INTELLIGENCE

As a reminder, the Wordfence Intelligence Vulnerability Database API is completely free to query and utilize, both personally and commercially, and contains all the same vulnerability data as the user interface. Please review the API documentation and Webhook documentation for more information on how to query the vulnerability API endpoints and configure webhooks utilizing all the same data present in the Wordfence Intelligence user interface.

BuddyBoss Platform <= 2.8.50 - Authenticated (Subscriber+) Stored Cross-Site Scripting via 'invitee_name'

6.4

Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N

CVE	CVE-2024-13858
CVSS	6.4 (Medium)
Publicly Published	May 1, 2025
Last Updated	May 2, 2025
Researcher	Kaique Peres

Description

The Buddyboss Platform plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'invitee_name' parameter in all versions up to, and including, 2.8.50 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The vulnerability was partially patched in version 2.8.41.
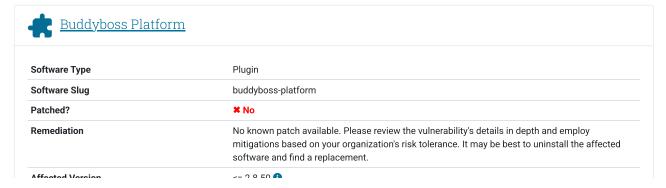
References

- www.buddyboss.com

Share

Facebook   Twitter   LinkedIn   Email

Vulnerability Details for Buddyboss Platform

Buddyboss Platform

Software Type	Plugin
Software Slug	buddyboss-platform
Patched?	✖ No
Remediation	No known patch available. Please review the vulnerability's details in depth and employ mitigations based on your organization's risk tolerance. It may be best to uninstall the affected software and find a replacement.
Affected Version	<= 2.8.50 ⓘ

Have information to add, or spot any errors? Contact us at wfi-support@wordfence.com so we can make any appropriate adjustments.

Did you know Wordfence Intelligence provides free personal and commercial API access to our comprehensive WordPress vulnerability database, along with a free webhook integration to stay on top of the latest vulnerabilities added and updated in the database? Get started today!

Want to get notified of the latest vulnerabilities that may affect your WordPress site?
Install Wordfence on your site today to get notified immediately if your site is affected by a vulnerability that has been added to our database.

The Wordfence Intelligence WordPress vulnerability database is completely free to access and query via API. Please review the documentation on how to access and consume the vulnerability data via API.

LEARN MORE

GET WORDFENCE

DOCUMENTATION

Our business hours are 9am-8pm ET, 6am-5pm PT and 2pm-1am UTC/GMT excluding weekends and holidays.
Response customers receive 24-hour support, 365 days a year, with a 1-hour response time.

Terms of Service

Privacy Policy and Notice at Collection

Products

[Wordfence Free](#)
[Wordfence Premium](#)
[Wordfence Care](#)
[Wordfence Response](#)
[Wordfence CLI](#)
[Wordfence Intelligence](#)
[Wordfence Central](#)

Support

[Documentation](#)
[Learning Center](#)
[Free Support](#)
[Premium Support](#)

News

[Blog](#)
[In The News](#)
[Vulnerability Advisories](#)

About

[About Wordfence](#)
[Affiliate Program](#)
[Careers](#)
[Contact](#)
[Security](#)
[CVE Request Form](#)

Stay Updated

Sign up for news and updates from our panel of experienced security professionals.

you@example.com

☐ By checking this box I agree to the [terms of service](#) and [privacy policy](#).*

SIGN UP

ISO 27001
CERTIFICATION