DefenseCode ThunderScan SAST Advisory

WordPress Clean Up Optimizer Plugin
SQL injection Security Vulnerability

WordPress Clean Up Optimizer Plugin – SQL injection Security Vulnerability	
Advisory ID:	**DC-2017-12-004**
Software:	**WordPress Clean Up Optimizer plugin**
Software Language:	**PHP**
Version:	**4.0.0 and below**
Vendor Status:	**Vendor contacted, update released**
Release Date:	**2017/12/13**
Risk:	**High**

1. General Overview

During the security audit of Clean Up Optimizer 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, Clean Up Optimizer is an optimizes your WordPress as well as clean up the obsolete data from database. You can schedule the process of Cleaning, Optimizing, Deleting and Repairing the database tables without going to phpMyAdmin.

Homepage:
https://wordpress.org/plugins/wp-clean-up-optimizer/
http://beta.tech-banker.com/

According to wordpress.org, it has more than 7,000 active installs.

3. Vulnerability Description

During the security analysis, ThunderScan discovered SQL injection vulnerability in Clean Up Optimizer 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 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 the missing nonce token, the vulnerable code is also directly exposed to attack vectors such as Cross Site request forgery (CSRF).

3.1 SQL injection	
Vulnerable Function:	**$wpdb->get_results**
Vulnerable Variable:	**$_REQUEST["table_name"]**

Vulnerable URL:

```
http://vulnerablesite.com/wp-
admin/admin.php?page=cpo_database_view_records&table_name=wp3_wsd_plugin_alerts WHERE
123=123 AND 456=456–DCDC
```

File: wp-clean-up-optimizer\includes\queries.php

```
$table_name_database = isset($_REQUEST["table_name"]) ?
esc_attr($_REQUEST["table_name"]) : "";
...
"SELECT * FROM $table_name_database"
...
"SHOW columns FROM $table_name_database"
```

4. Solution

After the vulnerability was reported the vendor resolved the security issues. All users are strongly advised to update WordPress Clean Up Optimizer plugin to the latest available version.

5. Credits

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

6. Disclosure Timeline

2017/04/04	**Vendor contacted**
2017/04/10	**Vendor responded**
2017/04/10	**Update released**
2017/12/13	**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/