Server-Side Request Forgery Vulnerability in a11y-mcp #17

Open

wing3e opened 2 weeks ago · edited by wing3e Edits Owner

a11y-mcp Server-Side Request Forgery Vulnerability

1) CNA / Submission Type

- Submission type: Report a vulnerability (CVE ID request)
- Reporter role: Independent security researcher
- Report date: March 15, 2026

2) Reporter Contact (fill before submit)

- Reporter name: `Winegee`
- Reporter email: `Winegee@zju.edu.cn`
- Permission to share contact with vendor: `Yes`

3) Vendor / Product Identification

- Vendor: priyankark
- Product: a11y-mcp
- Repository: https://github.com/priyankark/a11y-mcp
- Reviewed local source path: `datasets_set/001/datasets_001/priyankark_a11y-mcp`
- Affected component(s):
- `src/index.js`

4) Vulnerability Type

- CWE: CWE-918 (Server-Side Request Forgery)
- Short title: SSRF in exposed MCP/HTTP request handler

5) Affected Versions

- Confirmed affected: 1.0.4
- Suspected affected range: versions containing the same request-to-sink flows documented below
- Fixed version: Not available at time of report (March 15, 2026)

6) Vulnerability Description

priyankark a11y-mcp contains a server-side request forgery (SSRF) vulnerability in `src/index.js`. The affected MCP request handlers pass an attacker-controlled URL to Puppeteer navigation logic without enforcing a strict destination allowlist or equivalent network restrictions. An attacker who can invoke the vulnerable handlers can cause the server to initiate requests to arbitrary internal or external resources, including loopback, private-address, link-local, or cloud metadata endpoints, subject to network reachability.

7) Technical Root Cause

1. `js/request-forgery-from-request`
   - Source: `src/index.js:83` (`request`)
   - Sink: `src/index.js:117`
   - Sink code: `await page.goto(args.url, { waitUntil: 'networkidle2', timeout: 30000 });`
2. `js/request-forgery-from-request`
   - Source: `src/index.js:83` (`request`)
   - Sink: `src/index.js:205`
   - Sink code: `await page.goto(args.url, { waitUntil: 'networkidle2', timeout: 30000 });`

8) Attack Prerequisites

- Ability to invoke the exposed MCP tool, RPC method, or HTTP route that reaches the vulnerable handler.
- No patch or runtime policy that strips or allowlists the attacker-controlled parameter before it reaches the sink.
- Network egress from the server to the attacker-chosen destination or to internal targets reachable through SSRF.

9) Proof of Concept / Reproduction Guidance

PoC transport: MCP JSON-RPC request.

Representative request:

```
{"jsonrpc":"2.0","id":1,"method":"tools/call","params":{"name":"audit_webpage","argumer {'
```

Analysis:

- `src/index.js` dispatches `audit_webpage` and `get_summary` from `CallToolRequestSchema`.
- Both handlers call `page.goto(args.url, ...)` on a Puppeteer page.
- A listener under attacker control will receive the server-side navigation request, which is sufficient to reproduce SSRF.

10) Security Impact

- Confidentiality: High where internal HTTP services or metadata endpoints are reachable.
- Integrity: Low to Medium depending on whether internal administrative APIs accept state-changing requests.
- Availability: Low to Medium through request fan-out, internal service interaction, or unintended long-running fetches.
- Scope: Unchanged.

11) CVSS v3.1 Suggestion

- Suggested vector for deployments that expose the vulnerable handler to untrusted callers: `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L`
- Suggested base score: 8.6 (High)
- If the vulnerable route is only reachable by trusted authenticated operators, adjust `PR` accordingly.

12) Workarounds / Mitigations

- Apply a strict URL allowlist for scheme, host, port, and path.
- Reject loopback, link-local, RFC1918, and cloud metadata destinations after DNS resolution and redirect handling.
- Disable arbitrary user-supplied fetch or navigation targets where business logic does not require them.
- Add authentication, authorization, audit logging, and rate limiting around sensitive MCP/HTTP handlers.

