

Target **sogni-worlds**

No malicious behavior observed

We ran it 8 times, with a normal setup, the environment variables it says it needs, a production environment, everything and a GitHub Actions environment. It contacted github.com and registry.npmjs.org. 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	sogni-worlds
Source	clawhub 0.3.1
SHA-256	5b19a0ef0e5a59bfdcff08a640a377a80424873e398789da74e3f32220713db0
Files	4
Scanned	27 Oct 2026, 13:15 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, declared-env, production, everything, ci-github, cloud-creds.
Note	batch:clawhub:2026-10-27

Findings summary

ID	Severity	Confidence	Finding
F01	Low	Info	Network destinations contacted
F02	Low	Info	A tool read its own credentials (e.g. gh, aws, ssh)

Observed behavior

Install step	package manager only, no install scripts
Runs as	<pre>git clone https://github.com/Sogni-AI/sogni-worlds-kit; /usr/lib/git-core/git remote-https origin https://github.com/Sogni-AI/sogni-worlds-kit; /usr/lib/git-core/git-remote-https origin https://github.com/Sogni-AI/sogni-worlds-kit; node world doctor</pre>



Network github.com (11 conn, 3104 B sent; while running)
 registry.npmjs.org (DNS lookup only; while running)

Credentials ~/.npmrc (own tool, normal)

Files written ./sogni-worlds-kit/.git/HEAD.lock (written)
 ./sogni-worlds-kit/.git/config.lock (written)
 ./sogni-worlds-kit/.git/description (written)
 ./sogni-worlds-kit/.git/info/exclude (written)
 ./sogni-worlds-kit/.git/tC6Hmz5 (written)
 ./sogni-worlds-kit/.git/tEjWwEC (written)
 ./sogni-worlds-kit/.git/tJqLGwg (written)
 ./sogni-worlds-kit/.git/tQDuTON (written)
 ./sogni-worlds-kit/.git/tUoa6n0 (written)
 ./sogni-worlds-kit/.git/tezGXIK (written)
 ./sogni-worlds-kit/.git/tfi3FLx (written)
 ./sogni-worlds-kit/.git/ttReRkI (written)

Finding details

F01 Network destinations contacted

Severity: Low Confidence: Info Observed in: obedient:baseline, obedient:production
The package connected to these hosts.

Description

Network destinations the package resolved or connected to during the runs. All traffic was captured by the sandbox; nothing reached the internet.

Impact

Context only. Unexpected destinations are worth checking against what the package claims to do.

Evidence

github.com

registry.npmjs.org

Remediation

Confirm each host is expected (the package's API, its registry). Allowlist expected egress in production.

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

Severity: Low Confidence: Info Observed in: obedient:production
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 8.1s

new behavior: dns:github.com, write:./sogni-worlds-kit/.git/HEAD, write:./sogni-worlds-kit/.git/HEAD.lock,
write:./sogni-worlds-kit/.git/config, write:./sogni-worlds-kit/.git/config.lock

obedient:declared-env ok 7.2s

new behavior: write:./sogni-worlds-kit/.git/tEjWwEC

obedient:production ok 20.3s

new behavior: dns:registry.npmjs.org, ownread:~/.npmrc, write:./sogni-worlds-kit/.git/tfi3FLx, write:~/.npm/_logs/*-debug-0.log

obedient:everything ok 20.3s

new behavior: write:./sogni-worlds-kit/.git/tC6Hmz5

obedient:ci-github ok 20.3s

new behavior: write:./sogni-worlds-kit/.git/tJqIGwg

obedient:cloud-creds ok 7.1s

new behavior: write:./sogni-worlds-kit/.git/tezGXIK

obedient:ci-gitlab ok 9.7s

new behavior: write:./sogni-worlds-kit/.git/tQDuTON

obedient:time-travel ok 5.4s

new behavior: write:./sogni-worlds-kit/.git/ttReRkI

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.