

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

## WordPress WP CSV Exporter Plugin <= 2.0 is vulnerable to CSV Injection



### Low priority

No impactful threat



### <= 2.0


Vulnerable version(s)



### No official patch available

Patched version

 WordPress plugin

 No VDP

8 Dec, 2022 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

wp-csv-exporter

Type

Plugin

Vulnerable versions <sup>i</sup>

<= 2.0

OWASP Top 10 <sup>i</sup>

A1: Injection

Classification <sup>i</sup>

CSV Injection

CVE ID <sup>i</sup>

[Expand full details](#)

[CVE-2022-38702](#)

Patchstack priority <sup>i</sup>

Low

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

CVSS severity <sup>i</sup>

5.8

Required privilege <sup>i</sup>

Contributor

Developer

[Claim ownership](#)

PSID <sup>i</sup>

c865116adc7d

Credits

Mika

Published

8 Dec, 2022

[Go to](#)

[WordPress plugin](#)

[No VDP](#)

[Pricing](#)

[Case studies](#)

[Login](#)

[Start trial](#)



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? ▼

**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](#)