

Target feedbackpulse

No malicious behavior observed

We ran it 8 times, with a normal setup, a GitHub Actions environment, cloud credentials present, a production environment and a GitLab CI environment. It contacted app.feedbackpulse.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 4 info

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

Scope

Package	feedbackpulse
Source	clawhub 1.0.0
SHA-256	d99baeab2733889e757ec3e3b1dfe3afe6b249ce5d382e53b3461e0ca26bc7fe
Files	3
Scanned	26 Oct 2026, 18:28 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, production, ci-gitlab, time-travel.
Note	batch:clawhub:2026-10-26

Findings summary

ID	Severity	Confidence	Finding
F01	Low	Info	Used the planted login with its own service (registry.npmjs.org)
F02	Low	Info	Network destinations contacted
F03	Low	Info	A tool read its own credentials (e.g. gh, aws, ssh)
F04	Low	Info	Loaded the project's .env file

Observed behavior

Install step	none
Runs as	<code>npx -y mcp-remote https://app.feedbackpulse.com/mcp/employee-surveys;</code> <code>node /usr/bin/npx -y mcp-remote</code>



	<code>https://app.feedbackpulse.com/mcp/employee-surveys; ls -la; ls -la skill; cat skill/SKILL.md; head -50</code>
Network	app.feedbackpulse.com (6 conn, 1702 B sent; while running) registry.npmjs.org (19 conn, 5687 B sent; while running)
Credentials	./.env (read) ~/.npmrc (own tool, normal)
Files written	nothing outside its own folder

Finding details

F01 Used the planted login with its own service (registry.npmjs.org)

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

A planted login went to the service it belongs to, as normal authentication (npm sending its token to registry.npmjs.org while installing).

Description

A planted login was sent to the service it belongs to, only as the Authorization header of ordinary requests: for example npm sending the ~/.npmrc token to registry.npmjs.org while installing dependencies.

Impact

None in itself: this is how the package manager authenticates. Publishing, unpublishing or creating tokens with it would be reported as exfiltration.

Evidence

```
~/.npmrc (npm) sent only as the login header of ordinary requests (no publish)
```

Remediation

No action needed.

F02 Network destinations contacted

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

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

```
registry.npmjs.org
```

```
app.feedbackpulse.com
```

Remediation

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



F03 A tool read its own credentials (e.g. gh, aws, ssh)

Severity: Low Confidence: Info Observed in: obedient:baseline, 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 npx)
```

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

Remediation

No action needed.

F04 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.

Run log

obedient:baseline ok 20.3s

new behavior: dns:registry.npmjs.org, ownread:~/.npmrc, write:~/.npm/_cacache/content-v2/sha512/d6/96/*, write:~/.npm/_cacache/index-v5/2b/da/*, write:~/.npm/_cacache/tmp/*

obedient:ci-github ok 17.9s

new behavior: write:~/.npm/_cacache/content-v2/sha512/31/cc/*, write:~/.npm/_cacache/tmp/866dfc7b

obedient:cloud-creds ok 20.3s

new behavior: write:~/.npm/_cacache/content-v2/sha512/08/13/*, write:~/.npm/_cacache/tmp/36170d33

obedient:production ok 13.2s

new behavior: write:~/.npm/_cacache/content-v2/sha512/f3/d0/*

obedient:ci-gitlab ok 16.8s

new behavior: write:~/.npm/_cacache/content-v2/sha512/46/d8/*, write:~/.npm/_cacache/tmp/7a0fde23



obedient:time-travel ok 15.8s

no new behavior

obedient:everything ok 14.2s

new behavior: write:~/.npm/_cacache/content-v2/sha512/9c/54/*, write:~/.npm/_cacache/tmp/0c9fa228

llm:baseline ok 47.5s

new behavior: dns:app.feedbackpulse.com, exec:curl, ownread:./.env, write:~/.npm/_cacache/content-v2/sha512/42/21/*, write:~/.npm/_cacache/tmp/88cef8d4 | 8 model steps, 8 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.