Target il-reader

No malicious behavior observed

We ran it 8 times, with a normal setup, a GitHub Actions environment and cloud credentials present. 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	il-reader
Source	clawhub 1.2.1
SHA-256	74eb3160477636a77387dc94ec5f574197ec2a709b0d797d8796d3513e67ec7f
Files	290
Scanned	26 Oct 2026, 19:33 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, ci-github, cloud-creds.
Note	batch:clawhub:2026-10-26

Observed behavior

Install step	none
Runs as	node <skill>/lib/asset-cache.cjs; node <skill>/lib/question-bank.cjs; node <skill>/lookup.cjs
Network	no connections
Credentials	no planted credential touched
Files written	nothing outside its own folder

Run log

scripts:baseline ok 0.8s
no new behavior

scripts:ci-github ok 0.9s
no new behavior

scripts:cloud-creds ok 0.8s
no new behavior

scripts:baseline ok 0.7s
no new behavior

scripts:ci-github ok 0.9s
no new behavior

scripts:cloud-creds ok 0.9s
no new behavior

scripts:baseline ok 1.1s
no new behavior

scripts:ci-github ok 0.9s
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.