

*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:**

12/23/2015

**SUBJECT:**

Multiple vulnerabilities in Joomla Could Allow Arbitrary Code Execution

**OVERVIEW:**

Multiple vulnerabilities have been discovered in Joomla, which could result in remote code execution or SQL injection. Joomla is an open source content management system for websites. This vulnerability can be exploited by an attacker sending a maliciously crafted packet to a vulnerable server.

Successful exploitation of this vulnerability could allow for an attacker to execute arbitrary code in the context of the browser, perform SQL injection, obtain sensitive information, bypass security restrictions, or cause denial-of-service conditions.

**THREAT INTELLIGENCE:**

There are reports of this vulnerability being exploited in the wild.

**SYSTEMS AFFECTED:**

- Joomla versions 1.5 through 3.4.6 (vulnerable to Remote Code Execution)
- Joomla versions 3.0.0 through 3.4.6 (vulnerable to SQL Injection)

**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: Low**

**TECHNICAL SUMMARY:**

A remote code execution vulnerability exists in Joomla versions 1.5 through 3.4.6 when the session deserializer calls `php_var_unserialize()` multiple times (CVE-2015-8566). A SQL injection vulnerability exists in Joomla! CMS versions 3.0.0 through 3.4.6 due to inadequate filtering of request data. These vulnerabilities may be exploited by a remote attacker sending a maliciously crafted packet to a

vulnerable server. Successful exploitation of this vulnerability could allow a remote attacker to execute arbitrary code in the context of the application, obtain sensitive information, bypass security restrictions, or cause denial-of-service conditions. It is worth noting that the vulnerability exists in PHP itself and was remediated in September with the release of versions 5.4.45, 5.5.29, 5.6.13 and all iterations of version 7.

#### **RECOMMENDATIONS:**

The following actions should be taken:

- Apply appropriate patches provided by Joomla to vulnerable Joomla 3.X systems immediately after appropriate testing.
- Apply appropriate hotfixes provided by Joomla to vulnerable Joomla 1.0.0 and 2.3.0 systems immediately after appropriate testing.
- Verify no unauthorized system modifications have occurred on system before applying patch.
- Monitor intrusion detection systems for any signs of anomalous activity.

#### **REFERENCES:**

##### **Joomla:**

<https://www.joomla.org/announcements/release-news/5643-joomla-3-4-7-released.html>

<https://developer.joomla.org/security-centre/639-20151206-core-session-hardening.html>

<https://developer.joomla.org/security-centre/640-20151207-core-sql-injection.html>

##### **PHP:**

<https://bugs.php.net/bug.php?id=70219>

##### **CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8566>

#### **TLP: WHITE**

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

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