

[Pricing](#)

[Case studies](#)

[Login](#)

[Start trial](#)

WordPress Comment Guestbook Plugin <= 0.8.0 is vulnerable to Cross Site Scripting (XSS)



Low priority

No impactful threat



<= 0.8.0

Vulnerable version(s)



No official patch available

Patched version

WordPress plugin

No VDP

26 Sep, 2022

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.

Details

[Pricing](#)

[Case studies](#)

[Login](#)

[Start trial](#)

Software

Comment Guestbook

Type

Plugin

Vulnerable versions ⁱ

<= 0.8.0

OWASP Top 10 ⁱ

A7: Cross-Site Scripting (XSS)

Classification ⁱ

Cross Site Scripting (XSS)

CVE ID ⁱ

[↗ Expand full details](#)

[CVE-2021-36830 ↗](#)

Patchstack priority ⁱ

Low

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

4.8

Required privilege ⁱ

Administrator


Developer

[Claim ownership ↗](#)

PSID ⁱ

289b122abf17

Credits


 bug hunter

Published

26 Sep, 2022

[Go to](#)

 [WordPress plugin](#)

 [No VDP](#)

[Pricing](#)

[Case studies](#)

[Login](#)

[Start trial](#)



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? ▼

Vulnerability mitigation

[Pricing](#)

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

[RapidMitigate](#) NEW

[Threat Intelligence \(API\)](#)

[VS Monarx](#)

[VS Imunify360](#)

[WordPress](#)

[Documentation](#)

[Service status](#)

[Log in](#)

Code security

[Managed VDP](#) NEW

[Active VDP directory](#) 1,178

Weekly WordPress security intelligence delivered to your inbox.

[Subscribe](#)

[Pricing](#)

[Case studies](#)

[Login](#)

[Start trial](#)

[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](#)

[Merch store](#)

[Pricing](#)

[Case studies](#)

[Login](#)

[Start trial](#)

[Facebook](#)

[X](#)

[Report Vulnerability](#)

 **patchstack**

© Patchstack

[DPA](#)

[Privacy Policy](#)

[Accessibility](#)

[Terms & Conditions](#)