WordPress Simple CSV/XLS Exporter Plugin <= 1.5.8 is vulnerable to CSV Injection

Low priority
No impactful threat

<= 1.5.8
Vulnerable version(s)

No official patch available
Patched version

WordPress plugin | No VDP

2 Mar, 2023 by Patchstack

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.

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

Software	Simple CSV/XLS Exporter
Type	Plugin
Vulnerable versions	<= 1.5.8
OWASP Top 10	A1: Injection
Classification	CSV Injection
CVE ID	CVE-2022-42882 ↗
Patchstack priority	Low
CVSS severity	5.8
Required privilege	Editor
Developer	Claim ownership ↗
PSID	88fece4e6031
Credits	Mika
Published	2 Mar, 2023

⤢ Expand full details

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

Go to | WordPress plugin | No VDP

Reported by Mika

20 Oct, 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?

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