
DefenseCode ThunderScan SAST Advisory

# WordPress Dbox 3D Slider Lite Plugin
# Multiple SQL injection Security Vulnerabilities

| WordPress Dbox 3D Slider Lite Plugin – Multiple SQL injection Security Vulnerabilities | |
|---|---|
| Advisory ID: | **DC-2017-01-003** |
| Software: | **WordPress Dbox 3D Slider Lite plugin** |
| Software Language: | **PHP** |
| Version: | **1.2.2 and below** |
| Vendor Status: | **Vendor contacted** |
| Release Date: | **2018/01/10** |
| Risk: | **Medium** |

## 1. General Overview

During the security audit of Dbox 3D Slider Lite plugin for WordPress CMS, multiple 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, Dbox 3D Slider Lite plugin for WordPress enables users to embed 3D Responsive Slider of Media Library Images, Recent Posts, Category Posts and Custom Post Types.

Homepage:
https://wordpress.org/plugins/dbox-slider-lite/
http://slidervilla.com/dbox-lite/

## 3. Vulnerability Description

During the security analysis, ThunderScan discovered SQL injection vulnerabilities in Dbox 3D Slider Lite WordPress plugin.

The easiest way to reproduce the vulnerabilities is to modify the POST request for the slider rename or reorder and append parts of the SQL query to the current_slider_id parameter, the result being something like "current_slider_id=1 AND SLEEP(5)". Users that do not have full administrative privileges could abuse the database access the vulnerabilities provide 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: | **$wpdb->query()** |
| Vulnerable Variable: | **$_POST['current_slider_id'];** |

Vulnerable URL:

http://vulnerablesite.com/wp-admin/admin.php?page=dboxlite-slider-admin

File: dbox-slider-lite\settings\sliders.php

```
66 $slider_id=$_POST['current_slider_id'];
...
70 $sql = 'UPDATE '.$slider_meta.' SET slider_name="'.$slider_name.'" WHERE
slider_id='.$slider_id;
71 $wpdb->query($sql);
```

| 3.2 SQL injection | |
|---|---|
| Vulnerable Function: | **$wpdb->query()** |
| Vulnerable Variable: | **$_POST['current_slider_id'];** |

Vulnerable URL:

http://vulnerablesite.com/wp-admin/admin.php?page=dboxlite-slider-admin

File: dbox-slider-lite\settings\sliders.php

```
55 $slider_id=$_POST['current_slider_id'];
...
58 $sql = 'UPDATE '.$table_name.' SET slide_order='.$i.' WHERE post_id='.$slide_order.' and
slider_id='.$slider_id;
59 $wpdb->query($sql);
```

## 4. Solution

All users are strongly advised to update WordPress Dbox 3D Slider Lite plugin to the latest available when the vendor releases an update that fixes the vulnerabilities.

## 5. Credits

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

## 6. Disclosure Timeline

| | |
|---|---|
| 2016/11/11 | **Vulnerabilities discovered** |
| 2017/03/31 | **Vendor contacted** |
| 2017/04/28 | **Vendor contacted** |
| 2017/05/08 | **Vendor responded** |
| 2018/01/10 | **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/