VDB-355409 · CVE-2026-5619 · GCVE-100-355409

BRAFFOLK MCP-SUMMARIZATION-FUNCTIONS UP TO 0.1.5 SUMMARIZE_COMMAND SRC/SERVER/MCP-SERVER.TS OS COMMAND INJECTION

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
4.8	$0-$5k	2.60-

Summary

A vulnerability was found in Braffolk mcp-summarization-functions up to 0.1.5. It has been classified as critical. Affected is an unknown function of the file *src/server/mcp-server.ts* of the component *summarize_command*. The manipulation of the argument *command* leads to os command injection. This vulnerability is traded as CVE-2026-5619. An attack has to be approached locally. Furthermore, there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.

Details

A vulnerability was found in Braffolk mcp-summarization-functions up to 0.1.5. It has been rated as critical. This issue affects an unknown code block of the file *src/server/mcp-server.ts* of the component *summarize_command*. The manipulation of the argument `command` with an unknown input leads to a os command injection vulnerability. Using CWE to declare the problem leads to 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. Impacted is confidentiality, integrity, and availability.

The advisory is shared at github.com. The identification of this vulnerability is CVE-2026-5619. The exploitation is known to be easy. An attack has to be approached locally. Technical details as well as a public exploit are known. MITRE ATT&CK project uses the attack technique T1202 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.

Product

Type

- Artificial Intelligence Software

Vendor

- Braffolk

Name

- mcp-summarization-functions

Version

- 0.1.0
- 0.1.1
- 0.1.2
- 0.1.3
- 0.1.4
- 0.1.5

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-2026-5619 (🔒)
GCVE (CVE): GCVE-0-2026-5619
GCVE (VulDB): GCVE-100-355409
scip Labs: https://www.scip.ch/en/?labs.20161013

Entry

Created: 04/05/2026 06:02 PM
Changes: 04/05/2026 06:02 PM (57)
Complete: 🔍
Submitter: BruceJin
Cache ID: 172:428:179

Submit

Accepted

- Submit #785574: Braffolk mcp-summarization-functions 0.1.5 Command Injection (by BruceJin)

Discussion

No comments yet. Languages: en.

Please log in to comment.