VDB-355411 · CVE-2026-5621 · GCVE-100-355411

CHRISCHINCHILLA VALE-MCP UP TO 0.1.0 HTTP INTERFACE SRC/INDEX.TS CONFIG_PATH OS COMMAND INJECTION

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
4.8	$0-$5k	2.23-

Summary

A vulnerability was found in ChrisChinchilla Vale-MCP up to 0.1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file *src/index.ts* of the component *HTTP Interface*. This manipulation of the argument *config_path* causes os command injection. This vulnerability is handled as CVE-2026-5621. It is possible to launch the attack on the local host. Additionally, an exploit exists. The vendor was contacted early about this disclosure but did not respond in any way.

Details

A vulnerability classified as critical was found in ChrisChinchilla Vale-MCP up to 0.1.0. Affected by this vulnerability is an unknown function of the file *src/index.ts* of the component *HTTP Interface*. The manipulation of the argument `config_path` with an unknown input leads to a os command injection vulnerability. The CWE definition for the vulnerability is CWE-78. The product constructs all or part of an OS command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended OS command when it is sent to a downstream component. As an impact it is known to affect confidentiality, integrity, and availability.

It is possible to read the advisory at github.com. This vulnerability is known as CVE-2026-5621. The exploitation appears to be easy. Attacking locally is a requirement. Technical details and also a public exploit are known. The attack technique deployed by this issue is T1202 according to MITRE ATT&CK.

It is possible to download the exploit at github.com. It is declared as proof-of-concept. The vendor was contacted early about this disclosure but did not respond in any way.

There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.

Entries connected to this vulnerability are available at VDB-169422, VDB-222729, VDB-344765 and VDB-348559.

Product

Type

- Artificial Intelligence Software

Vendor

- ChrisChinchilla

Name

- Vale-MCP

Version

- 0.1.0

CPE 2.3

- 🔒

CPE 2.2

- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv3

VulDB Meta Base Score: 5.3
VulDB Meta Temp Score: 4.8

VulDB Base Score: 5.3
VulDB Temp Score: 4.8
VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv2

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

Exploiting

Class: Os command injection
CWE: CWE-78 / CWE-77 / CWE-74
CAPEC: 🔒
ATT&CK: 🔒

Physical: Partially
Local: Yes
Remote: No

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

Threat Intelligence

Interest: 🔍
Active Actors: 🔍
Active APT Groups: 🔍

Countermeasures

Recommended: no mitigation known
Status: 🔍

0-Day Time: 🔒

Timeline

04/05/2026		Advisory disclosed
04/05/2026	+0 days	VulDB entry created
04/05/2026	+0 days	VulDB entry last update

Sources

Advisory: github.com
Status: Not defined

CVE: CVE-2026-5621 (🔒)
GCVE (CVE): GCVE-0-2026-5621
GCVE (VulDB): GCVE-100-355411
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 04/05/2026 06:06 PM
Changes: 04/05/2026 06:06 PM (57)
Complete: 🔍
Submitter: BruceJin
Cache ID: 40:81B:179

Submit

Accepted

- Submit #785591: ChrisChinchilla Vale-MCP 0.1.0 Command Injection (by BruceJin)

Discussion

No comments yet. Languages: en.

Please log in to comment.