DefenseCode

DefenseCode ThunderScan SAST Advisory

WordPress Simple Slideshow Plugin

Multiple Security Vulnerabilities

WordPress Simple Slideshow Plugin – Multiple Security Vulnerabilities	
Advisory ID:	**DC-2017-02-016**
Software:	**WordPress Simple Slideshow Plugin**
Software Language:	**PHP**
Version:	**2.2 and below**
Vendor Status:	**Vendor contacted, update released**
Release Date:	**2017/05/29**
Risk:	**Medium**

1. General Overview

During the security audit of Simple Slideshow Manager plugin for WordPress CMS, multiple 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, Simple Slideshow Manager is "*The easy and best slideshow manager plugin where you can create any number of slideshow. Can have any number of video or image slides, enjoy displaying slideshow using widgets, shortcodes or php codes.*" It has more than 9,000 active installs according to wordpress.org.

Homepage:
https://wordpress.org/plugins/simple-slideshow-manager/
http://www.acurax.com/products/simple-slideshow-manager/

3. Vulnerability Description

During the security analysis, ThunderScan discovered Cross-Site Scripting vulnerabilities in Simple Slideshow Manager WordPress plugin.

The Cross-Site Scripting vulnerabilities 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.

In the specific case of the second Cross-Site scripting vulnerability (3.2), some modern browsers URL encode the < and > characters. The easiest way to reproduce the vulnerability is to use Internet Explorer, or older version of some other browser.

3.1 Cross-Site Scripting	
Vulnerable Function:	**echo**
Vulnerable Variable:	**$_GET['name']**

Vulnerable URL:

```
http://www.vulnerablesite.com/wp-admin/admin.php?page=Acurax-Slideshow-Add-
Images&name="></script><script>alert(42)</script>
```

File: simple-slideshow-manager\includes\option_fields.php

```
1276  $acx_selected_gallery_name = trim($_GET['name']);
...
1282  <input type = "text" autocomplete="off" id = "rename" name = "rename" class="field"
value="<?php echo $acx_selected_gallery_name;  ?>" onblur="if (this.value == '') {this.value
= '<?php echo $acx_selected_gallery_name;  ?>';}" onfocus="if (this.value == '<?php echo
$acx_selected_gallery_name;  ?>') {this.value = '';}" />
```

3.2 Cross-Site Scripting	
Vulnerable Function:	**echo**
Vulnerable Variable:	**$_SERVER['REQUEST_URI']**

Vulnerable URL:

```
http://www.vulnerablesite.com/wp-admin/admin.php?page=Acurax-Slideshow-Add-
Images&name="></script><script>alert(42)</script>
```

File: simple-slideshow-manager\includes\option_fields.php

```
1284  <input type = "hidden" id = "url" name = "url" value = "<?php echo str_replace( '%7E',
'~', $_SERVER['REQUEST_URI']); ?>"/>
```

4. Solution

Vendor resolved the security issues after we reported the vulnerabilities. All users are strongly advised to update WordPress Simple Slideshow plugin to the latest available version.

5. Credits

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

6. Disclosure Timeline

2017/03/28	**Vendor contacted**
2017/04/06	**Update released**
2017/05/29	**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/