



🦋👻 Calling all superheroes and haunters! Introducing the **Cybersecurity Month Spooktacular Haunt** and the **WordPress Superhero Challenge** for the **Wordfence Bug Bounty Program**! Through November 11th, 2024, all in-scope vulnerability types for WordPress plugins/themes with **>= 1,000 active installations** are in-scope for **ALL researchers**, top-tier researchers earn **automatic bonuses of between 10% to 120%** for valid submissions, pending report limits are increased for all, and it's possible to **earn up to \$31,200** for high impact vulnerabilities!

[Review what's in scope for your tier and updated bounties with bonuses here!](#)

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.

User Meta – User Profile Builder and User management plugin <= 3.1 - Insecure Direct Object Reference to Sensitive Information Exposure

[Wordfence Intelligence](#) > [Vulnerability Database](#) > User Meta – User Profile Builder and User management plugin <= 3.1 - Insecure Direct Object Reference to Sensitive Information Exposure



Authorization Bypass Through User-Controlled Key

[CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N](#)

CVE	CVE-2024-9262
CVSS	6.5 (Medium)
Publicly Published	November 8, 2024
Last Updated	November 9, 2024
Researcher	wesley (wcraft)

Description

The User Meta – User Profile Builder and User management plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 3.1 via the `getUser()` due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with Contributor-level access and above, to obtain user meta values from form fields. Please note that this requires a site administrator to create a form that displays potentially sensitive information like password hashes. This may also be exploited by unauthenticated users if the 'user-meta-public-profile' shortcode is used insecurely.

References

- [plugins.trac.wordpress.org](#)

Share

Facebook

Twitter

LinkedIn

Email

Vulnerability Details for User Meta – User Profile Builder and User management plugin



[User Meta – User Profile Builder and User management plugin](#)

management, or your organization's vulnerability management process to identify the software and find a replacement.

Affected Version<= 3.1 

This record contains material that is subject to copyright.

Copyright 2012-2024 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 1999-2024 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](#)

Stay Updated

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

you@example.com

[SIGN UP](#)

© 2012-2024 Defiant Inc. All Rights Reserved

