



# CVE-2025-55449

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2025-55449   |
| <b>State</b>           | PUBLISHED  |
| <b>Assigner</b>        | mitre  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback   |
| <b>Published</b>       | 2026-05-08 07:16:28 UTC  |
| <b>Updated</b>         | 2026-05-08 07:16:28 UTC  |
| <b>Description</b>     | AstrBotDevs AstrBot 3.5.15 has Advanced_System_for_Text_Response_and_Bot_Operations_Tool as the hardcoded priv |

## Risk And Classification

**Problem Types:** n/a

## Vendor Declared Affected Products

| Source | Vendor | Product | Version      | Platforms     |
|--------|--------|---------|--------------|---------------|
| CNA    | Na     | N/a     | affected n/a | Not specified |

## References

| Reference                                      | Source        | Link                         | Tags                |
|--|---------------|------------------------------|---------------------|
| github.com/AstrBotDevs/AstrBot                 | cve@mitre.org | <a href="#">github.com</a>   |                     |
| github.com/Marven11/CVE-2025-55449-AstrBot-RCE | cve@mitre.org | <a href="#">github.com</a>   |                     |
| CVE Program record                             | CVE.ORG       | <a href="#">www.cve.org</a>  | canonical           |
| NVD vulnerability detail                       | NVD           | <a href="#">nvd.nist.gov</a> | canonical, analysis |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)