VDB-355385 · CVE-2026-5586 · GCVE-100-355385

ZHONGYU09 OPENCHATBI UP TO 0.2.1 MULTI-STAGE TEXT2SQL WORKFLOW KEYWORDS SQL INJECTION

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
5.7	$0-$5k	3.09-

Summary

A vulnerability identified as critical has been detected in zhongyu09 openchatbi up to 0.2.1. This affects an unknown function of the component *Multi-stage Text2SQL Workflow*. The manipulation of the argument *keywords* leads to sql injection. This vulnerability is referenced as CVE-2026-5586. Remote exploitation of the attack is possible. Furthermore, an exploit is available. The vendor was contacted early about this disclosure but did not respond in any way.

Details

A vulnerability, which was classified as critical, has been found in zhongyu09 openchatbi up to 0.2.1. This issue affects some unknown functionality of the component *Multi-stage Text2SQL Workflow*. The manipulation of the argument `keywords` with an unknown input leads to a sql injection vulnerability. Using CWE to declare the problem leads to CWE-89. The product constructs all or part of an SQL command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended SQL command when it is sent to a downstream component. Impacted is confidentiality, integrity, and availability.

The advisory is shared at github.com. The identification of this vulnerability is CVE-2026-5586. The exploitation is known to be easy. The attack may be initiated remotely. Technical details as well as a public exploit are known. MITRE ATT&CK project uses the attack technique T1505 for this issue.

The exploit is available 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.

Similar entries are available at VDB-273748, VDB-285985, VDB-290788 and VDB-302053.

Product

Vendor

- zhongyu09

Name

- openchatbi

Version

- 0.2.0
- 0.2.1

CPE 2.3

- 🔒
- 🔒

CPE 2.2

- 🔒
- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv3

VulDB Meta Base Score: 6.3
VulDB Meta Temp Score: 5.7

VulDB Base Score: 6.3
VulDB Temp Score: 5.7
VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv2

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

Exploiting

Class: Sql injection
CWE: CWE-89 / CWE-74 / CWE-707
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: no mitigation known
Status: 🔍

0-Day Time: 🔒

Timeline

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

Sources

Advisory: github.com
Status: Not defined

CVE: CVE-2026-5586 (🔒)
GCVE (CVE): GCVE-0-2026-5586
GCVE (VulDB): GCVE-100-355385
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 04/04/2026 11:47 PM
Changes: 04/04/2026 11:47 PM (56)
Complete: 🔍
Submitter: Goku
Cache ID: 172:63D:179

Submit

Accepted

- Submit #784454: openchatbi v0.2.1 SQL Injection (by Goku)

Discussion

No comments yet. Languages: en.

Please log in to comment.