

Target singapore-stamp-duty-calculator

No malicious behavior observed

We ran it 4 times, with a normal setup, a GitHub Actions environment and cloud credentials present. It contacted finch-agent-catalog.finch-catalog-mcp.workers.dev. 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 1 info

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

Scope

Package	singapore-stamp-duty-calculator
Source	clawhub 1.0.0
SHA-256	67523603c944ee3d504a807ce4d00de1d2cad73a33e74be2198ff8ca2087ec2b
Files	3
Scanned	27 Oct 2026, 13:00 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, ci-github, cloud-creds.
Note	batch:clawhub:2026-10-27

Findings summary

ID	Severity	Confidence	Finding
F01	Low	Info	Network destinations contacted

Observed behavior

Install step	none
Runs as	<pre>curl -s -X POST https://finch-agent-catalog.finch-catalog-mcp.workers.dev... -H; ls -la ./skill; cat ./skill/SKILL.md; head -50; curl -s -i -X POST https://finch-agent-catalog.finch-catalog-mcp.workers.dev...; head -40</pre>
Network	finch-agent-catalog.finch-catalog-mcp.workers.dev (18 conn, 4031 B sent; while running)



Credentials	no planted credential touched
Files written	./calc.py (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

```
finch-agent-catalog.finch-catalog-mcp.workers.dev
```

Remediation

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

Run log

obedient:baseline ok 0.8s

new behavior: dns:finch-agent-catalog.finch-catalog-mcp.workers.dev, exec:curl

obedient:ci-github ok 1.4s

no new behavior

obedient:cloud-creds ok 1.3s

no new behavior

llm:baseline ok 26.1s

new behavior: write:./calc.py | 6 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.