

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 ISSUED:

8/5/2013

SUBJECT:

Joomla CMS is Vulnerable to Arbitrary File Upload

OVERVIEW:

Joomla! is an open source content management system for websites. Joomla! Content Management System (CMS) is prone to a vulnerability that could allow an attacker to upload arbitrary files, which could completely compromise the website running the Joomla! CMS.

Successful exploitation could allow an attacker to control the website; view, change, or delete data; or perform a defacement.

SYSTEMS AFFECTED:

- Joomla! versions prior to 2.5.14 and 3.1.5

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:

Joomla! Content Management System (CMS) is prone to a vulnerability that allows attackers to upload arbitrary files bypassing file type upload restrictions. This is due to the failure of properly validating '.php' file extensions being uploaded. Specifically, this issue affects the

'administrator/components/com_media/helpers/media.php' script. The 'media.php' page is used for managing media files or folders.

An attacker can exploit this vulnerability by crafting a malicious file and uploading it to the web server through the compromised application. Successful exploitation could allow an attacker to control the website; view, change, or delete data; or perform a defacement.

RECOMMENDATIONS:

The following actions should be taken:

- Update vulnerable systems running Joomla! immediately after appropriate testing.
- Confirm that the operating system and all other applications on the system are updated with the most recent patches.
- Unless there is a business need, do not allow for the uploading of files using the website.
- If uploading of files is necessary, consider restricting file permissions to upload to directories that prevent execution of files.
- Deploy NIDS to detect and block attacks and anomalous activity such as requests containing suspicious URI sequences.
- Run all software as a non-privileged user with minimal access rights.

REFERENCES:

Joomla:

<http://developer.joomla.org/security/news/563-20130801-core-unauthorised-uploads>

<http://www.joomla.org/announcements/release-news/5506-joomla-2-5-14-released.html>

<http://www.joomla.org/announcements/release-news/5505-joomla-3-1-5-stable-released.html>

JoomlaCode.org:

http://joomlancode.org/gf/project/joomla/tracker/?action=TrackerItemEdit&tracker_item_id=31626

Securityfocus:

<http://www.securityfocus.com/bid/61582>