

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:

08/19/2016

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. Successful exploits may allow an attacker to inject and run arbitrary code in the context of the application or obtain sensitive information that may aid in further attacks. Failed exploit attempts may 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.

SYSTEM AFFECTED:

- PHP 5.6 prior to 5.6.25
- PHP 7 prior to 7.0.10

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 5.6.25

- Bug #72837 (integer overflow in bzdecompress caused heap corruption).

- Bug #70436 (Use After Free Vulnerability in unserialize()).
- Bug #72024 (microtime() leaks memory).
- Bug #72581 (previous property undefined in Exception after deserialization).
- Bug #72641 (phpize (on Windows) ignores PHP_PREFIX).
- Bug #72663 (Create an Unexpected Object and Don't Invoke __wakeup() in Deserialization).
- Bug #72681 (PHP Session Data Injection Vulnerability).
- Bug #67976 (cal_days_month() fails for final month of the French calendar).
- Bug #71894 (AddressSanitizer: global-buffer-overflow in zif_cal_from_jd).
- Bug #71144 (Segmentation fault when using cURL with ZTS).
- Bug #71929 (Certification information (CERTINFO) data parsing error).
- Bug #72807 (integer overflow in curl_escape caused heap corruption).
- Bug #66502 (DOM document dangling reference).
- Bug #72838 (Integer overflow lead to heap corruption in sql_regcase).
- Bug #72627 (Memory Leakage In exif_process_IFD_in_TIFF).
- Bug #72735 (Samsung picture thumb not read (zero size)).
- Bug #71745 (FILTER_FLAG_NO_RES_RANGE does not cover whole 127.0.0.0/8 range).
- Bug #72575 (using --allow-to-run-as-root should ignore missing user).
- Bug #43828 (broken transparency of imagearc for truecolor in blendingmode).
- Bug #66555 (Always false condition in ext/gd/libgd/gdkanji.c).
- Bug #68712 (suspicious if-else statements).
- Bug #70315 (500 Server Error but page is fully rendered).
- Bug #72596 (imagetypes function won't advertise WEBP support).
- Bug #72604 (imagearc() ignores thickness for full arcs).
- Bug #72697 (select_colors write out-of-bounds).
- Bug #72709 (imagesetstyle() causes OOB read for empty \$styles).
- Bug #72730 (imagegammacorrect allows arbitrary write access).
- Bug #72691 (mb_ereg_search raises a warning if a match zero-width).
- Bug #72693 (mb_ereg_search increments search position when a match zero-width).
- Bug #72694 (mb_ereg_search_setpos does not accept a string's last position).
- Bug #72710 (`mb_ereg` causes buffer overflow on regexp compile error).
- Bug #72688 (preg_match missing group names in matches).
- Bug #70313 (PDO statement fails to throw exception).
- Bug #72222 (ReflectionClass::export doesn't handle array constants).
- Bug #72708 (php_snmp_parse_oid integer overflow in memory allocation).
- Bug #72330 (CSV fields incorrectly split if escape char followed by UTF chars).
- Bug #72836 (integer overflow in base64_decode).
- Bug #72848 (integer overflow in quoted_printable_encode).
- Bug #72849 (integer overflow in urlencode).
- Bug #72850 (integer overflow in php_uuencode).
- Bug #72716 (initialize buffer before read).
- Bug #41021 (Problems with the ftps wrapper).
- Bug #54431 (opendir() does not work with ftps:// wrapper).
- Bug #72667 (opendir() with ftp:// attempts to open data stream for non-existent directories).
- Bug #72764 (ftps:// opendir wrapper data channel encryption fails with IIS [FTP 7.5](#), 8.5).
- Bug #72771 (ftps:// wrapper is vulnerable to protocol downgrade attack).
- Bug #72122 (IteratorIterator breaks '@' error suppression).

- Bug #72646 (SplFileObject::getCsvControl does not return the escape character).
- Bug #72684 (AppendIterator segfault with closed generator).
- Bug #72142 (WDDX Packet Injection Vulnerability in wddx_serialize_value()).
- Bug #72749 (wddx_deserialize allows illegal memory access) (Stas)
- Bug #72750 (wddx_deserialize null dereference).
- Bug #72790 (wddx_deserialize null dereference with invalid xml).
- Bug #72799 (wddx_deserialize null dereference in php_wddx_pop_element).

