



Target @modelcontextprotocol/server-everything

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 contacted example.com and raw.githubusercontent.com. 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	@modelcontextprotocol/server-everything
Source	npm 1.0.0
SHA-256	564b83331f296eaca46f71d01c859eb0152ce93f825e11635dece4ec04d29f70
Files	49
Scanned	25 Oct 2026, 12:11 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)

Finding details

F01

Network destinations contacted

Severity: Low Confidence: Info Observed in: mcp:baseline, mcp-agent:agent

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

example.com

raw.githubusercontent.com

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 38.1s

new behavior: dns:example.com, dns:raw.githubusercontent.com, ownread:~/.npmrc,
write:<skill>/node_modules/.bin/mcp-server-everything, write:<skill>/node_modules/.bin/node-which | install scripts: exit 0; 52 tool calls

mcp:time-travel ok 13.7s

no new behavior | install scripts: exit 0; 52 tool calls

mcp:ci-github ok 38.2s

no new behavior | install scripts: exit 0; 52 tool calls

mcp-agent:agent ok 18.9s

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.