Target mochi-meal-planner

No malicious behavior observed

We ran it 8 times, with a normal setup, WATCH_REPORT_DEPENDENCIES set 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	mochi-meal-planner
Source	clawhub 1.0.0
SHA-256	b37616a3f2c71e7a9024e4e78f4d8bbcd0b006ae7415b3e0bbcd818609314a99
Files	11
Scanned	26 Oct 2026, 19:30 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.
Note	batch:clawhub:2026-10-26

Observed behavior

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

Run log

scripts:baseline ok 0.9s
no new behavior

scripts:guided:WATCH_REPORT_DEPENDENCIES ok 1.0s
no new behavior

scripts:ci-github ok 0.6s
no new behavior

scripts:baseline ok 1.1s
no new behavior

scripts:guided:WATCH_REPORT_DEPENDENCIES ok 1.0s
no new behavior

scripts:ci-github ok 0.8s
no new behavior

scripts:baseline ok 1.0s
no new behavior

scripts:guided:WATCH_REPORT_DEPENDENCIES ok 2.5s
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.