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
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
08/31/2017

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. 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 the most severe of these vulnerabilities could allow for 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.

SYSTEMS AFFECTED:
- PHP 7.0 prior to 7.0.23

RISK:
Government:
- Large and medium government entities: High
- Small government: 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 7.0.23
- Fixed bug #74947 (Segfault in scanner on INF number).
- Fixed bug #74954 (null deref and segfault in zend_generator_resume()).
- Fixed bug #74725 (html_errors=1 breaks unhandled exceptions).
- Fixed bug #74125 (Fixed finding CURL on systems with multiarch support).
- Fixed bug #75002 (Null Pointer Dereference in timelib_time_clone).
Fixed bug #74993 (Wrong reflection on some locale_* functions).
Fixed bug #71606 (Segmentation fault mb_strcut with HTML-ENTITIES encoding).
Fixed bug #62934 (mb_convert_kana() does not convert iteration marks).
Fixed bug #75001 (Wrong reflection on mb_ereg_replace).
Fixed bug #74968 (PHP crashes when calling mysqli_result::fetch_object with an abstract class).
Fixed bug #74991 (include_path has a 4096 char limit in some cases).
Fixed bug #74949 (null pointer dereference in _function_string).
Fixed bug #74833 (SID constant created with wrong module number).
Fixed bug #74950 (nullpointer deref in simplexml_element_getDocNamespaces).
Fixed bug #75049 (spl_autoload_unregister can't handle spl_autoload_functions results).
Fixed bug #74669 (Unserialize ArrayIterator broken).
Fixed bug #75015 (Crash in recursive iterator destructors).
Fixed bug #75075 (unpack with X* causes infinity loop).
Fixed bug #74103 (heap-use-after-free when unserializing invalid array size).
Fixed bug #75054 (A Denial of Service Vulnerability was found when performing deserialization).
Fixed bug #73793 (WDDX uses wrong decimal separator).
Fixed bug #74975 (Incorrect xmlrpc serialization for classes with declared properties).

Successfully exploiting the most severe of these vulnerabilities could allow for 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.
- Verify no unauthorized system modifications have occurred on system before applying patch.
- 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.

REFERENCES:
NOTE: Visiting this link may trigger an IDS signature match for a Possible Encrypted Webshell Download. This is a false positive alert that is matching content on the page below.

PHP:
http://php.net/ChangeLog-7.php#7.0.23

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/