



Target `create-vagejs`

Could not run: not tested

This does not look like an MCP server (it printed a usage message and exited), so none of its behavior was tested.

Recommendation	Confidence	Findings
Review	n/a	0 high 0 med 1 info

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

Scope

Package	<code>create-vagejs</code>
Source	<code>npm 0.5.0</code>
SHA-256	<code>c7fcb3ed5062d24ba9c251407e392ff6972db7c17e317f80aa5092fd309ca024</code>
Files	<code>4</code>
Scanned	<code>25 Oct 2026, 18:23 UTC</code>
Engine	<code>detonator 0.5.1</code>
Method	<code>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.</code>

Findings summary

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

Observed behavior

Install step	<code>package manager only, no install scripts</code>
Runs as	<code>node index.js</code>
Network	<code>no connections</code>
Credentials	<code>~/.npmrc (own tool, normal)</code>
Files written	<code>nothing outside its own folder</code>

Finding details



F01 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 2.0s

new behavior: ownread:~/.npmrc, write:<skill>/node_modules/.bin/create-vagejs, write:<skill>/node_modules/.bin/marked, write:<skill>/node_modules/.bin/nanoid, write:<skill>/node_modules/.bin/rolldown | server did not complete the handshake: no response; server crashed: Usage: npm create vagejs@latest <directory>; 0 tool calls

mcp:time-travel ok 1.8s

no new behavior | server did not complete the handshake: no response; server crashed: Usage: npm create vagejs@latest <directory>; 0 tool calls

mcp:ci-github ok 1.9s

no new behavior | server did not complete the handshake: no response; server crashed: Usage: npm create vagejs@latest <directory>; 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.