

*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:**

04/28/2015

**SUBJECT:**

Vulnerability in WordPress Content Management System Could Allow Remote Code Execution

**OVERVIEW:**

A vulnerability has been discovered in WordPress content management system (CMS), which could allow an attacker to take control of the affected system. WordPress is an open source content management system for websites.

Successful exploitation of this vulnerability could result in an attacker resetting the administrator password or gaining complete control of the WordPress blog. Depending on the privileges gained, an attacker could install extensions; view, change, or delete data; or create new accounts with full user rights.

**THREAT INTELLIGENCE**

This vulnerability can be exploited using a web browser.

**SYSTEM AFFECTED:**

- WordPress versions prior to 4.2.1

**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 identified in WordPress CMS that could allow an attacker to inject malicious code by making a comment on a blog or article post hosted on a vulnerable version of WordPress. If the comment is viewed by a user with administrator privileges, arbitrary code could be executed with the same administrator privileges.

Successful exploitation of this vulnerability could allow the attacker to bypass certain security restrictions, gain unauthorized access, run malicious HTML and script codes, or steal cookie-based authentication credentials.

WordPress has released WordPress 4.2.1, which corrects this issue.

**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](http://codex.wordpress.org/Hardening_WordPress)

**REFERENCES:**

**Security Focus:**

<http://www.securityfocus.com/bid/74334>

**WordPress:**

<https://wordpress.org/news/2015/04/wordpress-4-2-1/>

**TLP: WHITE**

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

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