

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

## WordPress Posts and Users Stats Plugin $\leq 1.1.3$ is vulnerable to CSV Injection



### Low priority

No impactful threat



### $\leq 1.1.3$

Vulnerable version(s)



### 1.1.4

Patched version

 WordPress plugin

 No VDP

2 Feb, 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.

### **Update to version 1.1.4 or later.**

Update to version 1.1.4 or later to resolve the vulnerability. Patchstack users can turn on auto-update for vulnerable plugins only.

[Pricing](#)

[Case studies](#)

[Login](#)

[Start trial](#)

# Details

Software

Posts and Users Stats

Type

Plugin

Vulnerable versions i

<= 1.1.3

Patched in i

1.1.4

OWASP Top 10 i

A1: Injection

Classification i

[Expand full details](#)

CSV Injection

CVE ID i

[CVE-2022-44738](#) ↗

Patchstack priority i

Low

CVSS severity i

5.8

Required privilege i

Subscriber

Developer

[Claim ownership](#) ↗

PSID i

adb9c8d12136

Credits

 [Mika](#)

Published

2 Feb, 2023

[Pricing](#)

[Case studies](#)

[Login](#)

[Start trial](#)

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

Go to




WordPress plugin



No VDP

## Timeline



Reported by  **Mika**

7 Nov, 2022

How does Patchstack provide the fastest protection? ▼

Pricing

How does Patchstack mitigate vulnerabilities? ▼

Application security (SCA)

RapidMitigate NEW

Why would a hacker target my website? ▼

Threat Intelligence (ATI)

VS Monarx

What if my website has already been compromised? ▼

VS Imunity360

VS Wordfence

Documentation

[Pricing](#)

[Case studies](#)

[Login](#)

[Start trial](#)

### Code security

[Managed Email](#)

[Subscribe](#)

[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

[Pricing](#)

[Case studies](#)

[Login](#)

[Start trial](#)

## Patchstack

[About](#)

[Careers](#)

[Merch store](#)

[Media kit](#)

[LinkedIn](#)

[Facebook](#)

[X](#)

[Report Vulnerability](#)



© Patchstack

[DPA](#)

[Privacy Policy](#)

[Accessibility](#)

[Terms & Conditions](#)