Target prepublish-mcp

Could not run: not tested

We could not start this server, so none of its behavior was tested. It said: TypeError: fetch failed

Recommendation	Confidence	Findings
Review	**n/a**	**0 high 0 med 2 info**

We could not start it, so nothing was tested. Treat it as unverified.

Scope

Package	prepublish-mcp
Source	npm 1.0.3
SHA-256	bd5a18204a491022912a471cdb2e4b1b5114585ef74aa1aa54fe953cd2ed3954
Files	6
Scanned	25 Oct 2026, 18:51 UTC
Engine	detonator 0.5.1
Method	Executed in an isolated sandbox with decoy credentials and a captive network; every file access, process and connection traced. 3 runs: baseline, time-travel, ci-github.

Findings summary

ID	Severity	Confidence	Finding
F01	Low	Info	Network destinations contacted
F02	Low	Info	A tool read its own credentials (e.g. gh, aws, ssh)

Observed behavior

Install step	package manager only, no install scripts
Runs as	node dist/bridge.js
Network	mcp.prepublish.ai (2 conn, 3218 B sent; while running)
Credentials	~/.npmrc (own tool, normal)
Files written	nothing outside its own folder

Finding details

F01 Network destinations contacted

Severity: Low Confidence: Info Observed in: mcp:baseline
The package connected to these hosts.

Description

Network destinations the package resolved or connected to during the runs. All traffic was captured by the sandbox; nothing reached the internet.

Impact

Context only. Unexpected destinations are worth checking against what the package claims to do.

Evidence

```
mcp.prepublish.ai
```

Remediation

Confirm each host is expected (the package's API, its registry). Allowlist expected egress in production.

F02 A tool read its own credentials (e.g. gh, aws, ssh)

Severity: Low Confidence: Info Observed in: mcp:baseline
A tool opened its own login or config file, such as npm reading ~/.npmrc.

Description

A tool opened its own configuration or login file, such as npm reading ~/.npmrc or gh reading its hosts file.

Impact

None in itself: this is how those tools work. Listed so the report shows every credential access.

Evidence

```
~/.npmrc (by npm)
```

Remediation

No action needed.

Run log

mcp:baseline ok 4.6s

new behavior: dns:mcp.prepublish.ai, ownread:~/.npmrc, write:<skill>/node_modules/.bin/node-which, write:<skill>/node_modules/.bin/prepublish-mcp, write:~/.npm/_logs/*-debug-0.log | server did not complete the handshake: no response; server crashed: TypeError: fetch failed; 0 tool calls

mcp:time-travel ok 2.7s

no new behavior | server did not complete the handshake: no response; server crashed: McpError: MCP error -32001: Request timed out; 0 tool calls

mcp:ci-github ok 4.7s

no new behavior | server did not complete the handshake: no response; server crashed: TypeError: fetch failed; 0 tool calls

Observed behavior only. A clean result does not prove a package is safe. Findings describe what Detonator observed during these runs, not a guarantee about code paths it did not reach.