DefenseCode

DefenseCode ThunderScan SAST Advisory

WordPress AffiliateWP Plugin Security Vulnerability

AffiliateWP – Cross-site Scripting (XSS) Security Vulnerability	
Advisory ID:	**DC-2017-05-005**
Software:	**AffiliateWP**
Software Language:	**PHP**
Version:	**2.0.8 and below (taken from the official GitHub repo)**
Vendor Status:	**Vendor contacted, update released**
Release Date:	**2017/05/24**
Risk:	**Medium**

1. General Overview

During the security audit of AffiliateWP plugin for WordPress CMS, security vulnerability was discovered 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 plugin developers, AffiliateWP is an easy-to-use, reliable WordPress plugin that gives you the affiliate marketing tools you need to grow your business and make more money. In 2016 it surpassed $500,000 in annual revenue:
https://pippinsplugins.com/2016-in-review/

Homepage:
https://affiliatewp.com
https://github.com/AffiliateWP/AffiliateWP

3. Vulnerability Description

During the security analysis, ThunderScan discovered Cross-Site Scripting vulnerability in AffiliateWP WordPress plugin.

The Cross-Site Scripting vulnerability can enable the attacker to construct the URL that contains malicious JavaScript code. If the administrator of the site makes a request to such an URL, the attacker's code will be executed, with unrestricted access to the WordPress site in question. The attacker can entice the administrator to visit the URL in various ways, including sending the URL by email, posting it as a part of the comment on the vulnerable site or another forum.

3.1 Cross-Site Scripting	
Vulnerable Function:	**Echo**
Vulnerable Variable:	**$_REQUEST['filter_from']**

Vulnerable URL:

```
http://vulnerablesite.com//wp-admin/admin.php?page=affiliate-wp-
referrals&filter_from=%27%3C%2Fscript%3E%3Cscript%3Ealert%2842%29%3C%2Fscript%3E
```

File: AffiliateWP-master\includes\admin\referrals\class-list-table.php

```
571 $from = ! empty( $_REQUEST['filter_from'] ) ? $_REQUEST['filter_from'] : '';
...
574 echo "<input type='text' class='affwp-datepicker' autocomplete='off' name='filter_from'
placeholder='" . __( 'From - mm/dd/yyyy', 'affiliate-wp' ) . "' value='" . $from . "'/>";
```

4. Solution

Vendor resolved the security issues after we reported the vulnerability. All users are strongly advised to update WordPress AffiliateWP plugin to the latest available version.

5. Credits

Discovered with DefenseCode ThunderScan Source Code Security Analyzer by Neven Biruski.

6. Disclosure Timeline

2017/05/16	**Vendor contacted**
2017/05/16	**Vendor responded**
2017/05/17	**Update released**
2017/05/24	**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/