DefenseCode

DefenseCode ThunderScan SAST Advisory

WordPress Booking Calendar Plugin
Multiple Security Vulnerabilities

WordPress Booking Calendar Plugin – Multiple Security Vulnerabilities	
Advisory ID:	**DC-2017-005**
Software:	**WordPress Booking Calendar plugin**
Software Language:	**PHP**
Version:	**7.0/7.1 and below**
Vendor Status:	**Vendor contacted, updates released**
Release Date:	**2017/12/13**
Risk:	**Medium**

1. General Overview

During the security audit of Booking Calendar 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

Booking Calendar plugin - described by the authors as the ultimate booking system for online reservation and availability checking service for your site.

According to wordpress.org, it has more than 40,000 active installs.

Homepage:
https://wordpress.org/plugins/booking/
http://wpbookingcalendar.com/
https://wordpress.org/plugins/booking/#developers

3. Vulnerability Description

During the security analysis, ThunderScan discovered SQL injection and Local file inclusion vulnerabilities in Booking Calendar WordPress plugin.

The easiest way to reproduce the SQL injection vulnerabilities is to send the specified parameter to 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 vulnerabilities provide to either escalate their privileges or obtain and modify database contents they were not supposed to be able to.

By requesting a specially crafted URL, the attacker can cause remote server to execute a php file of his choosing. Although the user requesting the URL has to be logged into the WordPress administrative console, the attacker can cause the administrator to request such a URL by using various social engineering/phishing approaches. Specified file will be interpreted by php interpreter, and any valid php code will indeed be executed. If the php installation on server has "allow_url_include=1" configuration option set, this attack can be expanded to execute a php file from any remote URL. If the php version is less than 5.3.4, the ".php" that gets appended to the end of the file name attacker chose can be omitted by adding a null character ("%00") to the requested URL, and enable the attacker to execute any file, regardless of the extension.

Due to the CSRF token needed to perform the attack the risk is lowered to medium.

3.1 SQL injection

Vulnerable Function:	**$wpdb->query()**
Vulnerable Variable:	**$_POST["booking_id"];**

Vulnerable URL:

```
/wp-admin/admin-ajax.php
```

File: booking\lib\wpbc-ajax.php

```
152    $booking_id          = $_POST[ "booking_id" ];
153    $approved_id         = explode('|',$booking_id);
...
162    $approved_id_str = join( ',', $approved_id);
...
165    if ( false === $wpdb->query( $wpdb->prepare( "UPDATE {$wpdb->prefix}bookingdates SET
approved = %s WHERE booking_id IN ({$approved_id_str})", $is_approve_or_pending ) ) ){
```

3.2 SQL injection

Vulnerable Function:	**$wpdb->query()**
Vulnerable Variable:	**$_POST["booking_id"];**

Vulnerable URL:

```
/wp-admin/admin-ajax.php
```

File: booking\lib\wpbc-ajax.php

```
        110    $id_of_new_bookings  = $_POST[ "booking_id" ];
        111    $arrayof_bookings_id = explode('|',$id_of_new_bookings);
```

```
...
114    wpbc_update_number_new_bookings( $arrayof_bookings_id, $is_new , $user_id );
```

File: booking\lib\wpdev-booking-functions.php

```
1468 function wpbc_update_number_new_bookings( $id_of_new_bookings, $is_new = '0' , $user_id
= 1 ){
...
1485   $update_sql = "UPDATE {$wpdb->prefix}booking AS bk SET bk.is_new = {$is_new} WHERE
bk.booking_id IN  ( {$id_of_new_bookings} ) ";
...
1487   if ( false === $wpdb->query( $update_sql  ) ) {
```

3.3 Local File Inclusion	
Vulnerable Function:	**include()**
Vulnerable Variable:	**$_POST['captcha_chalange']**

Vulnerable URL:

```
/wp-admin/admin-ajax.php
```

File: booking\core\lib\wpbc-booking-new.php

```
127    if (! wpbc_check_CAPTCHA( $_POST['captcha_user_input'], $_POST['captcha_chalange'],
$bktype ) ) {
...
19   function wpbc_check_CAPTCHA( $the_answer_from_respondent, $prefix, $bktype ) {
...
23       $correct = $captcha_instance->check($prefix, $the_answer_from_respondent);
```

File: wp-content\plugins\booking\js\captcha\captcha.php

```
139  function check( $prefix, $response ) {
...
141    include( $this->tmp_dir . $prefix . '.php' );
```

4. Solution

Vendor resolved the security issues. All users are strongly advised to update WordPress Booking Calendar plugin to the latest available version.

5. Credits

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

6. Disclosure Timeline

2016/11/15	**Vulnerabilities discovered**
2017/04/04	**Vendor contacted**
2017/04/04	**Vendor responded - 7.0 already fixed SQL injection vulnerabilities**
2017/04/04	**Update released for Local File Inclusion vulnerability (7.1)**
2017/12/13	**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/