Target mochi-workflow-blueprints

No malicious behavior observed

We ran it 8 times, with a normal setup, LC_MESSAGES set and a production environment. 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-workflow-blueprints
Source	clawhub 1.0.0
SHA-256	c8b739cbf6454657f432d0b10a0f864b735d4c1f2786d062278f0567c006543b
Files	13
Scanned	27 Oct 2026, 12:19 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:LC_MESSAGES, production.
Note	batch:clawhub:2026-10-27

Observed behavior

Install step	none
Runs as	python3 <skill>/scripts/run.py; python3 <skill>/scripts/runtime.py; python3 <skill>/scripts/task.py
Network	no connections
Credentials	no planted credential touched
Files written	nothing outside its own folder

Run log

scripts:baseline ok 2.7s
no new behavior

scripts:guided:LC_MESSAGES ok 2.1s
no new behavior

scripts:production ok 3.4s
no new behavior

scripts:baseline ok 1.4s
no new behavior

scripts:guided:LC_MESSAGES ok 1.8s
no new behavior

scripts:production ok 2.1s
no new behavior

scripts:baseline ok 2.2s
no new behavior

scripts:guided:LC_MESSAGES ok 2.1s
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.