

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:

02/03/2016

SUBJECT:

Multiple Vulnerabilities in WordPress Content Management System Could Allow for Information Disclosure

OVERVIEW:

Multiple vulnerabilities have been discovered in WordPress content management system (CMS), which could allow for information disclosure. WordPress is an open source content management system for websites. Successful exploitation could result in an attacker gaining access to sensitive information from the WordPress server and/or internal network behind the server, including passwords, documents, or photos. An attacker can also utilize the open redirect vulnerability in phishing campaigns to redirect unsuspecting users to a malicious site.

THREAT INTELLIGENCE:

There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEM AFFECTED:

- WordPress versions prior to 4.4.2

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 issued a security and maintenance release which fixes multiple vulnerabilities in versions prior to 4.4.2. This security and maintenance release addresses the following vulnerabilities, as well as 17 bugs found in version 4.4:

- A server side request forgery (SSRF) vulnerability that would allow an attacker access to the server hosting the WordPress installation or the internal network behind the server.
- Open redirection vulnerability that would allow an attacker to send phishing emails containing links to the vulnerable WordPress installation and redirect unsuspecting users to malicious sites.

RECOMMENDATIONS:

The following actions should be taken:

- 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.
- Confirm that the operating system and all other applications on the system running this CMS are updated with the most recent patches.

REFERENCES:

WordPress:

<https://wordpress.org/news/2016/02/wordpress-4-4-2-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/>