DefenseCode

Magento Multiple Stored Cross-Site Scripting Vulnerabilities

Magento Multiple Stored Cross Site Scripting Vulnerabilities	
Advisory ID:	**DC-2018-03-002**
Software:	**Magento Open Source**
Software Language:	**PHP**
Version:	**Magento 2.0 prior to 2.0.18**
Vendor Status:	**Vendor contacted / Fixed**
Release Date:	**06/03/2018**
Risk:	**Medium**

1. General Overview

During the security audit of Magento Open Source 2 multiple medium risk stored cross-site scripting vulnerabilities were discovered that could lead to administrator account takeover, putting the website customers and their payment information at risk.

2. Software Overview

Magento is an ecommerce platform built on open source technology which provides online merchants with a flexible shopping cart system, as well as control over the look, content and functionality of their online store. Magento offers powerful marketing, search engine optimization, and catalog-management tools. It is a leading enterprise-class eCommerce platform, empowering over 200,000 online retailers.

Homepage:
http://www.magento.com

3. Vulnerability Description

During the security analysis of Magento Open Source 2 prior to 2.0.18 it was discovered that the application returns unescaped and unsanitized user/customer controlled input on direct requests to several application URLs.

User/customer controlled information such as customer first and last name, street address, city, company, shipping and billing information are unsanitized and unescaped in an output resulted from a direct request to the following url:

```
http://website.com/admin/mui/index/render/?namespace=customer_listing&isAjax=true
```

User/customer first and last name information is unsanitized and unescaped in an output resulted from a direct request to the following urls:

```
http://website.com/admin/mui/index/render/?namespace=customer_online_grid&isAjax=
true
```

```
http://website.com/admin/mui/index/render/?namespace=sales_order_invoice_grid&isAjax=true
```

```
http://website.com/admin/mui/index/render/?namespace=sales_order_grid&isAjax=true
```

The application will return a text/html response with a json-formatted content. All aforementioned user-controlled input is prone to stored cross-site scripting.

The prerequisite for this attack is that the Add Secret Key to URLs option is disabled. Secret keys are an additional anti-CSRF measure in Magento, with form keys being the primary measure (that can not be disabled). In a team setting this option is often disabled in order to be able to to pass admin links to coleagues, tickets, chat, etc.

4. Solution

Vendor fixed the reported security issues and released a new version. All users are strongly advised to update to the latest available version.

5. Credits

Discovered by Bosko Stankovic (bosko@defensecode.com).

6. Disclosure Timeline

19/04/2017	**Vendor contacted through Bugcrowd platform**
19/04/2017	**Vendor responded**
28/02/2018	**Vulnerability fixed**
06/03/2018	**Advisory released**

7. About DefenseCode

DefenseCode L.L.C. delivers products and services designed to analyze and test web, desktop and mobile applications for security vulnerabilities.

DefenseCode ThunderScan is a SAST (Static Application Security Testing, WhiteBox Testing) solution for performing extensive security audits of application source code. ThunderScan performs fast and accurate analyses of large and complex source code projects delivering precise results and low false positive rate.

DefenseCode WebScanner is a DAST (Dynamic Application Security Testing, BlackBox Testing) solution for comprehensive security audits of active web applications. WebScanner will test a website's security by carrying out a large number of attacks using the most advanced techniques, just as a real attacker would.

Subscribe for free software trial on our website http://www.defensecode.com

E-mail: defensecode[at]defensecode.com

Website: http://www.defensecode.com
Twitter: https://twitter.com/DefenseCode/