

koel

github.com/koel/koel

Scanned 29 October 2026 at 09:43 · Report generated 29 October 2026 · PHP · 17,322 stars

OVERALL ASSESSMENT

Medium

Combined score 51 · 84 findings after filtering

Summary

16 findings likely need attention, 67 look like noise. Most notable: Executing non-constant commands. This can lead to command injection. (43% 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

Medium (49)

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

MALICIOUS PATTERN

Low (1)

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
dep_checker	Vulnerable, unpinned or typosquatted dependencies	0	0	64	64
semgrep	Insecure coding patterns across many languages	1	16	0	17
yara	Signatures of malicious behaviour in source files	3	0	0	3

16 of 84 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	semgrep	Executing non-constant commands. This can lead to command injection.	1	/scripts/koel-init.php:7
HIGH	yara	YARA rule matched: detect_download_and_execute — Downloads a remote resource AND executes it - the actually dangerous combination, not just downloading alone	3	/CLAUDE.md
MEDIUM	semgrep	RegExp() called with a `route` function argument, this might allow an attacker to cause a Regular Expression Denial-of-Service (ReDoS) within your application as RegExp blocks the main thread. For this reason, it is recommended to use hardcoded regexes instead. If your regex is run on user-controlled	1	/resources/assets/js/router.ts:71
MEDIUM	semgrep	Dynamically rendering arbitrary HTML on your website can be very dangerous because it can easily lead to XSS vulnerabilities. Only use HTML interpolation on trusted content and never on user-provided content.	8	/resources/assets/js/components/artist/ArtistInfo.vue:11
MEDIUM	semgrep	This pnpm workspace configuration does not set a minimum release age. Newly published packages can be malicious or unstable. Add `minimumReleaseAge: 10080` (minutes) to wait at least seven days before installing newly published package versions. Added in: v10.16.0 Reference: https://pnpm.io/settings	1	/pnpm-workspace.yaml:6
MEDIUM	semgrep	A secret is hard-coded in the application. Secrets stored in source code, such as credentials, identifiers, and other types of sensitive data, can be leaked and used by internal or external malicious actors. It is recommended to rotate the secret and retrieve them from a secure secret vault or Hardw	2	/config/database.php:140
MEDIUM	semgrep	Missing or incorrect trustPolicy. Set `trustPolicy: no-downgrade` to prevent malicious package updates from downgrading security settings. Added in: v10.21.0 Reference: https://pnpm.io/settings#trustpolicy	1	/pnpm-workspace.yaml:6

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
MEDIUM	semgrep	Missing or incorrect blockExoticSubdeps. Set `blockExoticSubdeps: true` to transitive dependencies from being installed from untrusted sources. Added in: v10.26.0 Reference: https://pnpm.io/settings#blockexoticsubdeps	1	/pnpm-workspace.yaml:6
MEDIUM	semgrep	Depending on the context, user control data in `Object.assign` can cause web response to include data that it should not have or can lead to a mass assignment vulnerability.	1	/resources/assets/js/services/httpUpload.ts:73
MEDIUM	semgrep	File name based on user input risks server-side request forgery.	1	/server.php:15
LOW	dep_checker	Loose version constraint: '@testing-library/user-event^14.6.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@fortawesome/free-regular-svg-icons^6.7.2' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@testing-library/vue^6.6.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'laravel-echo^2.1.6' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'jsdom^26.1.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'laravel-vite-plugin^2.1.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'lodash-es^4.18.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'lucide-vue-next^0.577.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'marked^17.0.4' — attacker could push malicious update	1	package.json

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
LOW	dep_checker	Loose version constraint: 'nouislider^14.7.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'nprogress^0.2.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'postcss-mixins^10.0.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'postcss-nested^6.2.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'postcss^8.5.23' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'pusher-js^8.6.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'qrcode^1.5.4' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'rollup-plugin-visualizer^6.0.3' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'style-observer^0.1.2' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'tailwindcss^4.3.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'three^0.146.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'tiny-typed-emitter^2.1.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'typescript^5.8.3' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'vitepress-plugin-lms^1.11.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'vitepress^1.6.3' — attacker could push malicious update	1	package.json

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
LOW	dep_checker	Loose version constraint: 'vue-advanced-cropper^2.8.9' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'vue-chartjs^5.3.4' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'vue-tsc^3.2.5' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'vue^3.5.44' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'youtube-player^5.6.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@tailwindcss/postcss^4.3.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@types/three^0.144.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@types/pusher-js^4.2.2' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@types/nprogress^0.2.3' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@types/lodash-es^4.17.12' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@tiptap/vue-3^3.31.4' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@tiptap/starter-kit^3.31.4' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@tiptap/pm^3.31.4' — attacker could push malicious update	1	package.json

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
LOW	dep_checker	Loose version constraint: '@tailwindcss/vite^4.3.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@types/youtube-player^5.5.11' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@laravel/echo-vue^2.1.6' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@fortawesome/vue-fontawesome^3.0.8' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@fortawesome/free-solid-svg-icons^6.7.2' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@fortawesome/free-brands-svg-icons^6.7.2' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@fortawesome/fontawesome-svg-core^6.7.2' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@floating-ui/dom^1.7.2' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@faker-js/faker^10.5.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@commitlint/config-conventional^19.8.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'dompurify^3.4.17' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@commitlint/cli^19.8.1' — attacker could push malicious update	1	package.json

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
LOW	dep_checker	Loose version constraint: 'jest-serializer-vue^2.0.2' — attacker could push malicious update	1	package.json

Showing the 60 most significant of 74 distinct findings. The counts in the previous section cover all of them.

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.