

Pricing

Case studies

Login

Start trial

WordPress Survey Maker Plugin <= 2.0.6 is vulnerable to Cross Site Scripting (XSS)



Low priority

No impactful threat



<= 2.0.6

Vulnerable version(s)



2.0.7

Patched version

WordPress plugin

No VDP

3 Dec, 2021

Get the fastest vulnerability mitigation with Patchstack!

Get started

Risks CVSS 4.7

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.

4.7 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 2.0.7 or later.

Update to version 2.0.7 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	Survey Maker
Type	Plugin
Vulnerable versions 	<= 2.0.6
Patched in 	2.0.7
OWASP Top 10 	A7: Cross-Site Scripting (XSS)
Classification 	Cross Site Scripting (XSS)
CVE ID 	CVE-2021-26256 ↗
Patchstack priority 	Low
CVSS severity 	4.7
Required privilege 	Unauthenticated
Developer	Claim ownership ↗
PSID 	f44bab10e1bf
Credits	 thiennv
Published	3 Dec, 2021

[Pricing](#)

[Case studies](#)


[Login](#)


[Start trial](#)

[↗ Expand full details](#)

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

Go to

 [WordPress plugin](#)

 [No VDP](#)

Timeline



Reported by  [thiennv](#)

NaN undefined, NaN

Vulnerability mitigation


[Pricing](#)

[How can Patchstack \(SaaS\) provide the fastest protection?](#) 


[RapidMitigate NEW](#)

[How does Patchstack \(API\) mitigate vulnerabilities?](#) 

[VS Monarx](#)

[Why would a hacker target my website?](#) 

[VS Wordfence](#)

[What if my website has already been compromised?](#) 

[Documentation](#)

[Pricing](#)

[Case studies](#)

[Login](#)

[Start trial](#)

Code security

[Managed VDP](#) NEW

Weekly WordPress security intelligence delivered to your inbox.

[Active VDP directory](#) 1,178

Security auditing

[Compliance \(GRC\)](#) NEW

[Subscribe](#)

[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](#)