

Pricing

Case studies

Login

Start trial

WordPress Icegram Plugin <= 2.0.2 is vulnerable to Cross Site Scripting (XSS)



Low priority

No impactful threat



<= 2.0.2

Vul



2.0

Pat

We value your privacy

We use cookies to enhance your browsing experience, serve personalised ads or content, and analyse our traffic. By clicking "Accept All", you consent to our use of cookies.

Read more.

Customize

Reject All

Accept All

WordPress plug

17 Aug, 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 an attacker to inject malicious code into the page, which will be executed when the page is rendered.

We value your privacy

We use cookies to enhance your browsing experience, serve personalised ads or content, and analyse our traffic. By clicking "Accept All", you consent to our use of cookies. [Read more.](#)

as redirects,

will be

way but which is not

CVSS score is a way to measure the severity of a vulnerability. It is not ideal for WordPress.

Solutions

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

Update to version 2.0.3 or later.

Update to version 2.0.3 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 Icegram

Type Plugin

Vulnerable versions 📘 <= 2.0.2

Patched in 📘 2.0.3

OWASP Top 10 Scripting (XSS)

Classification 📘 Scripting (XSS)

CVE ID 📘 [CVE-2021-36832](#) ↗

Patchstack priority Low

CVSS severity 📘 4.8

Required privilege 📘 Administrator

Developer [Claim ownership](#) ↗

PSID 📘 5c4871712415

Credits [👤 bugb hunter](#)

Published 17 Aug, 2021

We value your privacy

We use cookies to enhance your browsing experience, serve personalised ads or content, and analyse our traffic. By clicking "Accept All", you consent to our use of cookies.

[Read more.](#)

[Pricing](#)

[Case studies](#)

[Login](#)

[Start trial](#)

[↗ Expand full details](#)

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

Go to

[WordPress](#)

We value your privacy

We use cookies to enhance your browsing experience, serve personalised ads or content, and analyse our traffic. By clicking "Accept All", you consent to our use of cookies.
[Read more.](#)

Timeline

[Reported](#)
NaN undefin

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

We value your privacy

We use cookies to enhance your browsing experience, serve personalised ads or content, and analyse our traffic. By clicking "Accept All", you consent to our use of cookies.

[Read more.](#)



[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](#)

We value your privacy

We use cookies to enhance your browsing experience, serve personalised ads or content, and analyse our traffic. By clicking "Accept All", you consent to our use of cookies.
[Read more.](#)