DefenseCode

DefenseCode ThunderScan SAST Advisory

WordPress AccessPress Social Icons Plugin
Multiple SQL injection Security Vulnerabilities

WordPress AccessPress Social Icons Plugin - Multiple SQL injection Security Vulnerabilities	
Advisory ID:	**DC-2017-03-005**
Software:	**WordPress AccessPress Social Icons plugin**
Software Language:	**PHP**
Version:	**1.6.6 and below**
Vendor Status:	**Vendor contacted**
Release Date:	**20170419**
Risk:	**Medium**

1. General Overview

During the security audit of AccessPress Social Icons plugin for WordPress CMS, multiple security vulnerabilities were 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, AccessPress Social Icons, allows you to create various social icons and link your social profiles from your website. You can create, customize and build the beautiful icons for your social media profiles on your own.

It has more than 80,000 downloads on wordpress.org.

Homepage:
https://wordpress.org/plugins/accesspress-social-icons/
https://accesspressthemes.com/wordpress-plugins/accesspress-social-icons/

3. Vulnerability Description

During the security analysis, ThunderScan discovered SQL injection vulnerabilities in AccessPress Social Icons WordPress plugin. The easiest way to reproduce the vulnerability is to visit the provided URL while being logged in as administrator or another user that is authorized to access the plugin settings page. Any user with such privileges can obtain the valid _wpnonce value by previously visiting the settings page. Users that do not have full administrative privileges could abuse the database access the vulnerability provides to either escalate their privileges or obtain and modify database contents they were not supposed to be able to.

3.1 SQL injection	
Function:	**$wpdb->get_results**
Variable:	**$_GET['si_id']**

Sample URL:

```
http://www.vulnerablesite.com/wp-admin/admin-
post.php?action=aps_copy_action&si_id=1%20AND%20SLEEP(5)&_wpnonce=8945828dex
```

File: accesspress-social-icons\inc\backend\copy-icon-set.php

```
4   $si_id = sanitize_text_field($_GET['si_id']);
...
6   $icon_sets = $wpdb->get_results("SELECT * FROM $table_name where si_id = $si_id");
```

3.2 SQL injection	
Function:	**$wpdb->get_results**
Variable:	**$_GET['si_id']**

Sample URL:

```
http://www.vulnerablesite.com/wp-admin/admin-
post.php?action=aps_copy_action&si_id=1%20AND%20SLEEP(5)&_wpnonce=8945828dex
```

File: accesspress-social-icons\inc\backend\edit-icon-set.php

```
4   $si_id = sanitize_text_field($_GET['si_id']);
...
6   $icon_sets = $wpdb->get_results("SELECT * FROM $table_name where si_id = $si_id");
```

4. Solution

Vendor did not respond to our repeated attempts to send this advisory. All users are strongly advised to update WordPress AccessPress Social Icons plugin to the latest available version.

5. Credits

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

6. Disclosure Timeline

03/24/2017	**Vendor contacted**
04/12/2017	**Vendor contacted**
04/13/2017	**Vendor contacted**
04/19/2017	**Still no response. Advisory released to the public**

7. About DefenseCode ThunderScan

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/