

Pricing

Case studies

Login

Start trial

WordPress Coming Soon Plugin <= 1.5.9 is vulnerable to SQL Injection



Low priority

No impactful threat



<= 1.5.9

Vul



1.6

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

Jul, 2023 by Patchstack

Get the fastest vulnerability mitigation with Patchstack!

Get started

Risks CVSS 7.6

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.

7.6 SQL Injection

This could allow a malicious actor to directly interact with your database, including but not limited to stealing information.

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 is **Critical** and **Unauthenticated**.

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.

Update to version 1.6.0 or later.

Update to version 1.6.0 or later to resolve the vulnerability. Patchstack users can turn on auto-update for vulnerable plugins only.

Details

[Pricing](#)

[Case studies](#)

[Login](#)

[Start trial](#)

Type

Plugin

Vulnerable versions ⓘ

<= 1.5.9

Patched in ⓘ

1.6.0

OWASP Top 10 ⓘ

A1: Injection

Classification ⓘ

SQL Injection

CVE ID ⓘ

[CVE-2022-46849](#) ↗

Patchstack price

Low

CVSS severity ⓘ

7.6

Required privileges

Administrator

Developer

[Plugin ownership](#) ↗

PSID ⓘ

0a93f0e48b26

Credits

[Le Ngoc Anh](#)

Published

5 Jul, 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.](#)

[↗ Expand full details](#)

Pricing

Case studies

Login

Start trial

Go to



WordPress plugin



No VDP

Timeline



Reported by Le Ngoc Anh

9 Dec, 2022

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
How can Patchstack help?

RapidMitigate NEW

Threat Intelligence (ATI)
How does Patchstack mitigate vulnerabilities?

VS Monarx

VS Immunify360
Why would a hacker target my website?

VS Wordfence

Recovery
What if my website has already been compromised?

Service status

Log in

Code security

Managed VDP NEW

Active VDP 1,180

Security auditing

Compliance (CRA) NEW

Weekly WordPress security intelligence delivered to your inbox.

Pricing

Case studies

Login

Start trial

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 data

Whitepaper 2026 NEW

Articles

Case studies NEW

Webinars NEW

Vulnerability statistics

Patchstack

About

Careers

Merch store

Media kit

LinkedIn

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.](#)

[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.](#)