

Target cgartlab-quill

No malicious behavior observed

We ran it 8 times, with a normal setup, WATCH_REPORT_DEPENDENCIES set, a GitHub Actions environment, the clock moved a year ahead and AGENT_TIMEOUT_MS and BASELINE and CURL_CA_BUNDLE and DENO_CERT... set. It made no network connections. 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 0 info

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

Scope

Package	cgartlab-quill
Source	clawhub 0.11.0
SHA-256	9ef4ec651c16963c18182c131dd7041625e9a2d2754643b12b4525b8a63330a0
Files	53
Scanned	26 Oct 2026, 19:26 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. 8 runs: baseline, guided:WATCH_REPORT_DEPENDENCIES, ci-github, time-travel, guided:AGENT_TIMEOUT_MS,BASELINE,CURL_CA_BUNDLE,DENO_CERT....
Note	batch:clawhub:2026-10-26

Observed behavior

Install step	none
Runs as	node <skill>/evals/check-workspace.mjs; node <skill>/evals/run.mjs; /usr/bin/node <skill>/evals/check-workspace.mjs --workspace <skill>/results/workspaces/eva; /usr/bin/node <skill>/evals/check-workspace.mjs --eval 1 --workspace <skill>/results/works; /usr/bin/node <skill>/evals/check-workspace.mjs --eval 2 --workspace <skill>/results/works; /usr/bin/node <skill>/evals/check-workspace.mjs --eval 3 --workspace <skill>/results/works
Network	no connections
Credentials	no planted credential touched



Files written

- ./quill-snapshot.json (written)
- ./true/coverage-13-1793042783613-0.json (written)
- ./true/coverage-13-1793042786078-0.json (written)

Run log

scripts:baseline ok 1.2s
new behavior: write:./quill-snapshot.json

scripts:guided:WATCH_REPORT_DEPENDENCIES ok 1.7s
no new behavior

scripts:ci-github ok 3.1s
no new behavior

scripts:baseline timeout 20.3s
no new behavior

scripts:time-travel timeout 20.3s
no new behavior

scripts:guided:AGENT_TIMEOUT_MS,BASELINE,CURL_CA_BUNDLE,DENO_CERT... ok 1.2s
new behavior: write:./true/coverage-13-*-*0.json

scripts:guided:AGENT_TIMEOUT_MS,BASELINE,CURL_CA_BUNDLE,DENO_CERT... ok 0.8s
no new behavior

scripts:ci-github timeout 20.3s
no new behavior

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.