



Target chrome-devtools-mcp

No malicious behavior observed

We ran it 4 times, with a normal setup, the clock moved a year ahead, a GitHub Actions environment and an AI agent using it. It started as an MCP server, exposed 32 tools and we called them 300 times. It contacted play.googleapis.com and registry.npmjs.org. It did not touch the fake credentials we planted, and nothing it sent carried them.

Recommendation	Confidence	Findings
No action needed	n/a	0 high 0 med 2 info

Nothing observed calls for action. This is evidence, not a guarantee.

Scope

Package	chrome-devtools-mcp
Source	npm 1.12.0
SHA-256	0b8a54b7eb89fffd126623333843392636cdc665ef1ff49a39bde73c411f2d37
Files	378
Scanned	25 Oct 2026, 17:15 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. 4 runs: baseline, time-travel, ci-github, agent.

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 ./build/src/bin/chrome-devtools-mcp.js
Tools exposed	32 (300 calls tested): click, close_page, drag, emulate, evaluate_script, fill, fill_form, get_console_message, get_css_styles, get_network_request, handle_dialog, hover, lighthouse_audit, list_console_messages, list_network_requests, list_pages, navigate_page, new_page, performance_analyze_insight, performance_start_trace,



	performance_stop_trace, press_key, resize_page, screencast_start
Network	play.googleapis.com (36 conn, 14110 B sent; while running) registry.npmjs.org (2 conn, 782 B sent; while running)
Credentials	~/.npmrc (own tool, normal)
Files written	~/.cache/chrome-devtools-mcp/latest.json (written) ~/.local/share/chrome-devtools-mcp/telemetry_state.json (written)

Finding details

F01 Network destinations contacted

Severity: Low Confidence: Info Observed in: mcp:baseline, mcp:ci-github
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

play.googleapis.com

registry.npmjs.org

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 35.2s**

new behavior: dns:play.googleapis.com, dns:registry.npmjs.org, ownread:~/.npmrc, write:<skill>/node_modules/.bin/chrome-devtools, write:<skill>/node_modules/.bin/chrome-devtools-mcp | install scripts: exit 0; restarted once; 100 tool calls

mcp:time-travel ok 35.0s

no new behavior | install scripts: exit 0; 100 tool calls

mcp:ci-github ok 29.2s

no new behavior | install scripts: exit 0; 100 tool calls

mcp-agent:agent ok 17.0s

no new behavior | install scripts: exit 0

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.