

Target mobile-merge-request

No malicious behavior observed

We ran it 8 times, with a normal setup, a GitHub Actions environment, a production environment, a GitLab CI environment and everything. It contacted github.com. 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	mobile-merge-request
Source	clawhub 1.0.1
SHA-256	28d0493b72ccca4ddbe58e4daefc93b5e0563853393dfda7d04fed2f5ba8351a
Files	6
Scanned	27 Oct 2026, 12:09 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, production, ci-gitlab, everything, cloud-creds.
Note	batch:clawhub:2026-10-27

Findings summary

ID	Severity	Confidence	Finding
F01	Low	Info	Network destinations contacted
F02	Low	Info	Loaded the project's .env file

Observed behavior

Install step	none
Runs as	<pre>git fetch origin; /usr/bin/ssh -o SendEnv=GIT_PROTOCOL git@github.com git-upload-pack 'acme-corp/payments-ap; git switch -c feature/AH/PROJ-123-ble-reconnect-backoff origin/main; git switch -c feature/AH/PROJ-124-pairing-ui feature/AH/PROJ-123-pairing-api; git push --force; git rebase origin/main</pre>



Network	github.com (DNS lookup only; while running)
Credentials	./.env (read)
Files written	./.git/COMMIT_EDITMSG (written) ./.git/FETCH_HEAD (written) ./.git/index.lock (written) ./.git/objects/19/tmp_obj_FQmcXs (written) ./.git/objects/19/tmp_obj_JBpuRq (written) ./.git/objects/19/tmp_obj_WiwPf9 (written) ./.git/objects/19/tmp_obj_uvPOHl (written) ./.git/objects/19/tmp_obj_vRmfGo (written) ./.git/objects/19/tmp_obj_yA6n9X (written) ./.git/objects/19/tmp_obj_yzfMGP (written) ./.git/objects/33/tmp_obj_1JLKp7 (written) ./.git/objects/33/tmp_obj_EPXI2a (written)

Finding details

F01 Network destinations contacted

Severity: Low Confidence: Info Observed in: obedient: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

```
github.com
```

Remediation

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

F02 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 15.4s

new behavior: dns:github.com, exec:ssh, write:./.git/COMMIT_EDITMSG, write:./.git/FETCH_HEAD, write:./.git/index

obedient:ci-github ok 5.7s

new behavior: write:./.git/objects/19/tmp_obj_uvPOHl, write:./.git/objects/33/tmp_obj_WOE7rF,
write:./.git/objects/3a/tmp_obj_xA3Kp5, write:./.git/objects/93/tmp_obj_nrDOTR, write:./.git/objects/d0/tmp_obj_WINUQw

obedient:production ok 4.0s

new behavior: write:./.git/objects/19/tmp_obj_JBpuRq, write:./.git/objects/33/tmp_obj_EPXI2a,
write:./.git/objects/3a/tmp_obj_QMzRYi, write:./.git/objects/93/tmp_obj_hjddXG, write:./.git/objects/d0/tmp_obj_x8SqEs

obedient:ci-gitlab ok 5.8s

new behavior: write:./.git/objects/19/tmp_obj_FQmcXs, write:./.git/objects/33/tmp_obj_1JLKp7,
write:./.git/objects/3a/tmp_obj_fDQwzt, write:./.git/objects/93/tmp_obj_6Cf89X, write:./.git/objects/d0/tmp_obj_EYkLjm

obedient:everything ok 5.2s

new behavior: write:./.git/objects/19/tmp_obj_yzfMGP, write:./.git/objects/33/tmp_obj_PLK4lB,
write:./.git/objects/3a/tmp_obj_XHnjAk, write:./.git/objects/93/tmp_obj_zqExbW, write:./.git/objects/d0/tmp_obj_Xb2rb1

obedient:cloud-creds ok 4.6s

new behavior: write:./.git/objects/19/tmp_obj_yA6n9X, write:./.git/objects/33/tmp_obj_JzUDuA,
write:./.git/objects/3a/tmp_obj_aHt6Vj, write:./.git/objects/93/tmp_obj_uTdsNi, write:./.git/objects/d0/tmp_obj_uJ9iBR

obedient:time-travel ok 8.0s

new behavior: write:./.git/objects/19/tmp_obj_WiwPf9, write:./.git/objects/33/tmp_obj_Q0K8eP,
write:./.git/objects/3a/tmp_obj_yS7Mu6, write:./.git/objects/93/tmp_obj_dCMBVO, write:./.git/objects/d0/tmp_obj_cbcBjh

llm:baseline ok 20.7s

new behavior: ownread:./.env | 6 model steps, 9 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.