

[Pricing](#)[Case studies](#)[Login](#)[Start trial](#)

WordPress amr users Plugin $\leq 4.59.4$ is vulnerable to CSV Injection



Low priority

No impactful threat



$\leq 4.59.4$


Vulnerable version(s)



No official patch available

Patched version

 WordPress plugin

 No VDP

22 Mar, 2023 by Patchstack

Get the fastest vulnerability mitigation with Patchstack!

[Get started](#)

Risks CVSS 5.8

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.

[Pricing](#)[Case studies](#)[Login](#)[Start trial](#)

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.

5.8 CSV Injection

This could allow a malicious actor to craft malicious formulas to then exploit vulnerabilities in the spreadsheet software or to execute commands to gain access to the victim's PC.

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.

Details

[Pricing](#)

[Case studies](#)

[Login](#)

[Start trial](#)

Software

amr users

Type

Plugin

Vulnerable versions ⁱ

<= 4.59.4

OWASP Top 10 ⁱ

A1: Injection

Classification ⁱ

CSV Injection

CVE ID ⁱ

[Expand full details](#)

[CVE-2022-45348](#)

Patchstack priority ⁱ

Low

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

CVSS severity ⁱ

5.8

Required privilege ⁱ

Subscriber

Developer

[Claim ownership](#)

PSID ⁱ

af617aa8d2cb

Credits

Mika

Published

22 Mar, 2023

Go to

WordPress plugin

No VDP


[Pricing](#)

[Case studies](#)

[Login](#)

[Start trial](#)



Reported by  **Mika**

22 Nov, 2022

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? ▼

Vulnerability mitigation

[Pricing](#)

[Application security \(SCA\)](#)

[RapidMitigate](#) NEW

[Threat Intelligence \(API\)](#)

[VS Monarx](#)

[VS Imunify360](#)

[WordPress](#)

[Documentation](#)

[Service status](#)

[Log in](#)

Code security

[Managed VDP](#) NEW

[Active VDP directory](#) 1,180

Weekly WordPress security intelligence delivered to your inbox.

[Subscribe](#)

[Pricing](#)

[Case studies](#)

[Login](#)

[Start trial](#)

[Log in](#) NEW

Bug bounty

[Bug bounty](#)

[Leaderboard](#)

[Guidelines](#)

[Learn](#) NEW

[Report](#)

[Discord](#)

[Log in](#) NEW

Use cases

[Web developers](#)

[Webhosts](#) NEW

[Software vendors](#)

[WordPress](#)

[WooCommerce](#)

Resources

[Partners](#)

[Vulnerability database](#)

[Whitepaper 2026](#) NEW

[Articles](#)

[Case studies](#) NEW

[Webinars](#) NEW

[Vulnerability statistics](#)

Patchstack

[About](#)

[Careers](#)

[Merch store](#)

[Pricing](#)

[Case studies](#)

[Login](#)

[Start trial](#)

[Facebook](#)

[X](#)

[Report Vulnerability](#)



© Patchstack

[DPA](#)

[Privacy Policy](#)

[Accessibility](#)

[Terms & Conditions](#)