploit attempts potentially leading to denial of service conditions. 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 could allow remote attackers to execute arbitrary code in the context of the affected application. Failed exploitation could result in a denial-of-service condition.

**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.

**SYSTEMS AFFECTED:**

- PHP 7 prior to 7.0.12
- PHP 5 prior to 5.6.27

**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, the most severe of which could allow for arbitrary code execution. These vulnerabilities include:

Prior to 7.0.12

- Bug #73025 - Heap Buffer Overflow in virtual\_popen of zend\_virtual\_cwd.c.

- Bug #72703 - Out of bounds global memory read in BF\_crypt triggered by password\_verify.
- Bug #73058 - crypt broken when salt is 'too' long.
- Bug #69579 - Invalid free in extension trait.
- Bug #73156 - segfault on undefined function.
- Bug #73163 - PHP hangs if error handler throws while accessing undef const in default value.
- Bug #73172 - parse error: Invalid numeric literal.
- Bug #73240 - Write out of bounds at number\_format.
- Bug #73147 - Use After Free in PHP7 unserialize().
- Bug #73189 - Memcpy negative size parameter php\_resolve\_path.
- Bug #73126 - Cannot pass parameter 1 by reference.
- Bug #73091 - Unserializing DateInterval object may lead to \_\_toString invocation.
- Bug #73150 - missing NULL check in dom\_document\_save\_html.
- Bug #72972 - Bad filter for the flags FILTER\_FLAG\_NO\_RES\_RANGE and FILTER\_FLAG\_NO\_PRIV\_RANGE.
- Bug #73054 - default option ignored when object passed to int filter.
- Bug #67325 - imagetruecolorpalette: white is duplicated in palette.
- Bug #50194 - imagettftext broken on transparent background w/o alphablending.
- Bug #73003 - Integer Overflow in gdImageWebpCtx of gd\_webp.c.
- Bug #53504 - imagettfbbox gives incorrect values for bounding box.
- Bug #73157 - imagegd2() ignores 3rd param if 4 are given.
- Bug #73155 - imagegd2() writes wrong chunk sizes on boundaries.
- Bug #73159 - imagegd2(): unrecognized formats may result in corrupted files.
- Bug #73161 - imagecreatefromgd2() may leak memory.
- Bug #73218 - add mitigation for ICU int overflow.
- Bug #66797 - mb\_substr only takes 32 - bit signed integer.
- Bug #66964 - mb\_convert\_variables() cannot detect recursion.
- Bug #72992 - mbstring.internal\_encoding doesn't inherit default\_charset.
- Bug #72489 - PHP Crashes When Modifying Array Containing MySQLi Result Data.
- Bug #72982 - Memory leak in zend\_accel\_blacklist\_update\_regexp() function.
- Bug #73072 - Invalid path SNI\_server\_certs causes segfault.
- Bug #73276 - crash in openssl\_random\_pseudo\_bytes function.
- Bug #73275 - crash in openssl\_encrypt function.
- Bug #73121 - Bundled PCRE doesn't compile because JIT isn't supported on s390.
- Bug #73174 - heap overflow in php\_pcre\_replace\_impl.
- Bug #72414 - Never quote values as raw binary data.
- Bug #67130 - \PDOStatement::nextRowset() should succeed when all rows in current rowset haven't been fetched.
- Bug #72996 - phpdbg\_prompt.c undefined reference to DL\_LOAD.
- Bug #68015 - Session does not report invalid uid for files save handler.
- Bug #73100 - session\_destroy null dereference in ps\_files\_path\_create.
- Bug #73293 - NULL pointer dereference in SimpleXMLElement::asXML().
- Bug #71711 - Soap Server Member variables reference bug.
- Bug #71996 - Using references in arrays doesn't work like expected.
- Bug #73257 - SplObjectStorage unserialize allows use of non - object as key.
- Bug #73258 - SplObjectStorage unserialize allows use of non - object as key.
- Bug #70752 - Depacking with wrong password leaves 0 length files.

Prior to 5.6.27

- Bug #73025 - Heap Buffer Overflow in virtual\_popen of zend\_virtual\_cwd.c
- Bug #73058 - crypt broken when salt is 'too' long
- Bug #72703 - Out of bounds global memory read in BF\_crypt triggered by password\_verify
- Bug #73189 - Memcpy negative size parameter php\_resolve\_path
- Bug #73147 - Use After Free in unserialize()
- Bug #73190 - memcpy negative parameter \_bc\_new\_num\_ex
- Bug #73150 - missing NULL check in dom\_document\_save\_html
- Bug #73284 - heap overflow in php\_ereg\_replace function
- Bug #72972 - Bad filter for the flags FILTER\_FLAG\_NO\_RES\_RANGE and FILTER\_FLAG\_NO\_PRIV\_RANGE
- Bug #67167 - Wrong return value from FILTER\_VALIDATE\_BOOLEAN, FILTER\_NULL\_ON\_FAILURE
- Bug #73054 - default option ignored when object passed to int filter
- Bug #67325 - imagetruecolorpalette: white is duplicated in palette
- Bug #50194 - imagettftext broken on transparent background w/o alphablending
- Bug #73003 - Integer Overflow in gdImageWebpCtx of gd\_webp.c
- Bug #53504 - imagettfbbox gives incorrect values for bounding box
- Bug #73157 - imagegd2() ignores 3rd param if 4 are given
- Bug #73155 - imagegd2() writes wrong chunk sizes on boundaries
- Bug #73159 - imagegd2(): unrecognized formats may result in corrupted files
- Bug #73161 - imagecreatefromgd2() may leak memory
- Bug #73218 - add mitigation for ICU int overflow
- Bug #73208 - integer overflow in imap\_8bit caused heap corruption
- Bug #72994 - mbc\_to\_code() out of bounds read
- Bug #66964 - mb\_convert\_variables() cannot detect recursion
- Bug #72992 - mbstring.internal\_encoding doesn't inherit default\_charset
- Bug #73082 - string length overflow in mb\_encode\_\* function
- Bug #73174 - heap overflow in php\_pcre\_replace\_impl
- Bug #72590 - Opcache restart with kill\_all\_lockers does not work
- Bug #73072 - Invalid path SNI\_server\_certs causes segfault
- Bug #73275 - crash in openssl\_encrypt function
- Bug #73276 - crash in openssl\_random\_pseudo\_bytes function
- Bug #68015 - Session does not report invalid uid for files save handler
- Bug #73100 - session\_destroy null dereference in ps\_files\_path\_create
- Bug #73293 - NULL pointer dereference in SimpleXMLElement::asXML()
- Bug #73073 - CachingIterator null dereference when convert to string
- Bug #73240 - Write out of bounds at number\_format
- Bug #73017 - memory corruption in wordwrap function
- Bug #73069 - readfile() mangles files larger than 2G
- Bug #70752 - Depacking with wrong password leaves 0 length files

Successfully exploiting these issues could allow remote attackers to execute arbitrary code in the context of the affected application. Failed exploitation could result in a denial-of-service condition.

#### **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.

- Verify no unauthorized system modifications have occurred on system before applying patch.
- 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:**

**NOTE: Visiting these links may trigger an IDS signature match for a Possible Encrypted Webshell Download. This is a false positive alert that is matching content on the pages below.**

**PHP:**

<http://php.net/ChangeLog-7.php>

<http://www.php.net/ChangeLog-5.php>

**TLP: WHITE**

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

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