13) Recommended Fix

- Eliminate the direct request-to-sink data flow documented above.

- Introduce schema validation at the boundary where MCP or HTTP parameters enter the application.
- Add regression tests that prove attacker-controlled values cannot reach process execution sinks or arbitrary outbound request sinks.
- Publish a security advisory with an explicit fixed version once a patch is released.

14) References

- Repository: https://github.com/priyankark/a11y-mcp
- Package name: `a11y-mcp`
- Reviewed source file: `src/index.js`
- CWE-918: https://cwe.mitre.org/data/definitions/918.html

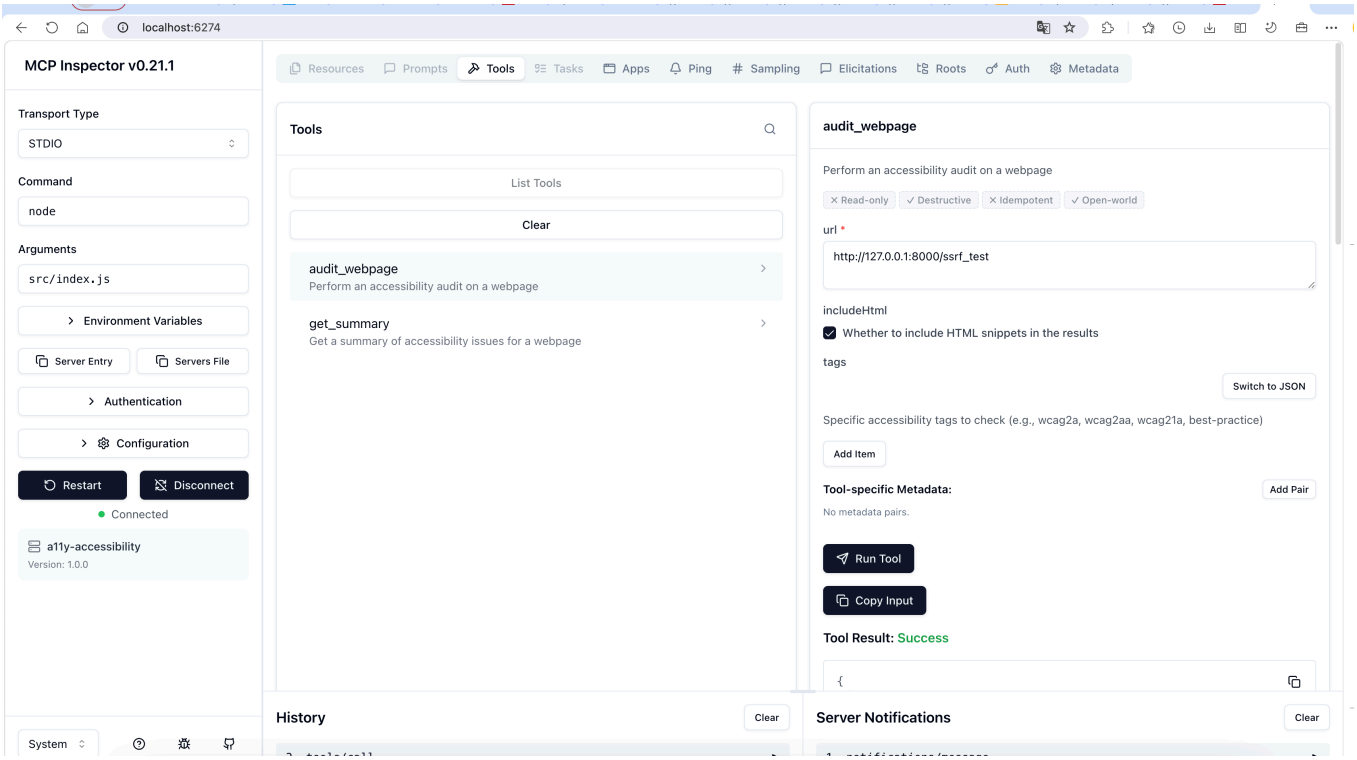
15) Credits

- Discoverer: `Winegee`
- Discovery method: Static analysis (CodeQL) plus repository source-code audit

