WordPress Email Subscribers & Newsletters Plugin <= 5.5.2 is vulnerable to CSV Injection

Low priority
No impactful threat

<= 5.5.2
Vulnerable version(s)

5.5.3
Patched version

WordPress plugin | No VDP

6 Feb, 2023 by Patchstack

Risks CVSS 6.1

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.

6.1 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.

Update to version 5.5.3 or later.

Update to version 5.5.3 or later to resolve the vulnerability. Patchstack users can turn on auto-update for vulnerable plugins only.

Details

Software	Email Subscribers & Newsletters
Type	Plugin
Vulnerable versions	<= 5.5.2
Patched in	5.5.3
OWASP Top 10	A1: Injection
Classification ⤢ Expand full details	CSV Injection
CVE ID	CVE-2022-45810 ↗
Patchstack priority	Low
CVSS severity	6.1
Required privilege	Unauthenticated
Developer	Claim ownership ↗
PSID	bc18fb9ece3e
Credits	Mika
Published	6 Feb, 2023

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

Go to | WordPress plugin | No VDP

Timeline

Reported by Mika
30 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?

Code security

Managed VDP NEW

Active VDP directory 1,180

Security auditing

Compliance (CRA) NEW

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

Patchstack

About

Careers

Merch store

Media kit

LinkedIn

Facebook

X

Report Vulnerability

patchstack

DPA

Privacy Policy

Accessibility

Terms & Conditions