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 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

Software Slug	user-meta (view on wordpress.org)
	software and find a replacement.
Affected Version	<= 3.1

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

you@example.com

SIGN UP