

blackbox-log-viewer

github.com/betaflight/blackbox-log-viewer

Scanned 24 September 2026 at 10:07 · Report generated 29 October 2026 · JavaScript · 507 stars

OVERALL ASSESSMENT

Medium

Combined score 27 · 32 findings after filtering

Summary

This repository has a medium vulnerability score of 23.0, which indicates that some code patterns are insecure and could potentially be exploited by an attacker to steal secrets or execute malicious code. However, the scan also identified a low-risk score of 4.0 for signs of intentional malicious intent, suggesting the code is likely not designed to harm users directly. The most concerning finding involves using variable interpolation in GitHub Actions workflows, which allows attackers to inject their own code and potentially bypass security controls. While this specific issue appears to be an ordinary insecure coding practice rather than a deliberate attempt to attack the system, it still represents a significant risk if left unaddressed. Additionally, there are several loose version constraints in the dependencies that could allow malicious updates to slip through, though these are considered low priority and unlikely to cause immediate harm.

Written by a language model running locally on the scanning machine, from the findings in this report. The risk levels above and below were decided by the scoring model, not by this summary.

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 (23)

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

MALICIOUS PATTERN

Low (4)

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	21	21
semgrep	Insecure coding patterns across many languages	1	9	0	10
yara	Signatures of malicious behaviour in source files	1	0	0	1

10 of 32 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	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	1	/.github/workflows/deploy.yml:49
HIGH	yara	YARA rule matched: detect_crypto_miner — Cryptocurrency mining pool connection patterns	1	/package-lock.json
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.	2	/src/components/ConfigurationPanel.vue:32
MEDIUM	semgrep	RegExp() called with a `field` 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	/src/graph_config.js:53

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
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	6	/.github/workflows/build.yml:27
LOW	dep_checker	Loose version constraint: 'sortablejs^1.15.7' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'webm-writer^1.0.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'vue^3.5.33' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'vue-router^4.6.4' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'vite^8.0.16' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'vite-plugin-pwa^1.3.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'throttle-debounce^5.0.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'tailwindcss^4.2.4' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@eslint/js^10.0.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'semver^7.7.4' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'prettier^3.8.3' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'pinia^3.0.4' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'leaflet^1.9.3' — attacker could push malicious update	1	package.json

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
LOW	dep_checker	Loose version constraint: 'leaflet-marker-rotation^0.4.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'html2canvas^1.0.0-rc.5' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'globals^17.6.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'eslint^10.3.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'eslint-config-prettier^10.1.8' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@vitejs/plugin-vue^6.0.6' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@nuxt/ui^4.8.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@iconify-json/lucide^1.2.105' — attacker could push malicious update	1	package.json

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 24 September 2026.