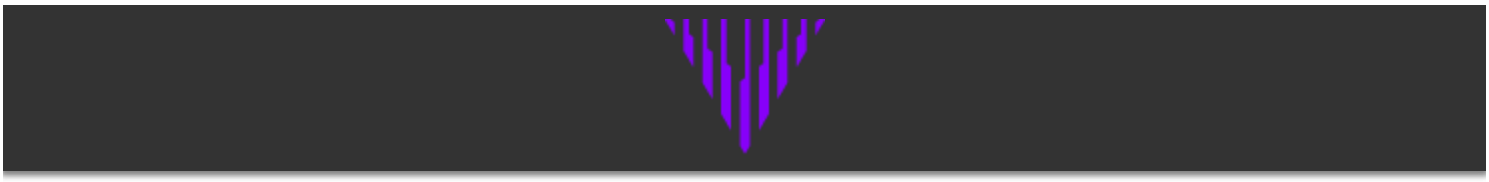

VDB-356977 · CVE-2026-6117 · ISSUE 7168

ASTRBOTDEVS ASTRBOT UP TO 4.22.1 INSTALL-UPLOAD ENDPOINT PLUGIN.PY INSTALL_PLUGIN_UPLOAD FILE SANDBOX

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
5.7	$0-$5k	2.40-

Summary

A vulnerability was found in AstrBotDevs AstrBot up to 4.22.1. It has been classified as critical. Impacted is the function `install_plugin_upload` of the file *astrbot/dashboard/routes/plugin.py* of the component *install-upload Endpoint*. This manipulation of the argument *File* causes sandbox. This vulnerability is tracked as CVE-2026-6117. The attack is possible to be carried out remotely. Moreover, an exploit is present. The project was informed of the problem early through an issue report but has not responded yet.

Details

A vulnerability classified as critical was found in AstrBotDevs AstrBot up to 4.22.1. Affected by this vulnerability is the function `install_plugin_upload` of the file *astrbot/dashboard/routes/plugin.py* of the component *install-upload Endpoint*. The manipulation of the argument `file` with an unknown input leads to a sandbox vulnerability. The CWE definition for the vulnerability is CWE-265. As an impact it is known to affect confidentiality, integrity, and availability.

The advisory is shared at github.com. This vulnerability is known as CVE-2026-6117. The exploitation appears to be easy. The attack can be launched remotely. Technical details and also a public exploit are known. MITRE ATT&CK project uses the attack technique T1611 for this issue.

It is possible to download the exploit 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-351145, VDB-352365, VDB-352404 and VDB-352422 are pretty similar.

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: Sandbox
CWE: CWE-265 / CWE-264
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: 7168
Status: Not defined

CVE: CVE-2026-6117 (🔒)
GCVE (CVE): GCVE-0-2026-6117
GCVE (VulDB): GCVE-100-356977
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: 74:515:179

Submit

Accepted

- Submit #792653: AstrBotDevs AstrBot 4.22.1 Arbitrary Code Execution via Plugin Upload (by Yu_Bao)

Discussion

No comments yet. Languages: en.

Please log in to comment.