

VDB-356990 · CVE-2026-6126 · ISSUE 2733

# ZHAYUJIE CHATGPT-ON-WECHAT COWAGENT 2.0.4 ADMINISTRATIVE HTTP ENDPOINT MISSING AUTHENTICATION

CVSS Meta Temp Score ⓘ

6.4

Current Exploit Price (≈) ⓘ

\$0-\$5k

CTI Interest Score ⓘ

2.93-

## Summary

A vulnerability was found in [zhayujie chatgpt-on-wechat CowAgent 2.0.4](#) and classified as **critical**. The impacted element is an unknown function of the component *Administrative HTTP Endpoint*. Such manipulation leads to missing authentication. This vulnerability is referenced as [CVE-2026-6126](#). It is possible to launch the attack remotely. Furthermore, an exploit is available. Restrictive firewalling should be applied. 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 2.0.4](#) and classified as **critical**. Affected by this issue is an unknown code of the component *Administrative HTTP Endpoint*. The manipulation with an unknown input leads to a missing authentication vulnerability. Using CWE to declare the problem leads to [CWE-306](#). The product does not perform any authentication for functionality that requires a provable user identity or consumes a significant amount of resources. Impacted is confidentiality, integrity, and availability.

The advisory is available at [github.com](#). This vulnerability is handled as [CVE-2026-6126](#). The exploitation is known to be easy. The attack may be launched remotely. No form of authentication is required for exploitation. Technical details are unknown but a public exploit is available.

The exploit is available 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.

Addressing this vulnerability is possible by firewalling .

Similar entry is available at [VDB-249545](#).

## Product

### Type

- [Chat Software](#)

### Vendor

- [zhayujie](#)

### Name

- [chatgpt-on-wechat CowAgent](#)

### Version

- [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

04/11/2026		Advisory disclosed
04/11/2026	+0 days	VulDB entry created
04/11/2026	+0 days	VulDB entry last update

## Sources

Advisory: 2733

Status: Not defined

CVE: CVE-2026-6126 (🔒)

GCVE (CVE): GCVE-0-2026-6126

GCVE (VulDB): GCVE-100-356990

scip Labs: <https://www.scip.ch/en/?labs.20161013>

See also: 🔒

## Entry

Created: 04/11/2026 10:27 PM

Changes: 04/11/2026 10:27 PM (58)

Complete: 🔍

Submitter: Yu\_Bao

Cache ID: 172:19D:179

## Submit

### Accepted

- [Submit #793554](#): zhayujie chatgpt-on-wechat (CowAgent) 2.0.4 Unauthenticated Administrative API Access (by Yu\_Bao)

### Duplicate

- 

## Discussion

No comments yet. Languages: en.

[Please log in to comment.](#)