DefenseCode

DefenseCode ThunderScan SAST Advisory

WordPress Spider Event Calendar Plugin SQL Injection Vulnerability

WordPress Spider Event Calendar Plugin – SQL Injection Vulnerability	
Advisory ID:	**DC-2017-01-017**
Software:	**WordPress Spider Event Calendar Plugin**
Software Language:	**PHP**
Version:	**1.5.49 and below**
Vendor Status:	**Vendor contacted, vulnerability confirmed**
Release Date:	**20170502**
Risk:	**High**

1. General Overview

During the security audit, multiple security vulnerabilities were discovered in WordPress Spider Event Calendar Plugin 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 developers, WordPress Event Calendar is a free, user-friendly responsive plugin to manage multiple recurring events and with various options.

It has more than 30,000 downloads on wordpress.org.

Homepage:
https://wordpress.org/plugins/spider-event-calendar/
https://web-dorado.com/products/wordpress-calendar.html

3. Vulnerability Description

During the security analysis, ThunderScan discovered SQL injection vulnerability in Spider Event Calendar 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 to 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.

Although the original request does include the nonce value (nonce_sp_cal POST parameter), it's not checked and can freely be omitted by the attacker. That leaves the vulnerability wide open to Cross site request forgery (CSRF) attacks – authors of any webpage the administrator visits while being logged into the vulnerable WordPress instance can enable the attacker to take full control of the WordPress database.

The attacker can entice the administrator to visit such a web page in various ways, including sending the URL by email, posting it as a part of the comment on the vulnerable site or another forum, causing the administrator's browser to execute the JavaScript found there, cause a POST request to the vulnerable plugin, and freely abuse the SQL injection vulnerability.

3.1 SQL injection	
Function:	**$wpdb->get_results($query);**
Variable:	**$_POST['order_by']**

Vulnerable URL:

```
http://www.vulnerablesite.com/wp-
admin/admin.php?page=SpiderCalendar&task=show_manage_event&calendar_id=1
```

Vulnerable Body:

```
search events by title=a&startdate=2011-11-11&enddate=2017-11-
11&page_number=1&serch_or_not=search&id_for_playlist=&asc_or_desc=&order_by=date AND (SELECT
* FROM (SELECT(SLEEP(5)))x)
```

File: spider-event-calendar\calendar_functions.php

```
440     $sort["sortid_by"] =esc_sql(esc_html(stripslashes($_POST['order_by'])));
...
445     $order = "ORDER BY " . $sort["sortid_by"] . " ASC";
...
450     $order = "ORDER BY " . $sort["sortid_by"] . " DESC";
...
486      $query = $wpdb->prepare ("SELECT " . $wpdb->prefix . "spidercalendar_event.*, " .
$wpdb->prefix . "spidercalendar event category.title as cattitle FROM " . $wpdb->prefix .
"spidercalendar event LEFT JOIN " . $wpdb->prefix . "spidercalendar event category ON " .
$wpdb->prefix . "spidercalendar event.category=" . $wpdb->prefix .
"spidercalendar_event_category.id WHERE calendar=%d " . $where . " " . $order . " " . "
LIMIT %d,20",$calendar_id,$limit);
...
489     $rows = $wpdb->get_results($query);
```

4. Solution

Vendor resolved the security issues in one of the subsequent releases. All users are strongly advised to update WordPress Spider Event Calendar plugin to the latest available version. Version 1.5.52 no longer seems to be vulnerable.

5. Credits

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

6. Disclosure Timeline

20170404	**Vendor contacted**
20170405	**Vendor responded: *"Thanks for noticing and told us about this, we will take into account and will fix the issues with upcoming update."***
?	**Update released**
20170502	**Latest plugin version tested. Vulnerability seems fixed.** **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/