WordPress Contact Form 7 – PayPal & Stripe Add-on Plugin <= 2.3.4 is vulnerable to Cross Site Scripting (XSS)

Low priority
vPatch unnecessary

<= 2.3.4
Vulnerable version

2.4.1
Fixed version

Plugin · No VDP · 07 May 2025 by Patchstack

Risks CVSS 5.9

5.9 **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.

Solutions

Update to version 2.4.1 or later.

Update to version 2.4.1 or later to remove the vulnerability. Patchstack users can turn on auto-update for vulnerable plugins only.

Details

⤢ Expand full details

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

Timeline

Reported by  Nabil Irawan
02 Apr 2025

Published by Patchstack
07 May 2025

How can Patchstack provide the fastest protection?

Patchstack is one of the largest open-source vulnerability disclosers in the world. For example, in 2023 more than 70% of new WordPress vulnerabilities were originally published by Patchstack. This focus on research enables us to deploy vulnerability protection rules faster than anybody else.

What is virtual patching?

Patchstack vPatching auto-mitigates security vulnerabilities even when there's no official patch available. It's the fastest and most effective way to eliminate new security vulnerabilities without sacrificing performance.

Why would a hacker target my website?

Hackers automate attacks against new security vulnerabilities to take over as 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.

What if my website has already been compromised?

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.

Enter e-mail Subscribe

European Innovation Council Co-funded by the European Union