

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:

02/12/2015

SUBJECT:

WordPress Content Management System Vulnerability

EXECUTIVE SUMMARY:

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

Successful exploitation of the vulnerability could result in an attacker resetting the administrator password and 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:

At this time, CIS has not observed this attack being used in the wild.

SYSTEM AFFECTED:

- All versions of WordPress

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 for an attacker to take control of the blog. Due to a security weakness because of a deficiency of CSPRNG (Cryptographically Secure Pseudo Random Number Generator), an attacker can predict the password reset token of an administrator to reset the administrator password and access sensitive information; deface the site; install extensions; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Update vulnerable systems running WordPress immediately after appropriate testing.
- 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.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

WordPress:

<https://core.trac.wordpress.org/attachment/ticket/28633/28633.3.patch>

Security Focus:

<http://www.securityfocus.com/bid/72589>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6412>

TLP: WHITE

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

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