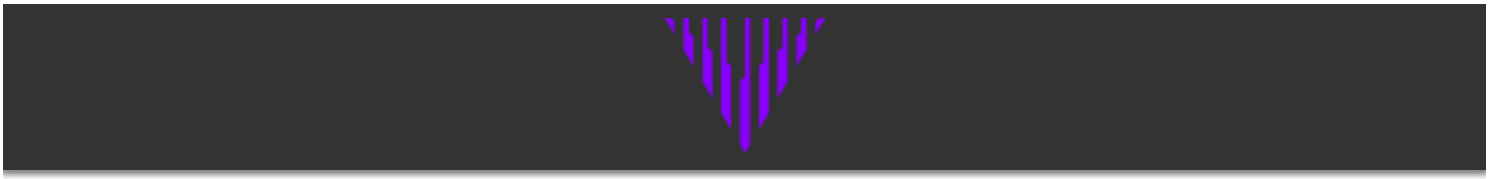

VDB-354655 · CVE-2026-5323 · GCVE-100-354655

PRIYANKARK A11Y-MCP UP TO 1.0.5 SRC/INDEX.JS A11YSERVER SERVER-SIDE REQUEST FORGERY

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

4.1 | $0-$5k | 2.95-

Summary

A vulnerability was found in priyankark a11y-mcp up to 1.0.5. It has been rated as critical. This issue affects the function `A11yServer` of the file *src/index.js*. This manipulation causes server-side request forgery. This vulnerability is registered as CVE-2026-5323. The attack needs to be launched locally. Furthermore, an exploit is available. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided. Upgrading the affected component is advised. The vendor acknowledged the issue but provides additional context for the CVSS rating: "a11y-mcp is a local stdio MCP server - it has no HTTP endpoint and is not network-accessible. The caller is always the local user or an LLM acting on their behalf with user approval."

Details

A vulnerability classified as critical was found in priyankark a11y-mcp up to 1.0.5. Affected by this vulnerability is the function `A11yServer` of the file *src/index.js*. The manipulation with an unknown input leads to a server-side request forgery vulnerability. The CWE definition for the vulnerability is 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. As an impact it is known to affect confidentiality, integrity, and availability.

It is possible to read the advisory at github.com. This vulnerability is known as CVE-2026-5323. The exploitation appears to be easy. Attacking locally is a requirement. Technical details and also a public exploit are known.

It is possible to download the exploit at github.com. It is declared as proof-of-concept. The vendor acknowledged the issue but provides additional context for the CVSS rating: "a11y-mcp is a local stdio MCP server - it has no HTTP endpoint and is not network-accessible. The caller is always the local user or an LLM acting on their behalf with user approval."

Upgrading to version 1.0.6 eliminates this vulnerability. Applying the patch e3e11c9e8482bd06b82fd9fced67be4856f0dffc is able to eliminate this problem. The bugfix is ready for download at github.com. The best possible mitigation is suggested to be upgrading to the latest version.

Similar entries are available at VDB-216475 and VDB-353189.

Product

Vendor

- priyankark

Name

- a11y-mcp

Version

- 1.0.0
- 1.0.1
- 1.0.2
- 1.0.3
- 1.0.4
- 1.0.5

License

- open-source

Website

- Product: https://github.com/priyankark/a11y-mcp/

CPE 2.3

- 🔒
- 🔒
- 🔒

CPE 2.2

- 🔒
- 🔒
- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv3

VulDB Meta Base Score: 4.3
VulDB Meta Temp Score: 4.1

VulDB Base Score: 5.3
VulDB Temp Score: 4.8
VulDB Vector: 🔒
VulDB Reliability: 🔍

Vendor Base Score (priyankark): 3.3
Vendor Vector (priyankark): 🔒

CVSSv2

VulDB Base Score: 🔒
VulDB Temp Score: 🔒
VulDB Reliability: 🔍

Exploiting

Class: Server-side request forgery
CWE: CWE-918
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: Upgrade
Status: 🔍

0-Day Time: 🔒

Upgrade: a11y-mcp 1.0.6
Patch: e3e11c9e8482bd06b82fd9fced67be4856f0dffc

Timeline

04/01/2026		Advisory disclosed
04/01/2026	+0 days	VulDB entry created
04/01/2026	+0 days	VulDB entry last update

Sources

Product: github.com

Advisory: github.com
Status: Confirmed

CVE: CVE-2026-5323 (🔒)
GCVE (CVE): GCVE-0-2026-5323
GCVE (VulDB): GCVE-100-354655
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 04/01/2026 03:17 PM
Changes: 04/01/2026 03:17 PM (59), 04/01/2026 03:18 PM (11)
Complete: 🔍
Submitter: BigW
Cache ID: 4:B59:179

Submit

Accepted

- Submit #780752: priyankark a11y-mcp 1.0.4 Server-Side Request Forgery (by BigW)

Discussion

No comments yet. Languages: en.

Please log in to comment.