

Pricing

Case studies

Login

Start trial

# WordPress Slide Anything Plugin <= 2.4.9 is vulnerable to a medium priority Cross Site Scripting (XSS)



## Medium priority

Mitigate with Patchstack



## <= 2.4.9

Vulnerable version(s)



## No official patch available

Patched version

WordPress plugin

No VDP

16 Mar, 2023

Get the fastest vulnerability mitigation with Patchstack!

Get started

## Risks CVSS 5.9

This vulnerability is moderately dangerous and expected to become exploited. Vulnerabilities like this one are used in mass-exploit campaigns. Attackers use these

[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.

### **5.9 Cross Site Scripting (XSS)**

This could allow a malicious actor to inject malicious scripts, such as redirects, advertisements, and other HTML payloads into your website which will be executed when guests visit your site.

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

We advise to mitigate or resolve the vulnerability immediately.

### **Automatically mitigate vulnerabilities and keep your websites safe.**

Patchstack has issued a mitigation rule to block any attacks until an official patch becomes available, can be tested and be safely applied.

[Pricing](#)

[Case studies](#)

[Login](#)

[Start trial](#)

[Get started](#)

## Details

Software

Slide Anything

Type

Plugin

Vulnerable versions i

<= 2.4.9

OWASP Top 10 i

A7: Cross-Site Scripting (XSS)

Classification i

Cross Site Scripting (XSS)

CVE ID i

[CVE-2023-28499](#) ↗

Patchstack priority i

Medium

CVSS severity i

5.9

Required privilege i

Author

Developer

[Claim ownership](#) ↗

PSID i

20dca4f988b8

[Pricing](#)

[Case studies](#)

[Login](#)

[Start trial](#)

Published

16 Mar, 2023

[↗ Expand full details](#)

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

Go to

[WordPress plugin](#)

[No VDP](#)

## Timeline



Reported by **RE-ALTER**

NaN undefined, NaN

How can Patchstack provide the fastest protection? ▼

### Vulnerability mitigation

How does Patchstack mitigate vulnerabilities? ▼

[Pricing](#)

[Application security \(SCA\)](#)

Why would a hacker target my website? ▼

[RapidMitigate](#) **NEW**

[Pricing](#)

[Case studies](#)

[Login](#)

[Start trial](#)

[VS Imunify360](#)

[VS Wordfence](#)

[Documentation](#)

[Service status](#)

[Log in](#)

**Weekly WordPress security intelligence delivered to your inbox.**

### Code security

[Managed VDP NEW](#)

[Subscribe](#)

[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](#)

[Pricing](#)

[Case studies](#)

[Login](#)

[Start trial](#)

[Articles](#)

[Case studies](#) NEW

[Webinars](#) NEW

[Vulnerability statistics](#)

## Patchstack

[About](#)

[Careers](#)

[Merch store](#)

[Media kit](#)

[LinkedIn](#)

[Facebook](#)

[X](#)

[Report Vulnerability](#)



© Patchstack

[DPA](#)

[Privacy Policy](#)

[Accessibility](#)

[Terms & Conditions](#)