DefenseCode

DefenseCode ThunderScan SAST Advisory

WordPress Podlove Podcast Publisher Plugin Security Vulnerability

WordPress Podlove Podcast Publisher Plugin – Security Vulnerability	
Advisory ID:	**DC-2017-05-006**
Software:	**WordPress Podlove Podcast Publisher plugin**
Software Language:	**PHP**
Version:	**2.5.3 and below**
Vendor Status:	**Vendor contacted, update released**
Release Date:	**2017/08/07**
Risk:	**High**

1. General Overview

During the security audit of Podlove Podcast Publisher plugin for WordPress CMS, security vulnerability was 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, Podlove Podcast Publisher tries to solve the problem from the podcasters' perspective and implements a variety of features and workflows that have been rather difficult to achieve with WordPress until now.

Homepage:
https://wordpress.org/plugins/podlove-podcasting-plugin-for-wordpress/
http://publisher.podlove.org/

3. Vulnerability Description

During the security analysis, ThunderScan discovered SQL injection vulnerability in Podlove Podcast Publisher 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. Users that do not have full administrative privileges could abuse the database access the vulnerability provides 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 attacker the vulnerable code is also directly exposed to attack vectors such as Cross Site request forgery (CSRF).

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

Vulnerable URL:

```
http://vulnerablesite.com/wp-
admin/admin.php?page=podlove_contributor_settings&order=asc&orderby=gender AND (SELECT *
FROM (SELECT(SLEEP(5)))DefenseCode)
```

File: lib\modules\contributors\contributor_list_table.php

```
176  $orderby = 'ORDER BY ' . esc_sql($_GET['orderby']);
...
203  $data = \Podlove\Modules\Contributors\Model\Contributor::all( $orderby . ' ' . $order
);
```

File: lib\model\base.php

```
234  public static function all( $sql_suffix = '' ) {
235    return self::find_all_by_sql(
236          'SELECT * FROM ' . static::table_name() . ' ' . $sql_suffix
237    );
...
548  public static function find_all_by_sql($sql) {
...
554    $rows = $wpdb->get_results($sql);
```

4. Solution

Vendor resolved the security issues after we reported the vulnerability. All users are strongly advised to update WordPress Podlove Podcast Publisher plugin to the latest available version.

5. Credits

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

6. Disclosure Timeline

2017/05/31	**Vendor contacted**
2017/06/05	**Update released**
2017/08/07	**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/