

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.

DATE(S) ISSUED:

09/12/2013

SUBJECT:

Vulnerability in WordPress Content Management System Could Allow Remote Code Execution

OVERVIEW:

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 this vulnerability could result in an attacker gaining the same privileges of the user running the application. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

- WordPress 3.6.0

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: N/A

DESCRIPTION:

A vulnerability has been identified in WordPress CMS that could allow for Remote Code Execution. This vulnerability occurs because the application fails to sanitize user-supplied data to the 'is_serialized()' function of the 'wp-includes/functions.php' script. Due to the nature of this vulnerability, an attacker would need to create a specially crafted request designed to leverage this issue, and then send the request to the vulnerable application. When the request is processed by the application, the attacker's code is run. This attack requires no user interaction to be successful.

Successful exploitation of this vulnerability could allow the attacker to gain the same user rights as the user running the application. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

WordPress has released WordPress 3.6.1 which corrects this issue.

RECOMMENDATIONS:

The following actions should be taken:

- Update vulnerable systems running WordPress immediately after appropriate testing.
- Confirm that the operating system and all other applications on the system running this CMS are updated with the most recent patches.
- Deploy NIDS to detect and block attacks and anomalous activity such as crafted requests containing suspicious URI sequences.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

WordPress:

http://codex.wordpress.org/Version_3.6.1

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4338>

SecurityFocus:

<http://www.securityfocus.com/bid/62345>