DefenseCode

DefenseCode ThunderScan SAST Advisory

WordPress Tracking Code Manager Plugin Cross-Site Scripting (XSS) and Denial of Service (DoS) Vulnerabilities

WordPress Tracking Code Manager plugin – Cross-Site Scripting (XSS) and Denial of Service (DoS) Vulnerabilities	
Advisory ID:	**DC-2017-01-020**
Software:	**WordPress Tracking Code Manager Plugin**
Software Language:	**PHP**
Version:	**1.11.1 and below**
Vendor Status:	**Vendor contacted**
Release Date:	**20170510**
Risk:	**Medium**

1. General Overview

During the security audit, multiple security vulnerabilities were discovered in WordPress Tracking Code Manager plugin using DefenseCode ThunderScan application source code security analysis platform.

More information about ThunderScan is available at URL:
http://www.defensecode.com

2. Software Overview

According to the developers, Tracking Code Manager is a plugin to manage all your tracking code and conversion pixels, simply. Compatible with Facebook Ads, Google Adwords, WooCommerce, Easy Digital Downloads, WP eCommerce.

It has more than 40,000 downloads on wordpress.org.

Homepage:
https://wordpress.org/plugins/tracking-code-manager/

3. Vulnerability Description

During the security analysis, ThunderScan discovered Cross-Site Scripting and remote Denial of Service vulnerabilities in Tracking Code Manager plugin. Denial of Service requires only one visit to a specific URL and whole WordPress becomes completely unresponsive until restart. DoS is based upon the ability of the user to select and call a function of it's choice (while safisfying specific conditions). By making a recursive call to the function that handles the request (tcmp_do_action()) DoS can easily be accomplished.

Both vulnerabilities can be found in the settings section of the plugin, and can be remotely triggered due to missing nonce token and validation. Since the DoS vulnerability relies on GET requests, is missing the nonce token, the vulnerability is also directly exposed to attack vectors such as Cross Site request forgery (CSRF).

DoS vulnerability was confirmed on windows OS.

3.1 Cross-Site Scripting	
URL Parameter:	**tcmp_action**
Sample URL:	http://vulnerablesite.com/wp-admin/options-general.php?page=tracking-code-manager&tab=editor&**tcmp_action=<script>alert(1)</script>**

3.2 Denial of Service	
URL Parameter:	**tcmp_action**
Function:	**tcmp_do_action()**
Sample URL:	http://vulnerablesite.com/wp-admin/options-general.php?page=tracking-code-manager&tab=editor&**tcmp_action=do_action**

4. Solution

Vendor should resolve the security issues in next release. All users are strongly advised to update WordPress Tracking Code Manager plugin to the latest available version as soon as the vendor releases an update.

5. Credits

Discovered by Neven Biruski with DefenseCode ThunderScan source code security analyzer.

6. Disclosure Timeline

04/04/2017	**Vendor contacted**
07/04/2017	**Vendor responded: *"We will fix it in the next update."***
09/05/2017	**Advisory released to the public**

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/