

Target gtrk-oralcut

No malicious behavior observed

We ran it 4 times, with a normal setup, the environment variables it says it needs 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 2 info

Nothing observed calls for action. This is evidence, not a guarantee.

Scope

Package	gtrk-oralcut
Source	clawhub 1.3.9
SHA-256	6aedb1a18bb6b741e26e3bcba2739d2cff7133b7875a3f54941ab0fcd6d05d52
Files	3
Scanned	27 Oct 2026, 13:16 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. 4 runs: baseline, declared-env, ci-github.
Note	batch:clawhub:2026-10-27

Findings summary

ID	Severity	Confidence	Finding
F01	Low	Info	Loaded the project's .env file
F02	Low	Info	A tool read its own credentials (e.g. gh, aws, ssh)

Observed behavior

Install step	none
Runs as	ls -la; which gtrk; head -50; sed s/=.*<redacted>/ .env; cat README.md package.json .gitignore; ls -la src skill
Network	no connections
Credentials	./.env (read) ~/.npmrc (own tool, normal)

Files written nothing outside its own folder

Finding details

F01 Loaded the project's .env file

Severity: Low Confidence: Info Observed in: llm:baseline

The package loaded the project's .env file.

Description

The process loaded the project's .env file. Configuration libraries (python-dotenv, pydantic-settings, the official Python MCP SDK) do this at startup.

Impact

None unless the values leave the process, which would be reported as a critical exfiltration finding.

Evidence

```
./ .env (by sed)
```

Remediation

No action needed. Keep long-lived secrets out of project .env files where possible.

F02 A tool read its own credentials (e.g. gh, aws, ssh)

Severity: Low Confidence: Info Observed in: llm:baseline

A tool opened its own login or config file, such as npm reading ~/.npmrc.

Description

A tool opened its own configuration or login file, such as npm reading ~/.npmrc or gh reading its hosts file.

Impact

None in itself: this is how those tools work. Listed so the report shows every credential access.

Evidence

```
~/.npmrc (by npm)
```

Remediation

No action needed.

Run log

obedient:baseline ok 1.8s

no new behavior

obedient:declared-env ok 1.6s

no new behavior

obedient:ci-github ok 1.8s

no new behavior

llm:baseline ok 38.8s

new behavior: ownread:./env, ownread:~/.npmrc | 4 model steps, 6 commands



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.