INTELLIGENCE

🦸 🧭 Calling all superheroes and explorers! Introducing the WordPress Superhero Challenge and WordPress XSSplorer Challenge for the **Wordfence Bug Bounty Program**: **Earn up to $31,200** for High Impact Vulnerabilities AND XSS vulnerabilities are in scope for all researchers in plugins/themes >= 1,000 Active Installs!

Through October 7th, 2024 all Cross-Site Scripting (XSS) vulnerabilities in plugins/themes with >= 1,000 Active Installs will be in scope for all researchers regardless of researcher tier. In addition, through October 14th, 2024, all vulnerabilities reported in plugins or themes with >= 5,000,000 active installs will be 3x our highest bounty rewards making our top reward $31,200.

Check out the **updated bounties 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.

Wechat Social login <= 1.3.0 - Authentication Bypass

Authentication Bypass Using an Alternate Path or Channel

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

CVE	CVE-2024-9106
CVSS	9.8 (Critical)
Publicly Published	September 30, 2024
Last Updated	October 1, 2024
Researcher	István Márton - Wordfence

Description

The Wechat Social login plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 1.3.0. This is due to insufficient verification on the user being supplied during the social login. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the user id. This is only exploitable if the app secret is not set, so it has a default empty value.

References

- plugins.trac.wordpress.org

Share

Facebook Twitter LinkedIn Email

Vulnerability Details for Wechat Social login 微信QQ钉钉登录插件

Wechat Social login 微信QQ钉钉登录插件

Software Type	Plugin
Software Slug	wechat-social-login (view on wordpress.org)
Patched?	✖ No

This site uses cookies in accordance with our Privacy Policy.

Cookie Settings ACCEPT ALL

Affected Version	<= 1.3.0

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.

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

This site uses cookies in accordance with our Privacy Policy.

This site uses cookies in accordance with our Privacy Policy.