

WordPress Custom Login and Registration Plugin <= 1.0.0 is vulnerable to Cross Site Scripting (XSS)



Medium priority

vPatch available



<= 1.0.0

Vulnerable version



No official fix available

Fixed version

Plugin



No VDP

02 May 2025 by Patchstack

Risks CVSS 6.5

This vulnerability is moderately dangerous and expected to become exploited.

6.5 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.

This is a general description of this vulnerability type, specific impact varies case by case. CVSS score is a way to evaluate and rank reported vulnerabilities in a standardized and repeatable way, but it is not ideal for CMSs.

We advise to mitigate or resolve the vulnerability immediately.



Automatically mitigate vulnerabilities and keep your websites safe




Patchstack has issued a virtual patch to mitigate this issue by blocking any attacks until an official fix becomes available, can be tested and be safely applied.


Get the fastest vulnerability mitigation with Patchstack! [Get Started](#)

Details

[↗ Expand full details](#)

Have additional information or questions about this entry? [Let us know.](#)

- Reported by  **Nguyen Ngoc Quang Bach (maysbachs)**
13 Apr 2025
-  Early warning sent out to Patchstack customers
02 May 2025
-  Published by Patchstack
04 May 2025

[Go to](#)[Plugin page](#) [No VDP](#)

How can Patchstack provide the fastest protection? 

Patchstack is one of the largest open-source vulnerability disclosers in the world.

~~What is virtual patching?~~ For example, in 2023 more than 70% of new WordPress vulnerabilities were 

originally published by Patchstack. This focus on research enables us to deploy Patchstack's Patching auto-mitigates security vulnerabilities even when there's no vulnerability protection rules faster than anybody else.

~~Why would a hacker target my website?~~ official patch available. It's the fastest and most effective way to eliminate new 

security vulnerabilities without sacrificing performance.

Hackers automate attacks against new security vulnerabilities to take over as 

~~What if my website has already been compromised?~~ many websites as they can before users have time to patch and update. The 

attacks are opportunistic and victims are not chosen - everyone is a target.

We recommend reaching out to your hosting provider for server-side malware 

scanning or use a professional incident response service. Don't rely on plugin

based malware scanners as they are commonly tampered with by malware.

Weekly WordPress security intelligence delivered to your inbox.

Website security	For plugin devs	For researchers	Resources	Patchstack
Pricing	Managed VDP	Bug bounty	Vulnerability Database	About
For WordPress	Log in NEW	Log in NEW	Whitepaper 2024	Careers
For WooCommerce	Active programs	Guidelines	WordPress Statistics NEW	Merch store
For agencies	Security auditing	Learn NEW	Case studies NEW	Media kit
API For hosts		Discord	Articles	
Documentation				
FAQ				
Log in				
Socials				
LinkedIn				
Facebook				
X				

