

DefenseCode



DefenseCode ThunderScan SAST Advisory

WordPress Snazzy Maps Plugin Multiple XSS Security Vulnerabilities

WordPress Snazzy Maps Plugin – Multiple XSS Security Vulnerabilities	
Advisory ID:	DC-2018-05-006
Software:	WordPress Snazzy Maps plugin
Software Language:	PHP
Version:	1.1.3 and below
Vendor Status:	Vendor contacted, no response
Release Date:	2018/07/24
Risk:	Medium

1. General Overview

During the security audit of Snazzy Maps plugin for WordPress CMS, multiple Cross-Site Scripting (XSS) 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, Snazzy Maps can apply styles to your Google Maps with the official Snazzy Maps WordPress plugin.

According to wordpress.org, it has more than 60,000 active installs.

Homepage:

<https://wordpress.org/plugins/snazzy-maps/>

3. Vulnerability Description

During the security analysis, ThunderScan discovered multiple Cross-Site Scripting vulnerabilities in Snazzy Maps WordPress plugin.

The Cross-Site Scripting vulnerability can enable the attacker to construct the URL that contains malicious JavaScript code. If the administrator of the site makes a request to such an URL, the attacker's code will be executed, with unrestricted access to the WordPress site in question. The attacker can entice the administrator to visit the URL in various ways, including sending the URL by email, posting it as a part of the comment on the vulnerable site or another forum.

3.1 Cross-Site Scripting

Vulnerable Function: **echo()**
Vulnerable Variable: **\$_GET['text']**

Vulnerable URL:

```
http://vulnerablesite.com/wp-admin/themes.php?page=snazzy_maps&tab=1&text="></script><script>alert(42)</script>
```

File: snazzy-maps/admin/explore.php

```
28 $text = isset($_GET['text']) ? $_GET['text'] : '';  
...  
34 <input name="text" type="text" placeholder="Search..." value="<?php echo $text ?>"/>
```

3.2 Cross-Site Scripting

Vulnerable Function: **echo()**
Vulnerable Variable: **\$_GET['tab']**

Vulnerable URL:

```
http://vulnerablesite.com/wp-admin/themes.php?page=snazzy_maps&tab=1"></script><script>alert(42)</script>
```

File: snazzy-maps/admin/index.php

```
69 $active_tab = isset($_GET['tab']) ? $_GET['tab'] : '0';  
...  
98 <a href="?page=snazzy_maps&tab=<?php echo $active_tab; ?>&welcome=hide" class="welcome-panel-close">Dismiss</a>
```

4. Solution

All users are strongly advised to update WordPress Snazzy Maps 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

2018/05/21	Vulnerabilities discovered
2018/05/21	Vendor contacted
2018/07/24	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/>