



[Home](#) > [Submit](#) > [785591](#) 

# Submit #785591: ChrisChinchilla Vale-MCP 0.1.0 Command Injection

**Title** ChrisChinchilla Vale-MCP 0.1.0 Command Injection

**Description** A command injection vulnerability (CWE-78) has been identified in vale-mcp, specifically within the vale-runner.ts component. An attacker with network access to the MCP/HTTP interface can supply maliciously crafted input through the config\_path or other tool arguments, which flows unsanitized into OS command execution via exec or execAsync. This allows arbitrary system commands to be executed with the privileges of the server process, leading to full host compromise, including data exposure, integrity loss, and potential service disruption. Versions up to and including 0.1.0 are confirmed affected.

**Source**  [https://github.com/wing3e/public\\_exp/issues/27](https://github.com/wing3e/public_exp/issues/27)

**User**  BruceJin (UID 96538)

**Submission** 03/22/2026 02:50 PM (15 days ago)

**Moderation** 04/05/2026 06:01 PM (14 days later)

**Status** Accepted

**VulDB entry** 355411 [ChrisChinchilla Vale-MCP up to 0.1.0 HTTP Interface src/index.ts config\_path os command injection]

**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](#)