



Home > Submit > 795335

Submit #795335: zhayujie chatgpt-on-wechat (CowAgent) 2.0.4 Unauthenticated Channel Credential Injection

Title zhayujie chatgpt-on-wechat (CowAgent) 2.0.4 Unauthenticated Channel Credential Injection

Description The POST /api/channels endpoint in chatgpt-on-wechat v2.0.4 Web Console allows an unauthenticated remote attacker to:

- Inject arbitrary channel credentials (Feishu App Secret, DingTalk Client Secret, WeCom Secret, QQ App Secret, WeChat MP App Secret, AES Keys, Verification Tokens) into the application's config.json via the save action.
- Activate new messaging channels and start network services on the server (binding to attacker-specified ports) via the connect action.

Both actions persist changes to disk and require zero authentication. This is a distinct vulnerability from the known /config POST endpoint (which writes to a different set of keys like open_at_api_key and model).

Source <https://github.com/zhayujie/chatgpt-on-wechat/issues/2742>

User York Shen (UID: 97025)

Submission 04/03/2026 10:06 AM (11 days ago)

Moderation 04/12/2026 06:27 AM (10 days later)

Status Pending

VulDB entry [\[zhayujie chatgpt-on-wechat CowAgent 2.0.4 Administrative HTTP Endpoint missing authentication\]](#)

Points 0

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](#)