

*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:**

08/05/2015

**SUBJECT:**

Vulnerability in PCRE Library Could Allow for Arbitrary Code Execution

**OVERVIEW:**

A vulnerability has been discovered in the Perl Compatible Regular Expression (PCRE) library, which could allow for arbitrary code execution. The PCRE library is a set of functions that implement regular expression pattern matching using the same syntax and semantics as Perl 5. Programs that utilize this library include Adobe Flash, Apache, Nginx, PHP, as well as many others.

**THREAT INTELLIGENCE**

There are no reports of this vulnerability being exploited in the wild, however there is a proof of concept available.

**SYSTEM AFFECTED:**

- PCRE version 8.37 and prior

**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: High**

**TECHNICAL SUMMARY:**

A vulnerability has been discovered in the PCRE Library, which could allow for arbitrary code execution. This vulnerability occurs because the library fails to perform adequate boundary-checks on user-supplied data. When the library writes to the compile\_regex function, it writes more than the allocated block size causing a heap buffer overflow.

Successful exploitation of this vulnerability through a specially crafted or vulnerable expression could trigger this issue, resulting in the execution of arbitrary code, in the context of the user running the application, with failed attempts triggering denial-of-service conditions.

**RECOMMENDATIONS:**

The following actions should be taken:

- Upgrade to the latest version of PCRE2 immediately after appropriate testing.
- Apply appropriate patches when available from affected vendors immediately after appropriate testing.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments, especially those from un-trusted sources.

**REFERENCES:**

**Bugzilla:**

[https://bugs.exim.org/show\\_bug.cgi?id=1667](https://bugs.exim.org/show_bug.cgi?id=1667)

**PCRE:**

<http://www.pcre.org/>

**Seclists:**

<http://seclists.org/oss-sec/2015/q3/295>

**TLP: WHITE**

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

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