

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:

Multiple Vulnerabilities in WordPress Content Management System Could Allow for Arbitrary Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in WordPress content management system (CMS), which could allow for arbitrary code execution. WordPress is an open source content management system for websites.

Successful exploitation of these vulnerabilities could allow for arbitrary code to be executed allowing an attacker to steal cookie-based authentication credentials, compromise the affected website, or allow access to or modify data.

THREAT INTELLIGENCE

These vulnerabilities can be exploited using a web browser.

SYSTEM AFFECTED:

- WordPress versions prior to 4.2.4

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:

WordPress has released a security and maintenance release which fixes multiple vulnerabilities in versions prior to 4.2.4. This security and maintenance release addresses the following vulnerabilities:

- Three cross-site scripting vulnerabilities due to its failure to sanitize user-supplied input that could allow for arbitrary code to be executed within a user's browser.
- A SQL-injection vulnerability due to its failure to sanitize user-supplied input that could allow a remote attacker to execute arbitrary SQL commands potentially compromising the website or allowing for data modification(CVE-2015-2213).
- A vulnerability that could allow a timing side-channel attack which could allow an attacker to analyze the time it takes for computations to complete.
- A vulnerability that could allow an attacker to lock a post from being edited resulting in a Denial of Service scenario.

Successful exploitation of these vulnerabilities could allow for arbitrary code to be executed allowing an attacker to steal cookie-based authentication credentials, compromise the affected website, or allow

access to or modify data.

RECOMMENDATIONS:

The following actions should be taken:

- Ensure no unauthorized systems changes have occurred before applying patches.
- Update WordPress CMS to the latest version after appropriate testing.
- Run all software as a non-privileged user to diminish effects of a successful attack.
- Review and follow WordPress hardening guidelines – http://codex.wordpress.org/Hardening_WordPress

REFERENCES:

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2213>

WordPress:

<https://wordpress.org/news/2015/08/wordpress-4-2-4-security-and-maintenance-release/>

TLP: WHITE

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

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