

kiro-account-manager

github.com/hj01857655/kiro-account-manager

Scanned 30 October 2026 at 09:17 · Report generated 30 October 2026 · Rust · 2,057 stars

OVERALL ASSESSMENT

High

Combined score 117 · 66 findings after filtering

Summary

26 findings likely need attention, 39 look like noise. Most notable: The application builds a file path from potentially untrusted data, which can lead to a... (100% 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

High (116)

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	37	37
semgrep	Insecure coding patterns across many languages	12	14	1	27
yara	Signatures of malicious behaviour in source files	0	0	2	2

26 of 66 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	The application builds a file path from potentially untrusted data, which can lead to a path traversal vulnerability. An attacker can manipulate the path which the application uses to access files. If the application does not validate user input and sanitize file paths, sensitive files such as confi	6	/src-tauri/src/services/session_storage.rs:310
HIGH	semgrep	Using variable interpolation `\${{...}}` with `github` context data in a `run:` step could allow an attacker to inject their own code into the runner. This would allow them to steal secrets and code. `github` context data can have arbitrary user input and should be treated as untrusted. Instead, use	6	/.github/workflows/release.yml:290
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	14	/.github/workflows/build.yml:77
LOW	semgrep	Detected string concatenation with a non-literal variable in a util.format / console.log function. If an attacker injects a format specifier in the string, it will forge the log message. Try to use constant values for the format string.	1	/src/utils/errorLogger.ts:11
LOW	dep_checker	Loose version constraint: '@types/react^18.3.18' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@radix-ui/react-accordion^1.2.12' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@vitejs/plugin-react^4.2.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'class-variance-authority^0.7.1' — attacker could push malicious update	1	package.json

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
LOW	dep_checker	Loose version constraint: 'clsx^2.1.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'cmdk^1.1.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'lucide-react^0.294.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'next-themes^0.4.6' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'react-dom^18.2.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'react^18.2.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'recharts^3.10.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'sonner^2.0.7' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'tailwind-merge^3.4.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'tailwindcss^4.0.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'tw-animate-css^1.4.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'typescript^5.9.3' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'vite^5.0.8' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@types/node^25.6.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@base-ui/react^1.4.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@radix-ui/react-checkbox^1.3.3' — attacker could push malicious update	1	package.json

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
LOW	dep_checker	Loose version constraint: '@radix-ui/react-dialog^1.1.15' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@radix-ui/react-dropdown-menu^2.1.16' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@radix-ui/react-label^2.1.8' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@radix-ui/react-popover^1.1.15' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@radix-ui/react-progress^1.1.8' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@radix-ui/react-scroll-area^1.2.10' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@radix-ui/react-select^2.2.6' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@radix-ui/react-separator^1.1.8' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@radix-ui/react-slot^1.2.4' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@radix-ui/react-switch^1.2.6' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@radix-ui/react-tabs^1.1.13' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@radix-ui/react-tooltip^1.2.8' — attacker could push malicious update	1	package.json

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
LOW	dep_checker	Loose version constraint: '@tailwindcss/vite^4.0.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@tauri-apps/plugin-fs^2.4.5' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@tauri-apps/plugin-opener^2.5.3' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@tauri-apps/plugin-process^2.3.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@types/react-dom^18.3.5' — attacker could push malicious update	1	package.json
LOW	yara	YARA rule matched: detect_downloader — Downloads a remote resource - common and low-signal alone; see detect_download_and_execute for the composite version	2	/.github/workflows/release.yml

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 30 October 2026.