

# WordPress AMP for WP Plugin <= 1.0.77.31 is vulnerable to Cross Site Scripting (XSS)



**Low priority**

No impactful threat



**<= 1.0.77.31**

Vulnerable version(s)



**1.0.77.32**

Patched version

WordPress plugin

No VDP

11 Dec, 2021

**Get the fastest vulnerability mitigation with Patchstack!**

Get started

## Risks CVSS 4.8

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.

### **4.8 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

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

### **Update to version 1.0.77.32 or later.**

Update to version 1.0.77.32 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

AMP for WP

Type

Plugin

Vulnerable versions i

<= 1.0.77.31

Patched in i

1.0.77.32

OWASP Top 10 i

A7: Cross-Site Scripting (XSS)

Classification i

[Expand full details](#)

Cross Site Scripting (XSS)

CVE ID i

[CVE-2021-23150](#) ↗

Patchstack priority i

Low

CVSS severity i

4.8

Required privilege i

Author


Developer

[Claim ownership](#) ↗

PSID i

b2110da609d7

Credits

 [Nguyen Anh Tien](#)

Published

11 Dec, 2021

[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 [Nguyen Anh Tien](#)

NaN undefined, NaN

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 (AI)

VS Monarx

What if my website has already been compromised? ▼

VS Imunity360

VS Wordfence

Documentation

[Pricing](#)

[Case studies](#)

[Login](#)

[Start trial](#)

### Code security

[Managed Email](#)

[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](#)