

Target `cn-mirror-download`

No malicious behavior observed

We ran it 8 times, with a normal setup, `ANDROID_DATA` and `APPENGINE_RUNTIME` and `CURL_CA_BUNDLE` and `DEB_PYTHON_INSTALL_LAYOUT...` set, `PIP_INDEX_URL` set, a GitHub Actions environment and `ANDROID_DATA` and `APPENGINE_RUNTIME` and `CI` and `CURL_CA_BUNDLE...` set. It contacted `cdn.npmmirror.com`, `ghfast.top` and `goproxy.cn` and others. 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	<code>cn-mirror-download</code>
Source	<code>clawhub 1.0.0</code>
SHA-256	<code>f654562c5c07a45fdf6005062c1909459ca424853db4f0be77079cd494f7372e</code>
Files	5
Scanned	27 Oct 2026, 13:06 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:ANDROID_DATA,APPENGINE_RUNTIME,CURL_CA_BUNDLE,DEB_PYTHON_INSTALL_LAYOUT..., guided:PIP_INDEX_URL, ci-github, guided:ANDROID_DATA,APPENGINE_RUNTIME,CI,CURL_CA_BUNDLE..., production.
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	none
--------------	------



Runs as	<pre>curl -sS -o /dev/null -m 8; curl -fL -C - --retry 5; git clone --depth 1 https://ghfast.top/https://github.com/OWNER/REPO.git; /usr/lib/git-core/git remote-https origin https://ghfast.top/https://github.com/OWNER/REPO; /usr/lib/git-core/git-remote-https origin https://ghfast.top/https://github.com/OWNER/REPO; pip config list</pre>
Network	<pre>cdn.npmirror.com (8 conn, 540 B sent; while running) ghfast.top (19 conn, 2309 B sent; while running) goproxy.cn (8 conn, 400 B sent; while running) hf-mirror.com (8 conn, 412 B sent; while running) maven.aliyun.com (8 conn, 584 B sent; while running) mirror.sjtu.edu.cn (8 conn, 416 B sent; while running) mirrors.aliyun.com (8 conn, 400 B sent; while running) mirrors.cloud.tencent.com (8 conn, 428 B sent; while running) mirrors.huaweicloud.com (8 conn, 464 B sent; while running) mirrors.ustc.edu.cn (8 conn, 404 B sent; while running) pypi.tuna.tsinghua.edu.cn (8 conn, 408 B sent; while running) registry.npmjs.org (5 conn, 0 B sent; while running) registry.npmirror.com (8 conn, 352 B sent; while running) rsproxy.cn (8 conn, 352 B sent; while running)</pre>
Credentials	<pre>~/.npmrc (own tool, normal)</pre>
Files written	<pre>./FILE (written) ./REPO/.git/HEAD.lock (written) ./REPO/.git/config.lock (written) ./REPO/.git/description (written) ./REPO/.git/info/exclude (written) ./REPO/.git/t1oh5t0 (written) ./REPO/.git/t6kWVoH (written) ./REPO/.git/t813V5g (written) ./REPO/.git/tC0MaAq (written) ./REPO/.git/tJg1596 (written) ./REPO/.git/tXSOFyz (written) ./REPO/.git/tb7jftu (written)</pre>

Finding details

F01 Network destinations contacted

Severity: Low Confidence: Info Observed in: obedient:baseline, obedient:ci-github
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

```
cdn.npmirror.com
```



ghfast.top

goproxy.cn

hf-mirror.com

maven.aliyun.com

mirror.sjtu.edu.cn

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: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 19.9s

new behavior: dns:cdn.npmirror.com, dns:ghfast.top, dns:goproxy.cn, dns:hf-mirror.com, dns:maven.aliyun.com

obedient:guided:ANDROID_DATA,APPENGINE_RUNTIME,CURL_CA_BUNDLE,DEB_PYTHON_INSTALL_LAYOUT... ok 21.1s

new behavior: write:./REPO/.git/t6kWWoH

obedient:guided:ANDROID_DATA,APPENGINE_RUNTIME,CURL_CA_BUNDLE,DEB_PYTHON_INSTALL_LAYOUT... ok 23.5s

new behavior: write:./REPO/.git/tXSOFyz

obedient:guided:PIP_INDEX_URL ok 26.1s

new behavior: write:./REPO/.git/tgkkyVv

obedient:guided:ANDROID_DATA,APPENGINE_RUNTIME,CURL_CA_BUNDLE,DEB_PYTHON_INSTALL_LAYOUT... ok 24.8s

new behavior: write:./REPO/.git/tb7jftu

obedient:ci-github ok 21.8s

new behavior: write:./REPO/.git/t813V5g

obedient:guided:ANDROID_DATA,APPENGINE_RUNTIME,CI,CURL_CA_BUNDLE... ok 20.1s

new behavior: write:./REPO/.git/tJg1596

**obedient:production ok 33.4s**

new behavior: write:./REPO/.git/tC0MaAq

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.