VDB-356979 · CVE-2026-6119 · ISSUE 7171

ASTRBOTDEVS ASTRBOT UP TO 4.22.1 API ENDPOINT POST_DATA.GET SERVER-SIDE REQUEST FORGERY

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
5.7	$0-$5k	2.50-

Summary

A vulnerability was found in AstrBotDevs AstrBot up to 4.22.1. It has been rated as critical. The impacted element is the function `post_data.get` of the component *API Endpoint*. Performing a manipulation results in server-side request forgery. This vulnerability is cataloged as CVE-2026-6119. It is possible to initiate the attack remotely. Furthermore, there is an exploit 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, was found in AstrBotDevs AstrBot up to 4.22.1. This affects the function `post_data.get` of the component *API Endpoint*. The manipulation with an unknown input leads to a server-side request forgery vulnerability. CWE is classifying the issue as CWE-918. The web server receives a URL or similar request from an upstream component and retrieves the contents of this URL, but it does not sufficiently ensure that the request is being sent to the expected destination. This is going to have an impact on confidentiality, integrity, and availability.

It is possible to read the advisory at github.com. This vulnerability is uniquely identified as CVE-2026-6119. The exploitability is told to be easy. It is possible to initiate the attack remotely. Technical details and a public exploit are known.

The exploit is shared for download 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.

The entries VDB-355018, VDB-355192, VDB-355204 and VDB-355831 are related to this item.

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: Server-side request forgery
CWE: CWE-918
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: 7171
Status: Not defined

CVE: CVE-2026-6119 (🔒)
GCVE (CVE): GCVE-0-2026-6119
GCVE (VulDB): GCVE-100-356979
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 (57)
Complete: 🔍
Submitter: Yu_Bao
Cache ID: 68:FAE:179

Submit

Accepted

- Submit #792661: AstrBotDevs AstrBot 4.22.1 Server-Side Request Forgery (SSRF) (by Yu_Bao)

Discussion

No comments yet. Languages: en.

Please log in to comment.