

Target diy-materials-estimator

No malicious behavior observed

We ran it 7 times, with a normal setup, LC_MESSAGES set, docs:paint --room 12x14 and a GitHub Actions 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	diy-materials-estimator
Source	clawhub 1.0.0
SHA-256	e03ba02ffacd1448ae968bbe9bdc7309ae9ebd2e91ed5d4c2af40ef6cb521262
Files	7
Scanned	26 Oct 2026, 18:14 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. 7 runs: baseline, guided:LC_MESSAGES, docs:paint --room 12x14, ci-github.
Note	batch:clawhub:2026-10-26

Observed behavior

Install step	none
Runs as	python3 <skill>/scripts/materials_estimator.py; python3 <skill>/scripts/materials_estimator.py paint --room 12x14; python3 scripts/materials_estimator.py paint --room 12x14 --height; python3 scripts/materials_estimator.py mulch --area 20x4 --depth-in; python3 scripts/materials_estimator.py concrete --slab 10x12x4 --bag-lb; python3 scripts/materials_estimator.py fence --length 200 --style
Network	no connections
Credentials	no planted credential touched
Files written	nothing outside its own folder



Run log

scripts:baseline ok 1.9s

no new behavior

scripts:guided:LC_MESSAGES ok 1.4s

no new behavior

scripts:docs:paint --room 12x14 ok 1.9s

no new behavior

obedient:baseline ok 11.5s

no new behavior

obedient:guided:LC_MESSAGES ok 9.0s

no new behavior

obedient:ci-github ok 9.5s

no new behavior

llm:baseline ok 19.4s

no new behavior | token budget reached

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.