Prior to 7.0.10

- Bug #72629 (Caught exception assignment to variables ignores references).
- Bug #72594 (Calling an earlier instance of an included anonymous class fatals).
- Bug #72581 (previous property undefined in Exception after deserialization).
- Bug #72496 (Cannot declare public method with signature incompatible with parent private method).
- Bug #72024 (microtime() leaks memory).
- Bug #71911 (Unable to set --enable-debug on building extensions by phpize on Windows).
- Bug #72641 (phpize (on Windows) ignores PHP_PREFIX).
- Bug #72663 (Create an Unexpected Object and Don't Invoke __wakeup() in Deserialization).
- Bug #72681 (PHP Session Data Injection Vulnerability).
- Bug #72683 (getmxrr broken).
- Bug #72742 (memory allocator fails to realloc small block to large one).
- Bug #72837 (integer overflow in bzdecompress caused heap corruption).
- Bug #67976 (cal_days_month() fails for final month of the French calendar).
- Bug #71894 (AddressSanitizer: global-buffer-overflow in zif_cal_from_jd).
- Bug #72569 (DOTNET/COM array parameters broke in PHP7).
- Bug #71709 (curl_setopt segfault with empty CURLOPT_HTTPHEADER).
- Bug #71929 (CURLINFO_CERTINFO data parsing error).
- Bug #72674 (Heap overflow in curl_escape).
- Bug #66502 (DOM document dangling reference).
- Bug #72735 (Samsung picture thumb not read (zero size)).
- Bug #72627 (Memory Leakage In exif_process_IFD_in_TIFF).
- Bug #71745 (FILTER_FLAG_NO_RES_RANGE does not cover whole 127.0.0.0/8 range).
- Bug #72575 (using --allow-to-run-as-root should ignore missing user).
- Bug #72596 (imagetypes function won't advertise WEBP support).
- Bug #72604 (imagearc() ignores thickness for full arcs).
- Bug #70315 (500 Server Error but page is fully rendered).
- Bug #43828 (broken transparency of imagearc for truecolor in blendingmode).
- Bug #66555 (Always false condition in ext/gd/libgd/gdkanji.c).
- Bug #68712 (suspicious if-else statements).
- Bug #72697 (select_colors write out-of-bounds).
- Bug #72730 (imagegammacorrect allows arbitrary write access).
- Bug #72639 (Segfault when instantiating class that extends IntlCalendar and adds a property).
- Bug #72691 (mb_ereg_search raises a warning if a match zero-width).
- Bug #72693 (mb_ereg_search increments search position when a match zero-width).
- Bug #72694 (mb_ereg_search_setpos does not accept a string's last position).
- Bug #72710 (`mb_ereg` causes buffer overflow on regex compile error).

- Bug #72782 (Heap Overflow due to integer overflows).
- Bug #72590 (Opcache restart with kill_all_lockers does not work).
- Bug #72688 (preg_match missing group names in matches).
- Bug #70313 (PDO statement fails to throw exception).
- Bug #72222 (ReflectionClass::export doesn't handle array constants).
- Bug #72588 (Using global var doesn't work while accessing SimpleXML element).
- Bug #72708 (php_snmp_parse_oid integer overflow in memory allocation).
- Bug #55701 (GlobIterator throws LogicException).
- Bug #72646 (SplFileObject::getCsvControl does not return the escape character).
- Bug #72684 (AppendIterator segfault with closed generator).
- Bug #72668 (Spurious warning when exception is thrown in user defined function).
- Bug #72571 (SQLite3::bindValue, SQLite3::bindParam crash).
- Bug #72622 (array_walk + array_replace_recursive create references from nothing).
- Bug #72152 (base64_decode \$strict fails to detect null byte).
- Bug #72263 (base64_decode skips a character after padding in strict mode).
- Bug #72264 (base64_decode \$strict fails with whitespace between padding).
- Bug #72330 (CSV fields incorrectly split if escape char followed by UTF chars).
- Bug #41021 (Problems with the ftps wrapper).
- Bug #54431 (opendir() does not work with ftps:// wrapper).
- Bug #72667 (opendir() with ftp:// attempts to open data stream for non-existent directories).
- Bug #72771 (ftps:// wrapper is vulnerable to protocol downgrade attack).
- Bug #72647 (xmlrpc_encode() unexpected output after referencing array elements).
- Bug #72564 (boolean always deserialized as "true") (Remi)
- Bug #72142 (WDDX Packet Injection Vulnerability in wddx_serialize_value()).
- Bug #72749 (wddx_deserialize allows illegal memory access) (Stas)
- Bug #72750 (wddx_deserialize null dereference).
- Bug #72790 (wddx_deserialize null dereference with invalid xml).
- Bug #72799 (wddx_deserialize null dereference in php_wddx_pop_element).
- Bug #72660 (NULL Pointer dereference in zend_virtual_cwd).

Successful exploits may allow an attacker to inject and run arbitrary code in the context of the application or obtain sensitive information that may aid in further attacks. Failed exploit attempts may 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://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/>