

Target mochi-content-workbench

No malicious behavior observed

We ran it 8 times, with a normal setup, WATCH_REPORT_DEPENDENCIES set, a GitHub Actions environment and NODE_TEST_CONTEXT and WATCH_REPORT_DEPENDENCIES 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	mochi-content-workbench
Source	clawhub 1.0.0
SHA-256	a577072b5914ae05f49f11c9904786b65314b3aa12ef57cab5f8ebe57d224021
Files	10
Scanned	26 Oct 2026, 19:43 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, guided:NODE_TEST_CONTEXT,WATCH_REPORT_DEPENDENCIES.
Note	batch:clawhub:2026-10-26

Observed behavior

Install step	none
Runs as	node <skill>/scripts/check.mjs; node <skill>/scripts/local.mjs; node <skill>/tests/check.test.mjs
Network	no connections
Credentials	no planted credential touched
Files written	nothing outside its own folder

Run log



scripts:baseline ok 1.0s

no new behavior

scripts:guided:WATCH_REPORT_DEPENDENCIES ok 1.1s

no new behavior

scripts:ci-github ok 0.9s

no new behavior

scripts:baseline ok 0.9s

no new behavior

scripts:guided:WATCH_REPORT_DEPENDENCIES ok 0.9s

no new behavior

scripts:ci-github ok 0.7s

no new behavior

scripts:baseline ok 2.1s

no new behavior

scripts:guided:NODE_TEST_CONTEXT,WATCH_REPORT_DEPENDENCIES ok 2.2s

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.