VDB-356978 · CVE-2026-6118 · ISSUE 7169

ASTRBOTDEVS ASTRBOT UP TO 4.22.1 MCP ENDPOINT TOOLS.PY ADD_MCP_SERVER COMMAND COMMAND INJECTION

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

5.7 | $0-$5k | 2.31

Summary

A vulnerability was found in AstrBotDevs AstrBot up to 4.22.1. It has been declared as critical. The affected element is the function `add_mcp_server` of the file *astrbot/dashboard/routes/tools.py* of the component *MCP Endpoint*. Such manipulation of the argument *command* leads to command injection. This vulnerability is listed as CVE-2026-6118. The attack may be performed from remote. In addition, an exploit is available. The project was informed of the problem early through an issue report but has not responded yet.

Details

A vulnerability, which was classified as critical, has been found in AstrBotDevs AstrBot up to 4.22.1. Affected by this issue is the function `add_mcp_server` of the file *astrbot/dashboard/routes/tools.py* of the component *MCP Endpoint*. The manipulation of the argument `command` with an unknown input leads to a command injection vulnerability. Using CWE to declare the problem leads to CWE-77. The product constructs all or part of a command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended command when it is sent to a downstream component. Impacted is confidentiality, integrity, and availability.

The advisory is available at github.com. This vulnerability is handled as CVE-2026-6118. The exploitation is known to be easy. The attack may be launched remotely. Technical details as well as a public exploit are known. This vulnerability is assigned to T1202 by the MITRE ATT&CK project.

The exploit is available at github.com. It is declared as proof-of-concept. The project was informed of the problem early through an issue report but has not responded yet.

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

See VDB-342303, VDB-342669, VDB-347262 and VDB-348829 for similar entries.

Product

Vendor

- AstrBotDevs

Name

- AstrBot

Version

- 4.22.0
- 4.22.1

Website

- Product: https://github.com/AstrBotDevs/AstrBot/

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: Command injection
CWE: CWE-77 / 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

04/11/2026		Advisory disclosed
04/11/2026	+0 days	VulDB entry created
04/11/2026	+0 days	VulDB entry last update

Sources

Product: github.com

Advisory: 7169
Status: Not defined

CVE: CVE-2026-6118 (🔒)
GCVE (CVE): GCVE-0-2026-6118
GCVE (VulDB): GCVE-100-356978
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 04/11/2026 10:55 AM
Changes: 04/11/2026 10:55 AM (59)
Complete: 🔍
Submitter: Yu_Bao
Cache ID: 40:AE8:179

Submit

Accepted

- Submit #792655: AstrBotDevs AstrBot 4.22.1 Arbitrary Command Execution (by Yu_Bao)

Discussion

No comments yet. Languages: en.

Please log in to comment.