

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

WordPress Simple History Plugin \leq 3.3.1 is vulnerable to CSV Injection



Low priority

No impactful threat



\leq 3.3.1

Vulnerable version(s)



3.4.0

Patched version

WordPress plugin

No VDP

2 Feb, 2023 by Patchstack

Get the fastest vulnerability mitigation with Patchstack!

[Get started](#)

Risks CVSS 3

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.

3 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 3.4.0 or later.

Update to version 3.4.0 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

Simple History

Type

Plugin

Vulnerable versions i

<= 3.3.1

Patched in i

3.4.0

OWASP Top 10 i

A1: Injection

Classification i

[Expand full details](#)

CSV Injection

CVE ID i

[CVE-2022-45350](#)

Patchstack priority i

Low

CVSS severity i

3

Required privilege i

Subscriber

Developer

[Claim ownership](#)

PSID i

d53822044a90

Credits

 ed32.dll

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 [ed32.dll](#)

17 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

 [Manage VDP mail](#)

[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](#)