

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:

01/26/2016

SUBJECT:

Multiple Vulnerabilities in Magento eCommerce Platform Could Allow Remote Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in the Magento eCommerce platform that could allow remote code execution. Magento Commerce is a company that provides eCommerce solutions to allow merchants to do business transactions over the Internet. Successful exploitation of these vulnerabilities could allow the attacker to perform remote code execution with administrator privileges.

THREAT INTELLIGENCE

There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- Magento Community Edition (CE) prior to 1.9.2.3
- Magento Enterprise Edition (EE) prior to 1.14.2.3
- Magento 2 CE & EE prior to 2.0.1

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: N/A

TECHNICAL SUMMARY:

Multiple vulnerabilities have been discovered in the Magento eCommerce platform that could allow remote code execution. Successful exploitation of these vulnerabilities could grant the attacker administrative access over the eCommerce platform and lead to remote code execution. Details of these vulnerabilities are as follows:

- Multiple stored cross-site scripting vulnerabilities exist that could allow for hijacking the administrator account and lead to remote code execution. (APPSEC-1213, APPSEC-1214, APPSEC-1239, APPSEC-1260, APPSEC-1267, APPSEC-1263, and APPSEC-1276)
- A reflected cross-site scripting vulnerability exists that could allow attackers to execute phishing or spam campaigns. (APPSEC-1255)

- Multiple cross-site forgery vulnerabilities exist that could lead users/administrators to unintentionally delete items from shopping carts or execute server-side actions. (APPSEC-1179, APPSEC-1206, and APPSEC-1212)
- A vulnerability exists that allows CAPTCHA bypassing that could allow brute-force password guessing and/or increase the risk of spam. (APPSEC-1283)
- Multiple information leakage vulnerabilities exist that could allow for leakage of sensitive customer data. (APPSEC-1171, APPSEC-1247, and APPSEC-1270)
- A vulnerability exists that allows any user to edit or delete product reviews. (APPSEC-1268)
- An SQL injection vulnerability exists that could lead the attacker to download sensitive parts of the Magento database. (APPSEC-1294)

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate updates provided by Magento Commerce to vulnerable systems, immediately after appropriate testing.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Review log files to determine if the identified vulnerabilities were exploited, and remediate per your security policy and procedures.

REFERENCES:

Magento Commerce:

<https://magento.com/security/patches/supee-7405>

<https://magento.com/security/patches/magento-201-security-update>

Sophos:

<https://nakedsecurity.sophos.com/2016/01/25/critical-xss-flaws-in-magento-leave-millions-of-ecommerce-sites-at-risk/>

TLP: WHITE

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

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