



Have you found a vulnerability in a WordPress plugin or theme? Report vulnerabilities in WordPress plugins and themes through our [bug bounty program](#) and earn a bounty on all in-scope submissions, while we handle the responsible disclosure process on your behalf.

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.

GmapsMania <= 1.1 - Authenticated (Contributor+) Stored Cross-Site Scripting via Shortcode

[Wordfence Intelligence](#) > [Vulnerability Database](#) > GmapsMania <= 1.1 - Authenticated (Contributor+) Stored Cross-Site Scripting via Shortcode



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-2025-4131
CVSS	6.4 (Medium)
Publicly Published	May 1, 2025
Last Updated	May 2, 2025
Researcher	muhammad.yudha

Description

The GmapsMania plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's gmap shortcode in all versions up to, and including, 1.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.

Wordfence blocked 11 attacks targeting this vulnerability in the past 24 hours.

References

- plugins.trac.wordpress.org

Share

Facebook

Twitter

LinkedIn

Email

Vulnerability Details for GmapsMania

Software Type

Plugin

Software Slug

gmapsmania ([view on wordpress.org](#))

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

<= 1.1 [i](#)

This record contains material that is subject to copyright.

Copyright 2012-2025 Defiant Inc.

License: Defiant hereby grants you a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, sublicense, and distribute this software vulnerability information. Any copy of the software vulnerability information you make for such purposes is authorized provided that you include a hyperlink to this vulnerability record and reproduce Defiant's copyright designation and this license in any such copy. [Read more.](#)

Copyright 1999-2025 The MITRE Corporation

License: CVE Usage: MITRE hereby grants you a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, sublicense, and distribute Common Vulnerabilities and Exposures (CVE®). Any copy you make for such purposes is authorized provided that you reproduce MITRE's copyright designation and this license in any such copy. [Read more.](#)

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!

[LEARN MORE](#)

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.

[GET WORDFENCE](#)

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.

[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](#)

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

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

SIGN UP

© 2012-2025 Defiant Inc. All Rights Reserved

