



Target mcp-exploit-demo

No malicious behavior observed

We ran it 3 times, with a normal setup, the clock moved a year ahead and a GitHub Actions environment. It made no network connections. 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 0 info

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

Scope

Package	mcp-exploit-demo
Source	github
SHA-256	d9771be562461305b54c06395c85d20203cf6c34ea6684ab4efb768677f05977
Files	3
Scanned	25 Oct 2026, 12:18 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. 3 runs: baseline, time-travel, ci-github.

Run log

mcp:baseline ok 0.4s
no new behavior | server did not complete the handshake: no response; 0 tool calls

mcp:time-travel ok 0.4s
no new behavior | server did not complete the handshake: no response; 0 tool calls

mcp:ci-github ok 0.4s
no new behavior | server did not complete the handshake: no response; 0 tool calls

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.