CVE-2020-9019 Details

Description:

The WPJobBoard plugin 5.5.3 for WordPress allows persistent XSS via the Add Job form, as demonstrated by title and description.

Additional Information

In wpjobboard WordPress plugin, an attacker can submit malicious javascript codes (persistent XSS) on some fields of "add job" form (in frontend). Then, when an admin want to edit (or delete) this job in control page, the malicious code is executed on his system.

Tested on:

Demo (https://wpjobboard.net/demo/)

Vulnerability Type:

Cross Site Scripting (XSS)

Vendor of Product:

https://wpjobboard.net

Affected Product Code Base:

Wpjobboard Wordpress Plugin - 5.5.3

Affected Component:

Job editing and deletion in admin panel

Attack Type:

Remote

Impact:

Code execution

Discovered By:

Mohamad Pishdar -Web security specialist in Imam Khomeini International University Cert Center (cert.ikiu.ac.ir)-IRAN.

How to Prevent:

To fix this vulnerability, the following points are proposed:

If you have access to new and secure version of wpjobboard WordPress plugin, be sure to use it:

Wpjobboard WordPress plugin Official Website

If for any reason you can't update, follow these instructions:

- If you are a programmer, reject any input values that contain any JavaScript codes. If need to accept JavaScript characters, the application must encode any values that interpreted as JavaScript. Full explanations are available at the bellowed link:

  OWASP Cross Site Scripting Prevention Cheat Sheet

- If you are unfamiliar with programming, follow these instructions:
  - In the admin section before viewing or deleting job's information, have a quick overview of JavaScript codes. If you see these codes, delete the row of malicious code from the database section.
  - Always have a backup of your system.