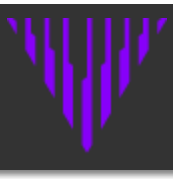

VDB-356992 · CVE-2026-6129 · ISSUE 2741

ZHAYUJIE CHATGPT-ON-WECHAT COWAGENT UP TO 2.0.4 AGENT MODE SERVICE MISSING AUTHENTICATION

CVSS Meta Temp Score ? | Current Exploit Price (≈) ? | CTI Interest Score ?

6.4 | $0-$5k | 3.10-

Summary

A vulnerability was found in zhayujie chatgpt-on-wechat CowAgent up to 2.0.4. It has been declared as critical. This impacts an unknown function of the component *Agent Mode Service*. Executing a manipulation can lead to missing authentication. This vulnerability is tracked as CVE-2026-6129. The attack can be launched remotely. Moreover, an exploit is present. The application of restrictive firewalling is recommended. The project was informed of the problem early through an issue report but has not responded yet.

Details

A vulnerability was found in zhayujie chatgpt-on-wechat CowAgent up to 2.0.4. It has been declared as critical. This vulnerability affects some unknown processing of the component *Agent Mode Service*. The manipulation with an unknown input leads to a missing authentication vulnerability. The CWE definition for the vulnerability is CWE-306. The product does not perform any authentication for functionality that requires a provable user identity or consumes a significant amount of resources. As an impact it is known to affect confidentiality, integrity, and availability.

The advisory is shared for download at github.com. This vulnerability was named CVE-2026-6129. The exploitation appears to be easy. The attack can be initiated remotely. No form of authentication is required for a successful exploitation. Technical details are unknown but a public exploit is available.

It is possible to download the exploit at github.com. It is declared as proof-of-concept. The project was informed of the problem early through an issue report but has not responded yet.

Proper firewalling of is able to address this issue.

Product

Type

- Chat Software

Vendor

- zhayujie

Name

- chatgpt-on-wechat CowAgent

Version

- 2.0.0
- 2.0.1
- 2.0.2
- 2.0.3
- 2.0.4

CPE 2.3

- 🔒
- 🔒
- 🔒

CPE 2.2

- 🔒
- 🔒
- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv3

VulDB Meta Base Score: 7.3
VulDB Meta Temp Score: 6.4

VulDB Base Score: 7.3
VulDB Temp Score: 6.4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv2

VulDB Base Score: 🔒
VulDB Temp Score: 🔒
VulDB Reliability: 🔍

Exploiting

Class: Missing authentication
CWE: CWE-306 / CWE-287
CAPEC: 🔒
ATT&CK: 🔒

Physical: No
Local: No
Remote: Yes

Availability: 🔒
Access: Public
Status: Proof-of-Concept
Download: 🔒
Price Prediction: 🔍
Current Price Estimation: 🔒

Threat Intelligence

Interest: 🔍
Active Actors: 🔍

Active APT Groups: 🔍

Countermeasures

Recommended: Firewall
Status: 🔍

0-Day Time: 🔒

Timeline

04/12/2026		Advisory disclosed
04/12/2026	+0 days	VulDB entry created
04/12/2026	+0 days	VulDB entry last update

Sources

Advisory: 2741
Status: Not defined

CVE: CVE-2026-6129 (🔒)
GCVE (CVE): GCVE-0-2026-6129
GCVE (VulDB): GCVE-100-356992
scip Labs: https://www.scip.ch/en/?labs.20161013

Entry

Created: 04/12/2026 06:28 AM
Changes: 04/12/2026 06:28 AM (58)
Complete: 🔍
Submitter: York Shen
Cache ID: 172:3A7:179

Submit

Accepted

- Submit #795272: zhayujie chatgpt-on-wechat (CowAgent) 2.0.4 Unauthenticated Remote Code Execution (by York Shen)

Discussion

No comments yet. Languages: en.

Please log in to comment.