

DefenseCode



DefenseCode ThunderScan SAST Advisory

WordPress Smooth Slider Plugin SQL injection Security Vulnerability

WordPress Smooth Slider Plugin – SQL injection Security Vulnerability	
Advisory ID:	DC-2018-01-004
Software:	WordPress Smooth Slider plugin
Software Language:	PHP
Version:	2.8.6 and below
Vendor Status:	Vendor contacted, update released
Release Date:	2018/01/10
Risk:	Medium

1. General Overview

During the security audit of Smooth Slider 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, Smooth Slider is a free WordPress slider plugin to create image slider, post slider, content slider, video slideshow with responsive design.

According to wordpress.org, it has more than 20 000 active installs.

Homepage:

<https://wordpress.org/plugins/smooth-slider/>

<http://slidervilla.com/smooth-slider/>

3. Vulnerability Description

During the security analysis, ThunderScan discovered SQL injection vulnerability in Smooth Slider 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_var()`**

Vulnerable Variable: **`$_GET['trid']`**

Vulnerable URL:

```
http://vulnerablesite.com/wp-admin/post.php?post=1&action=edit&source_lang=1&trid=22 OR SLEEP(5)
```

File: smooth-slider\smooth-slider.php

```
470     $id = $wpdb->get_var( "SELECT element_id FROM {$wpdb->prefix}icl_translations WHERE  
trid=" . $_GET['trid'] . " AND language_code='" . $_GET['source_lang'] . "' );
```

4. Solution

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

5. Credits

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

6. Disclosure Timeline

2016/11/11	Vulnerability 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](mailto:defensecode[at]defensecode.com)

Website: <http://www.defensecode.com>

Twitter: <https://twitter.com/DefenseCode/>