fix: patch SSRF vulnerability and upgrade vulnerable dependencies #14

Draft **Copilot** wants to merge 4 commits into `main` from `copilot/fix-ssrf-vulnerability`

Copilot AI commented 2 weeks ago • edited Contributor

User-supplied `fileUrl` in `uploadFile` was passed directly to `axios.get` with no validation, and any tool could override the Directus API `url` per-request — both sinks reachable by an unprivileged MCP client, enabling SSRF to loopback, RFC-1918, and cloud metadata endpoints.

SSRF fix (`index.ts`)

- **`validateUrl(rawUrl)`** — async guard applied at both sinks:
  - Rejects non-`http:`/`https:` schemes
  - Bare IP addresses validated directly via `net.isIPv4`/`net.isIPv6` (no DNS round-trip)
  - Hostnames DNS-resolved; request rejected if resolution fails entirely
  - All resolved addresses checked against `isForbiddenAddress()`
- **`isForbiddenAddress(addr)`** — blocks loopback, link-local, RFC-1918, RFC-6598 shared space, unique-local IPv6 (`fc00::/7`), link-local IPv6 (`fe80::/10`), IPv6 loopback (`::1`/`::`), IPv6-mapped IPv4 private ranges (`::ffff:10.x` etc.), multicast, and reserved ranges; unknown format defaults to forbidden
- **`extractMappedIPv4(addr)`** — detects `::ffff:x.x.x.x` bypass attempts in compact and expanded form
- `maxRedirects: 0` on the file-download fetch to block redirect-chain bypass

```
// Before — unvalidated user input reaches network sink
const fileResponse = await axios.get(fileUrl, { responseType: 'arraybuffer' });

// After
```

```
await validateUrl(fileUrl);
const fileResponse = await axios.get(fileUrl, { responseType: 'arraybuffer', maxRedirects: 0
```

Dependency upgrades (`package.json`)

Package	Before	After	CVEs
`@modelcontextprotocol/inspector`	`^0.10.2`	`^0.16.6`	XSS + missing proxy auth
`axios`	`^1.6.7`	`^1.13.5`	DoS via `__proto__`, data-size DoS, NO_PROXY SSRF bypass, metadata header injection
`form-data`	`^4.0.0`	`^4.0.4`	Predictable multipart boundary (`Math.random`)
`path-to-regexp` (transitive)	`8.2.0`	`^8.4.0` via `overrides`	ReDoS via optional groups / multiple wildcards

`Initial plan` `7476924`

Copilot AI assigned **Copilot** and **pixelsock** 2 weeks ago

Copilot started work on behalf of **pixelsock** 2 weeks ago View session

Copilot AI linked an issue 2 weeks ago that may be closed by this pull request

Server-Side Request Forgery Vulnerability in directus-mcp #13 Open

Copilot AI and others added 3 commits 2 weeks ago

`fix: prevent SSRF in uploadFile fileUrl and per-request url override` ··· `ef87ff0`

`chore: dependency vulnerability upgrade plan` ··· `59a2adf`

`fix: upgrade vulnerable dependencies (inspector, axios, form-data, pa…` ··· `c081bb2`

Copilot AI changed the title **[WIP] Fix Server-Side Request Forgery vulnerability in directus-mcp** **fix: patch SSRF vulnerability and upgrade vulnerable dependencies** 2 weeks ago

Copilot finished work on behalf of **pixelsock** 2 weeks ago

Copilot AI requested a review from **pixelsock** 2 weeks ago

pixelsock commented 2 weeks ago — Owner

@copilot resolve the merge conflicts in this pull request

Reviewers

pixelsock

Assignees

pixelsock

Copilot

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

Server-Side Request Forgery Vulnerability in directus-mcp

2 participants