16) Additional Notes for Form Mapping

- Issue status at report time: source-code confirmed in the local dataset.
- Dynamic exploit replay status: not performed for every repository unless separately noted.
- Version-range accuracy should be finalized by the maintainer against release history before public disclosure.

wing3e 2 weeks ago · edited by wing3e Edits Owner Author •••



Successful execution returns the following package


```
{
  "url": "http://127.0.0.1:8000/ssrf_test",
  "timestamp": "2026-03-16T10:32:25.035Z",
  "violations": [
    {
      "id": "document-title",
      "impact": "serious",
      "description": "Ensure each HTML document contains a non-empty <title> element",
      "helpUrl": "https://dequeuniversity.com/rules/axe/4.11/document-title?
application=axe-puppeteer",
      "nodes": [
        {
          "impact": "serious",
          "target": [
            "html"
          ],
          "failureSummary": "Fix any of the following:\n  Document does not have a non-
empty <title> element",
          "html": "<html>"
        }
      ]
    },
    {
      "id": "html-has-lang",
      "impact": "serious",
      "description": "Ensure every HTML document has a lang attribute",
      "helpUrl": "https://dequeuniversity.com/rules/axe/4.11/html-has-lang?
application=axe-puppeteer",
      "nodes": [
        {
          "impact": "serious",
          "target": [
```

```
            "html"
          ],
          "failureSummary": "Fix any of the following:\n  The <html> element does not have
a lang attribute",
          "html": "<html>"
        }
      ]
    },
    {
      "id": "landmark-one-main",
      "impact": "moderate",
      "description": "Ensure the document has a main landmark",
      "helpUrl": "https://dequeuniversity.com/rules/axe/4.11/landmark-one-main?
application=axe-puppeteer",
      "nodes": [
        {
          "impact": "moderate",
          "target": [
            "html"
          ],
          "failureSummary": "Fix all of the following:\n  Document does not have a main
landmark",
          "html": "<html>"
        }
      ]
    },
    {
      "id": "page-has-heading-one",
      "impact": "moderate",
      "description": "Ensure that the page, or at least one of its frames contains a
level-one heading",
      "helpUrl": "https://dequeuniversity.com/rules/axe/4.11/page-has-heading-one?
application=axe-puppeteer",
      "nodes": [
        {
          "impact": "moderate",
          "target": [
            "html"
          ],
          "failureSummary": "Fix all of the following:\n  Page must have a level-one
heading",
          "html": "<html>"
        }
      ]
    },
    {
      "id": "region",
      "impact": "moderate",
      "description": "Ensure all page content is contained by landmarks",
      "helpUrl": "https://dequeuniversity.com/rules/axe/4.11/region?application=axe-
puppeteer",
      "nodes": [
        {
          "impact": "moderate",
          "target": [
            "pre"
```

```
          ],
          "failureSummary": "Fix any of the following:\n  Some page content is not
contained by landmarks",
          "html": "<pre>{\n  \"message\": \"Hello from SSRF test endpoint!\",\n
\"status\": \"success\",\n  \"data\": {\n    \"route\": \"/ssrf_test\",\n    \"method\":
\"GET\",\n    \"note\": \"This endpoint is for SSRF testing\"\n  }\n}</pre>"
        }
      ]
    }
  ],
  "passes": 3,
  "incomplete": 0,
  "inapplicable": 82
}
```


Metadata

Assignees

No one assigned

Labels

No labels

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

Code with agent mode

No branches or pull requests

Participants