DefenseCode

DefenseCode ThunderScan SAST Advisory

WordPress Tribulant Slideshow Gallery Plugin Cross-Site Scripting Vulnerabilities

WordPress Tribulant Slideshow Gallery Plugin - Cross-Site Scripting Vulnerabilities	
Advisory ID:	**DC-2017-01-014**
Software:	**WordPress Tribulant Slideshow Gallery plugin**
Software Language:	**PHP**
Version:	**1.6.4 and below**
Vendor Status:	**Vendor contacted, fix released**
Release Date:	**20170410**
Risk:	**Medium**

1. General Overview

During the security audit of Tribulant Slideshow Gallery plugin for WordPress CMS, security vulnerability was discovered using DefenseCode ThunderScan web 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, Tribulant Slideshow Gallery, offers to feature content in beautiful and fast JavaScript powered slideshow gallery showcases on your WordPress website. It can easily display multiple galleries throughout your WordPress website displaying your custom added slides, slide galleries or showing slides from WordPress posts/pages.

It has more than 40,000 downloads on wordpress.org.

Homepage:
https://wordpress.org/plugins/slideshow-gallery/
http://tribulant.com/plugins/view/13/wordpress-slideshow-gallery

3. Vulnerability Description

During the security analysis, ThunderScan discovered multiple Cross-Site Scripting vulnerabilities in Tribulant Slideshow Gallery 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.

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, or embedding it as an IMG tag source in another web page administrator will visit, causing the administrator's browser to request the URL automatically - due to missing nonce token the vulnerability is directly exposed to Cross site request forgery, (CSRF) attacks.

The JavaScript code could enable the attacker to make requests with administrator privileges, or grab the session ID and be able to interact with the administrative pages through his own browser.

3.1 Cross-Site Scripting	
Variable:	**$_GET['id']**
Note:	**/**

Sample URL:

```
http://vulnerablesite.com/wp-admin/admin.php?page=slideshow-galleries&method=view&id=1%5C%22%3E%3Cscript%3Ealert%281%29%3C%2Fscript%3E
```

3.2 Cross-Site Scripting	
Variable:	**$_GET['method']**
Note:	**Subscriber id (parameter "id") must exist. Value 1 is a good guess for start ;)**

Sample URL:

```
http://vulnerablesite.com/wp-admin/admin.php?page=slideshow-galleries&method=view%5C%22%3E%3Cscript%3Ealert%281%29%3C%2Fscript%3E&id=1
```

3.3 Cross-Site Scripting	
Variable:	**$_GET['method']**
Note:	**Subscriber id (parameter "id") must exist. Value 1 is a good guess for start ;)**

Sample URL:

```
http://vulnerablesite.com/wp-admin/admin.php?page=slideshow-slides&method=save%5C%22%3E%3Cscript%3Ealert%281%29%3C%2Fscript%3E&id=1
```

3.4 Cross-Site Scripting	
Variable:	**$_GET['Gallerymessage']**
Note:	**/**

Sample URL:

http://vulnerablesite.com/wp-admin/admin.php?page=slideshow-slides&Galleryerror=true&Gallerymessage=No+slides+were+selected%5C%22%3E%3Cscript%3Ealert%281%29%3C%2Fscript%3E

3.5 Cross-Site Scripting	
Variable:	**$_GET['Galleryerror']**
Note:	**/**

Sample URL:

http://vulnerablesite.com/wp-admin/admin.php?page=slideshow-slides&Galleryerror=true%5C%22%3E%3Cscript%3Ealert%281%29%3C%2Fscript%3E&Gallerymessage=No+slides+were+selected

3.6 Cross-Site Scripting	
Variable:	**$_GET['Galleryupdated']**
Note:	**/**

Sample URL:

http://vulnerablesite.com/wp-admin/admin.php?page=slideshow-slides&Galleryupdated=true%5C%22%3E%3Cscript%3Ealert%281%29%3C%2Fscript%3E&Gallerymessage=Slides+added+to+selected+galleries

4. Solution

Vendor resolved security issues in latest release. All users are strongly advised to update WordPress Tribulant Slideshow Gallery plugin to the latest available version (1.6.6.1).

5. Credits

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

6. Disclosure Timeline

3/23/2017	**Vendor contacted**
3/24/2017	**Vendor responded**
3/29/2017	**Update released**
4/10/2017	**Advisory released to the public**

7. About DefenseCode ThunderScan

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/