WordPress Monetag Official Plugin Plugin <= 1.1.3 is vulnerable to Broken Access Control

Medium priority
vPatch available

<= 1.1.3
Vulnerable version

No official fix available
Fixed version

Plugin · No VDP · 29 January 2025 by Patchstack

Risks CVSS 7.2

This vulnerability is moderately dangerous and expected to become exploited.

7.2 Broken Access Control

A broken access control issue refers to a missing authorization, authentication or nonce token check in a function that could lead to an unprivileged user to executing a certain higher privileged action.

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.

Timeline

Reported by  Mika
27 Nov 2024

Early warning sent out to Patchstack customers
29 Jan 2025

Published by Patchstack
31 Jan 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. 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