

[Pricing](#)

[Case studies](#)

[Login](#)

[Start trial](#)

WordPress Launcher: Coming Soon & Maintenance Mode Plugin <= 1.0.11 is vulnerable to Cross Site Scripting (XSS)



Low priority

No impactful threat



<= 1.0.11


Vulnerable version(s)



No official patch available

Patched version

 WordPress plugin

 No VDP

25 Aug, 2022

Get the fastest vulnerability mitigation with Patchstack!

[Get started](#)

Risks CVSS 4.8

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

[Learn more.](#)

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.

[Pricing](#)

[Case studies](#)

[Login](#)

[Start trial](#)

Software

Launcher: Coming Soon & Maintenance Mode

Type

Plugin

Vulnerable versions ⓘ

<= 1.0.11

OWASP Top 10 ⓘ

A7: Cross-Site Scripting (XSS)

Classification ⓘ

Cross Site Scripting (XSS)

CVE ID ⓘ

[Expand full details](#)

[CVE-2021-36829](#)

Patchstack priority ⓘ

Low

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

CVSS severity ⓘ

4.8

Required privilege ⓘ

Administrator


Developer

[Claim ownership](#)

PSID ⓘ

c11cf9145f3e

Credits

 bugb hunter

Published

25 Aug, 2022

[Pricing](#)

[Case studies](#)

[Login](#)

[Start trial](#)

Timeline



Reported by **bugb hunter**

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

Weekly WordPress security intelligence delivered to your inbox.

VS Imunify360

VS Wordfence



Enter e-mail

Documentation

[Subscribe](#)

Service status

Log in

Code security

Managed VDP NEW

[Pricing](#)

[Case studies](#)

[Login](#)

[Start trial](#)

[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](#)

Patchstack

[About](#)

[Careers](#)

[Pricing](#)

[Case studies](#)

[Login](#)

[Start trial](#)

[LinkedIn](#)

[Facebook](#)

[X](#)

[Report Vulnerability](#)



© Patchstack

[DPA](#)

[Privacy Policy](#)

[Accessibility](#)

[Terms & Conditions](#)