DefenseCode

Magento Stored Cross-Site Scripting – Downloadable Products

Magento Stored Cross-Site Scripting – Downloadable Products	
Advisory ID:	**DC-2018-03-003**
Software:	**Magento Open Source**
Software Language:	**PHP**
Version:	**Magento 2.0 prior to 2.0.18, Magento 2.1 prior to 2.1.12, Magento 2.2 prior to 2.2.3**
Vendor Status:	**Vendor contacted / Fixed**
Release Date:	**06/03/2018**
Risk:	**Medium**

1. General Overview

During the security audit of Magento Open Source 2 a stored cross-site scripting vulnerability was discovered that could lead to administrator account takeover by a lower privileged administrator, 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 it was discovered that a lower privileged admin with access to Products editing can upload a file for a downloadable product using a random extension (ex. .aaa). Extensions like .html or .php are disallowed but if the content of the file is HTML the application will serve the file as such as there is no content disposition header set to force the download. The attacker can then use the link by enticing the higher privileged admin to open it.

Unlike a typical XSS which is often limited by length and payload type, this gives an attacker a whole HTML file to work with.

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

10/11/2017	**Vendor contacted**
15/11/2017	**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/