# DefenseCode

## DefenseCode ThunderScan SAST Advisory

## WordPress Facebook Plugin
## SQL Injection Vulnerability

| WordPress Facebook Plugin – SQL Injection Vulnerability | |
|---|---|
| Advisory ID: | **DC-2017-04-011** |
| Software: | **WordPress Facebook Plugin** |
| Software Language: | **PHP** |
| Version: | **1.0.13 and below** |
| Vendor Status: | **Vendor contacted, vulnerability confirmed** |
| Release Date: | **20170502** |
| Risk: | **High** |

## 1. General Overview

During the security audit, multiple security vulnerabilities were discovered in WordPress Facebook 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 plugin developers, WordPress Facebook is a well-equipped tool to integrate your website with Facebook. The product package contains a large number of widgets and plugins to make your website more social. Using it you will be able to add not only Like/Share and Registration buttons, but also Facepile, Facebook commenting box and etc.

It has more than 10,000 downloads on wordpress.org.

Homepage:

https://wordpress.org/plugins/spider-facebook/
http://web-dorado.com/products/wordpress-facebook.html

## 3. Vulnerability Description

During the security analysis, ThunderScan discovered SQL injection vulnerability in Facebook 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. Users that to 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.

Due to missing nonce token, the vulnerability is also wide open to Cross site request forgery (CSRF) attacks – authors of any webpage the administrator visits while being logged into the vulnerable WordPress instance can enable the attacker to take full control of the WordPress database.

The attacker can entice the administrator to visit such a web page in various ways, including sending the URL by email, posting it as a part of the comment on the vulnerable site or another forum, causing the administrator's browser to execute the JavaScript found there, cause a POST request to the vulnerable plugin, and freely abuse the SQL injection vulnerability.

| 3.1 SQL injection | |
|---|---|
| Function: | **$wpdb->get_results($query)** |
| Variable: | **$_POST['order_by']** |

Vulnerable URL:

```
http://vulnerablesite.com/wp-admin/admin.php?page=Spider_Facebook_manage
```

Vulnerable Body:

```
search_events_by_title=&page_number=1&serch_or_not=&asc_or_desc=1&order_by=type AND (SELECT
* FROM (SELECT(SLEEP(5)))DefenseCode)
```

File: spider-facebook\facebook_manager.php

```
25  $sort["sortid_by"]=$_POST['order_by'];
...
30  $order="ORDER BY ".sanitize_text_field($sort["sortid_by"])." ASC";
...
36  $order="ORDER BY ".sanitize_text_field($sort["sortid_by"])." DESC";
...
73  $query = "SELECT * FROM ".$wpdb->prefix."spiderfacebook_params".$where." ". $order." "."
LIMIT ".$limit.",20";
74  $rows = $wpdb->get_results($query);
```

## 4. Solution

Vendor resolved the security issues in one of the subsequent releases. All users are strongly advised to update WordPress Facebook plugin to the latest available version. Version 1.0.14 no longer seems to be vulnerable.

# 5. Credits

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

# 6. Disclosure Timeline

| 20170404 | **Vendor contacted** |
|----------|----------------------|
| 20170405 | **Vendor responded:** *"Thanks for noticing and told us about this, we will take into account and will fix the issues with upcoming update."* |
| ? | **Update released** |
| 20170502 | **Latest plugin version tested. Vulnerability seems fixed. 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/