

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

WordPress Sucuri Security Plugin \leq 1.8.33 is vulnerable to Cross Site Request Forgery (CSRF)



Low priority

No impactful threat



\leq 1.8.33

Vulnerable version(s)



1.8.34

Patched version

WordPress plugin

No VDP

14 Sep, 2022

Get the fastest vulnerability mitigation with Patchstack!

[Get started](#)

Risks CVSS 2.3

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.

2.3 Cross Site Request Forgery (CSRF)

This could allow a malicious actor to force higher privileged users to execute unwanted actions under their current authentication.

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 1.8.34 or later.

Update to version 1.8.34 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

Sucuri Security

Type

Plugin

Vulnerable versions i

<= 1.8.33

Patched in i

1.8.34

OWASP Top 10 i

A5: Broken Access Control

Classification i

[Expand full details](#) Cross Site Request Forgery (CSRF)

CVE ID i

[CVE-2022-29489](#)

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

Patchstack priority i

Low

CVSS severity i

2.3

Required privilege i

Unauthenticated

Developer

[Claim ownership](#)

PSID i

38e16a5d6ccd

Credits

 [Rafie Muhammad](#)

Published

14 Sep, 2022

Pricing

Case studies

Login

Start trial

Go to



WordPress plugin



No VDP

Timeline



Reported by Rafie Muhammad

NaN undefined, NaN

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? ▼

Pricing

Application security (SCA)

RapidMitigate NEW

Threat Intelligence (API)

VS Monarx

VS Imunify360

VS Wordfence

Documentation

Enter e-mail

Service status

Subscribe

Weekly WordPress security intelligence delivered to your inbox.

[Pricing](#)

[Case studies](#)

[Login](#)

[Start trial](#)

Code security

[Managed VDP](#) NEW

[Active VDP directory](#) 1,178

[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

[Vulnerability statistics](#)



[Pricing](#)

[Case studies](#)

[Login](#)

[Start trial](#)

[About](#)

[Careers](#)

[Merch store](#)

[Media kit](#)

[LinkedIn](#)

[Facebook](#)

[X](#)

[Report Vulnerability](#)



© Patchstack

[DPA](#)

[Privacy Policy](#)

[Accessibility](#)

[Terms & Conditions](#)