COMMUNITY CONTENT

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

Title zhayujie chatgpt-on-wechat (CowAgent) 2.0.4 Unauthenticated Remote Code Execution

Description chatgpt-on-wechat (CowAgent) is an open-source AI Agent framework with 16.4k+ GitHub stars that provides LLM-powered assistants for WeChat, Feishu, DingTalk, and other messaging platforms. In Agent mode (enabled by default since v2.0.0), the application grants the AI agent access to system-level tools including a bash shell, file read/write, and web fetch capabilities. This is the application's intended functionality — the Agent is designed to operate the computer on behalf of the user.
However, the Web Console that controls this Agent is exposed on x.x.x.x:9899 with zero authentication on all endpoints, including the /message endpoint that accepts chat messages. This means any unauthenticated remote attacker who can reach port 9899 can send instructions to the AI Agent, which will then execute OS commands, read/write files, and access network resources on the attacker's behalf.
The root cause is not the bash tool itself (which is working as designed), but the complete absence of authentication on the Web Console that exposes these powerful capabilities to the network.

Source https://github.com/zhayujie/chatgpt-on-wechat/issues/2741

User York Shen (UID 97025)

Submission 04/02/2026 08:03 AM (11 days ago)

Moderation 04/12/2026 06:23 AM (10 days later)

Status Published

VulDB entry [zhayujie chatgpt-on-wechat CowAgent up to 2.0.4 Agent Mode Service missing authentication]

Points 20

Community Content

Submissions are made by VulDB community users. VulDB is *not responsible* for their content nor the links to external sources.

Please use the raw information shown and the links listed *with caution*. They might contain malicious and harmful actions, code or data.

The corresponding VulDB entries contain the moderated, verified, and normalized information provided within the raw submission.

Documentation

- Submission Policy
- Data Processing
- CVE Handling