

Pricing

Case studies

Login

Start trial

WordPress Commenter Emails Plugin <= 2.6.1 is vulnerable to CSV Injection



Low priority

No impactful threat



<= 2.6.1

Vul



No

Pat

We value your privacy

We use cookies to enhance your browsing experience, serve personalised ads or content, and analyse our traffic. By clicking "Accept All", you consent to our use of cookies.

Read more.

Customize

Reject All

Accept All



WordPress plug

Feb, 2023 by Patchstack

Get the fastest vulnerability mitigation with Patchstack!

Get started

Risks CVSS 4.7

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.

4.7 CSV Injection

This could allow an attacker to exploit vulnerabilities and gain access to the system.

We value your privacy

We use cookies to enhance your browsing experience, serve personalised ads or content, and analyse our traffic. By clicking "Accept All", you consent to our use of cookies.

[Read more.](#)

CVSS score is a way to measure the severity of a vulnerability. It is not ideal for WordPress.

When exploit

s to gain

way but which is not

Solutions

This security issue has a low severity impact and is unlikely to be exploited.

Details

Pricing

Case studies

Login

Start trial

Software

Commenter Emails 2.6.1

Type

Plugin

Vulnerable versions ⓘ

<= 2.6.1

OWASP Top 10 ⓘ

A1: Injection

Classification ⓘ

CSV Injection

CVE ID ⓘ

↗ Expand full details

CVE-2022-45360 ↗

Patchstack price

Low

Have you
CVSS severity ⓘ

know.

4.7

Required privileges

authenticated

Developer

Ownership ↗

PSID ⓘ

7afa84e72c95

Credits

👤 Mika

Published

2 Feb, 2023

We value your privacy

We use cookies to enhance your browsing experience, serve personalised ads or content, and analyse our traffic. By clicking "Accept All", you consent to our use of cookies.

[Read more.](#)

Go to

WordPress plugin

No VDP

Pricing

Case studies

Login

Start trial



Reported by **Mika**

18 Nov, 2022

How can Patchstack provide the fastest protection? ▼

How does Patchstack mitigate vulnerabilities? ▼

Why would a hacker... ▼

What if my website... ▼

We value your privacy

We use cookies to enhance your browsing experience, serve personalised ads or content, and analyse our traffic. By clicking "Accept All", you consent to our use of cookies.

[Read more.](#)

Vulnerability mitigation

Pricing

Application security

RapidMitigate NEW

Threat Intelligence (API)

Weekly WordPress security intelligence delivered to your inbox.

VS Monarx

VS Imunify360

WordPress

Subscribe

Documentation

Service status

Log in

Code security

Managed VDP NEW

Active VDP directory 1,180

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

We value your privacy

We use cookies to enhance your browsing experience, serve personalised ads or content, and analyse our traffic. By clicking "Accept All", you consent to our use of cookies.

[Read more.](#)



[Pricing](#)

[Case studies](#)

[Login](#)

[Start trial](#)

[Facebook](#)

[X](#)

[Report Vulnerability](#)



© Patchstack

[DPA](#)

[Privacy Policy](#)

[Accessibility](#)

[Terms & Conditions](#)

We value your privacy

We use cookies to enhance your browsing experience, serve personalised ads or content, and analyse our traffic. By clicking "Accept All", you consent to our use of cookies.

[Read more.](#)