

matterpoll

github.com/matterpoll/matterpoll

Scanned 29 October 2026 at 10:14 · Report generated 29 October 2026 · Go · 299 stars

OVERALL ASSESSMENT

Medium

Combined score 30 · 8 findings after filtering

Summary

8 findings likely need attention. Most notable: Detects HTTP/HTTPS URL dependencies in package.json (dependency confusion, untrusted so... (98% confidence).

Generated from finding counts. A plain-English summary was not available for this scan.

Risk, by type

MalDet scores two different questions separately, because they call for different responses: code can be badly written without being hostile, and hostile code is not always badly written.

VULNERABILITY

Low (19)

Insecure coding an attacker could exploit. Usually mistakes, and usually fixable in place.

MALICIOUS PATTERN

Low (12)

Signs the code may be trying to do harm: hidden payloads, credential access, persistence, exfiltration.

What each detector found

DETECTOR	LOOKS FOR	HIGH	MEDIUM	LOW	TOTAL
semgrep	Insecure coding patterns across many languages	1	4	0	5
guarddog	Malicious package and install-time behaviour	1	0	2	3

8 of 8 findings were rated more likely genuine than noise by the classifier.

Evidence

Identical findings are grouped, so a single rule firing many times takes one row. Ordered worst first. “Seen” is how many times that finding occurred.

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
HIGH	guarddog	Detects HTTP/HTTPS URL dependencies in package.json (dependency confusion, untrusted sources) [threat-npm-http-dependency]	1	/webapp/package.json:108
HIGH	semgrep	This Node.js version file pins a runtime that is affected by CVE-2026-111497 (Brotli decoder out-of-bounds write, remote code execution) or a floating alias whose patch level cannot be verified. Pin to a fixed release 22.23.4, 24.22.1, 26.12.1 or later on the same line. Node.js 20 and older, 23 and	1	/.nvmrc:1
MEDIUM	semgrep	Detected 'io.WriteString()' writing directly to 'http.ResponseWriter'. This bypasses HTML escaping that prevents cross-site scripting vulnerabilities. Instead, use the 'html/template' package to render data to users.	1	/server/plugin/api.go:191
MEDIUM	semgrep	This .npmrc does not set a minimum release age or sets it too low. Newly published packages can be malicious or unstable. Add `min-release-age = 7` to wait 7 days before resolving newly published package versions. Added in: v11.10 Reference: https://github.blog/changelog/2026-02-18-npm-bulk-trusted-	1	/webapp/.npmrc:1
MEDIUM	semgrep	GitHub Actions step uses a mutable tag or branch reference. Tags and branch names can be silently repointed by the action owner, enabling supply-chain attacks — as seen in the trivy-action and kics-github-action compromises. Pin the reference to a full 40-character commit SHA instead, e.g. `uses: ac	2	/.github/workflows/check-mocks.yml:22
LOW	guarddog	Detects reading of environment variables (credential access, often contains secrets) [threat-runtime-environment-read]	2	/build/pluginctl/main.go:90

How to read this report

- **This is a static scan.** The code was read, never executed. Behaviour that only appears at runtime is outside what any of these detectors can see.

- **Findings are not all equally real.** A classifier rates each finding on how likely it is to be genuine rather than noise, and that rating weights the scores. Measured against a hand-reviewed sample it reached precision 0.52 and recall 0.62 — useful for ranking, not a verdict on any single finding.
- **A high score is not proof of malice.** Security tools, penetration-testing frameworks and malware research repositories contain the same patterns as real malware by design. The two risk types above exist to keep that distinction visible.
- **Absence of findings is not proof of safety.** A detector that is not installed, or a language none of them parse, produces silence rather than a warning.
- **This scan is a snapshot.** The repository may have changed since 29 October 2026.