Target gtrk-style-maker

No malicious behavior observed

We ran it 1 time, with a normal setup. It made no network connections. It read some credential files, but nothing it sent carried them.

Recommendation	Confidence	Findings
No action needed	**n/a**	**0 high 0 med 3 info**

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

Scope

Package	gtrk-style-maker
Source	clawhub 1.3.9
SHA-256	98b314fe8824eb0cf672d97bdda842ffe19e0f5c12dd9b99db49558aea945653
Files	9
Scanned	27 Oct 2026, 11:49 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. 1 runs: baseline.
Note	batch:clawhub:2026-10-27

Findings summary

ID	Severity	Confidence	Finding
F01	Low	Info	Loaded the project's .env file
F02	Low	Info	Agent read credential files (may be the agent's own choice)
F03	Low	Info	Agent put secrets in the model's context (may be the agent's own choice)

Observed behavior

Install step	none
Runs as	ls -la; ls -R ./skill; head -50; which gtrk npx node; ls ~/.gitruck; ls ~/.gitruck/columns
Network	no connections
Credentials	./.env (read) ~/.bash_history (read)

	~/.npmrc (read)
Files written	nothing outside its own folder

Finding details

F01 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 cat)
```

Remediation

No action needed. Keep long-lived secrets out of project .env files where possible.

F02 Agent read credential files (may be the agent's own choice)

Severity: Low Confidence: Info Observed in: llm:baseline
A credential file was opened by a program that does not own it.

Description

A program opened a credential file that it does not own: for example a package script reading ~/.npmrc, ~/.aws/credentials or ~/.ssh/id_rsa, rather than npm, the AWS CLI or ssh reading their own files. The reading program is named in the evidence. In this run the contents were not seen leaving the sandbox.

Impact

Reading credentials is the collection step that precedes theft. Exfiltration may be gated on conditions this run did not meet (a different date, CI variables, a reachable network), or the data may be staged for a later step.

Evidence

```
~/.bash_history (by cat)
```

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

Remediation

Review why this package needs the file. Legitimate tools read only their own configuration; anything else should be treated as hostile until explained. Prefer running it with credentials unavailable (separate user, container, or scoped environment).

References

ATT&CK T1552.001 Credentials in Files
CWE-200 Exposure of Sensitive Information
OWASP MCP01:2025 Token Mismanagement & Secret Exposure

F03 Agent put secrets in the model's context (may be the agent's own choice)

Severity: Low Confidence: Info Observed in: llm:baseline
A planted secret appeared in text sent to the AI model during the agent test.

Description

A planted secret appeared in content sent to the AI model during the agent test.

Impact

The model provider saw the value; it did not leave through the package.

Evidence

```
~/.npmrc (npm)
```

```
~/.bash_history (history)
```

Remediation

Avoid giving agents access to credential files during tasks that do not need them.

References

OWASP LLM02:2025 Sensitive Information Disclosure

Run log

llm:baseline ok 53.8s

new behavior: ownread:./.env, read:~/.bash_history, read:~/.npmrc, write:~/.npm/_logs/*-debug-0.log | 7 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.