VDB-354654 · CVE-2026-5322 · GCVE-100-354654

# ALEJANDROARCINIEGAS MCP-DATA-VIS MCP SERVER.JS REQUEST SQL INJECTION

CVSS Meta Temp Score | Current Exploit Price (≈) | CTI Interest Score

6.6 | $0-$5k | 1.10

## Summary

A vulnerability was found in AlejandroArciniegas mcp-data-vis bc597e391f184d2187062fd567599a3cb72adf51/de5a51525a69822290eaee569a1ab447b490746d. It has been declared as critical. This vulnerability affects the function `Request` of the file *src/servers/database/server.js* of the component *MCP Handler*. The manipulation results in sql injection. This vulnerability is cataloged as CVE-2026-5322. The attack may be launched remotely. Furthermore, there is an exploit available. This product operates on a rolling release basis, ensuring continuous delivery. Consequently, there are no version details for either affected or updated releases. The vendor was contacted early about this disclosure but did not respond in any way.

## Details

A vulnerability classified as critical has been found in AlejandroArciniegas mcp-data-vis bc597e391f184d2187062fd567599a3cb72adf51/de5a51525a69822290eaee569a1ab447b490746d. Affected is the function `request` of the file *src/servers/database/server.js* of the component *MCP Handler*. The manipulation with an unknown input leads to a sql injection vulnerability. CWE is classifying the issue as 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. This is going to have an impact on confidentiality, integrity, and availability.

The advisory is available at github.com. This vulnerability is traded as CVE-2026-5322. The exploitability is told to be easy. It is possible to launch the attack remotely. The exploitation doesn't require any form of authentication. Technical details and a public exploit are known. This vulnerability is assigned to T1505 by the MITRE ATT&CK project.

The exploit is shared for download 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.

The entries VDB-107880, VDB-108727, VDB-120100 and VDB-266579 are related to this item.

## Product

### Vendor

- AlejandroArciniegas

### Name

- mcp-data-vis

### Version

- bc597e391f184d2187062fd567599a3cb72adf51
- de5a51525a69822290eaee569a1ab447b490746d

## CPE 2.3

- 🔒

## CPE 2.2

- 🔒

## CVSSv4

**VulDB Vector**: 🔒
**VulDB Reliability**: 🔍

## CVSSv3

**VulDB Meta Base Score**: 7.3
**VulDB Meta Temp Score**: 6.6

**VulDB Base Score**: 7.3
**VulDB Temp Score**: 6.6
**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

| | | |
|---|---|---|
| **04/01/2026** | | Advisory disclosed |
| **04/01/2026** | +0 days | VulDB entry created |
| **04/01/2026** | +0 days | VulDB entry last update |

## Sources

**Advisory**: github.com
**Status**: Not defined

**CVE**: CVE-2026-5322 (🔒)
**GCVE (CVE)**: GCVE-0-2026-5322
**GCVE (VulDB)**: GCVE-100-354654
**scip Labs**: https://www.scip.ch/en/?labs.20161013
**See also**: 🔒

## Entry

**Created**: 04/01/2026 03:08 PM
**Changes**: 04/01/2026 03:08 PM (58)
**Complete**: 🔍
**Submitter**: BigW
**Cache ID**: 40:3DF:179

## Submit

**Accepted**

- Submit #780731: AlejandroArciniegas mcp-data-vis 1.0.0 SQL Injection (by BigW)

## Discussion

No comments yet. Languages: en.

Please log in to comment.