

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:

11/14/2016

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 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. There is known proof-of-concept code for these vulnerabilities.

SYSTEMS AFFECTED:

- PHP 7 prior to 7.0.13
- PHP 5 prior to 5.6.28

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 7.0.13

- Bug #73350 (Exception::__toString() cause circular references).

- Bug #73181 (parse_str() without a second argument leads to crash).
- Bug #66773 (Autoload with Opcache allows importing conflicting class name to namespace).
- Bug #66862 ((Sub-)Namespaces unexpected behaviour).
- Bug #73337 (try/catch not working with two exceptions inside a same operation).
- Bug #73338 (Exception thrown from error handler causes valgrind warnings (and crashes)).
- Bug #73329 ((Float)"Nano" == NAN).
- Bug #73213 (Integer overflow in imageline() with antialiasing).
- Bug #73272 (imagescale() is not affected by, but affects imagesetinterpolation()).
- Bug #73279 (Integer overflow in gdImageScaleBilinearPalette()).
- Bug #73280 (Stack Buffer Overflow in GD dynamicGetbuf).
- Bug #72482 (Illegal write/read access caused by gdImageAALine overflow).
- Bug #72696 (imagefilltoborder stackoverflow on truecolor images).
- Bug #73418 (Integer Overflow in "_php_imap_mail" leads to crash).
- Bug #71148 (Bind reference overwritten on PHP 7).
- Bug #70776 (Simple SIGINT does not have any effect with -rr).
- Bug #71234 (INI files are loaded even invoked as -n --version).
- Bug #73273 (session_unset() empties values from all variables in which is \$_session stored).
- Bug #73037 (SoapServer reports Bad Request when gzipped).
- Bug #73237 (Nested object in "any" element overwrites other fields).
- Bug #69137 (Peer verification fails when using a proxy with SoapClient).
- Bug #73333 (2147483647 is fetched as string).
- Bug #73203 (passing additional_parameters causes mail to fail).
- Bug #71241 (array_replace_recursive sometimes mutates its parameters).
- Bug #73192 (parse_url return wrong hostname).
- Bug #73331 (NULL Pointer Dereference in WDDX Packet Deserialization with PDORow).

Prior to 5.6.28

- Bug #73337 (try/catch not working with two exceptions inside a same operation).
- Bug #73356 (crash in bzcompress function).
- Bug #73213 (Integer overflow in imageline() with antialiasing).
- Bug #73272 (imagescale() is not affected by, but affects imagesetinterpolation()).
- Bug #73279 (Integer overflow in gdImageScaleBilinearPalette()).
- Bug #73280 (Stack Buffer Overflow in GD dynamicGetbuf).
- Bug #72482 (Illegal write/read access caused by gdImageAALine overflow).
- Bug #72696 (imagefilltoborder stackoverflow on truecolor images).
- Bug #73418 (Integer Overflow in "_php_imap_mail" leads Heap Overflow).
- Bug #73144 (Use-after-free in ArrayObject Deserialization).
- Bug #73037 (SoapServer reports Bad Request when gzipped).
- Bug #73333 (2147483647 is fetched as string).
- Bug #73203 (passing additional_parameters causes mail to fail).
- Bug #73188 (use after free in userspace streams).
- Bug #73192 (parse_url return wrong hostname).
- Bug #73331 (NULL Pointer Dereference in WDDX Packet Deserialization with PDORow)

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.
- 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

Disclosure is not limited. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

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