WordPress WP Project Manager Plugin <= 2.4.13 is vulnerable to Cross Site Scripting (XSS)

Low priority
No impactful threat

<= 2.4.13
Vulnerable version(s)

2.4.14
Patched version

WordPress plugin | No VDP 11 Oct, 2021

Risks CVSS 5.4

Vulnerabilities like this one are used in mass-exploit campaigns. Attackers use these to attack thousands of websites at a time, regardless of traffic size or popularity.

As immediate action, update the affected plugin. If you're unable to do so, ask your hosting provider or web developer for help.

User Interaction Required

While this vulnerability can be initiated by the role shown in "Required Privilege", successful exploitation requires a privileged user to perform an action — such as clicking a malicious link, visiting a crafted page, or submitting a form.

5.4 Cross Site Scripting (XSS)

This could allow a malicious actor to inject malicious scripts, such as redirects, advertisements, and other HTML payloads into your website which will be executed when guests visit your site.

CVSS score is a way to evaluate and rank reported vulnerabilities in a standardized and repeatable way but which is not ideal for WordPress.

Solutions

This security issue has a low severity impact and is unlikely to be exploited.

Update to version 2.4.14 or later.

Update to version 2.4.14 or later to resolve the vulnerability. Patchstack users can turn on auto-update for vulnerable plugins only.

Details

Software	WP Project Manager
Type	Plugin
Vulnerable versions	<= 2.4.13
Patched in	2.4.14
OWASP Top 10	A7: Cross-Site Scripting (XSS)
Classification	Cross Site Scripting (XSS)
CVE ID	CVE-2021-36826 ↗
Patchstack priority	Low
CVSS severity	5.4
Required privilege	Subscriber
Developer	Claim ownership ↗
PSID	d537f428425e
Credits	Jörgson
Published	11 Oct, 2021

⤢ Expand full details

Have additional information or questions about this entry? Let us know.

Go to | WordPress plugin | No VDP

Timeline

Reported by Jörgson

NaN undefined, NaN

Vulnerability mitigation

Pricing

Application security (SCA)

RapidMitigate NEW

Threat Intelligence (API)

VS Monarx

VS Imunify360

VS Wordfence

Documentation

How can Patchstack provide the fastest protection?

How does Patchstack mitigate vulnerabilities?

Why would a hacker target my website?

What if my website has already been compromised?

patchstack