

k8s-gitops

github.com/xunholy/k8s-gitops

Scanned 29 October 2026 at 10:31 · Report generated 29 October 2026 · PHP · 643 stars

OVERALL ASSESSMENT

Medium

Combined score 40 · 31 findings after filtering

Summary

10 findings likely need attention, 19 look like noise. Most notable: Detects keylogging and input capture patterns [threat-runtime-keylogging] (94% 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

Medium (21)

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	0	13	5	18
guarddog	Malicious package and install-time behaviour	1	1	5	7
yara	Signatures of malicious behaviour in source files	4	0	2	6

10 of 31 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 keylogging and input capture patterns [threat-runtime-keylogging]	1	/kubernetes/ apps/base/ network-system/ dex-k8s- authenticator/ app/resources/ html/static/ highlight.pack. min.js:1
HIGH	yara	YARA rule matched: detect_process_injection — Windows process-injection API sequence	1	/kubernetes/ apps/base/ network-system/ dex-k8s- authenticator/ app/resources/ html/static/ highlight.pack. min.js
HIGH	yara	YARA rule matched: detect_download_and_execute — Downloads a remote resource AND executes it - the actually dangerous combination, not just downloading alone	2	/kubernetes/ apps/base/ai- system/hermes/ app/ helmrelease.ya ml
HIGH	yara	YARA rule matched: detect_persistence_mechanism — Modifies a startup/scheduling location - legitimate application code essentially never does this	1	/kubernetes/ apps/base/ network-system/ dex-k8s- authenticator/ app/resources/ html/static/ highlight.pack. min.js
MEDIUM	semgrep	Pod may use the node network namespace. This gives the pod access to the loopback device, services listening on localhost, and could be used to snoop on network activity of other pods on the same node. Remove the 'hostNetwork' key to disable this functionality.	3	/talos/ integrations/ cilium/ cilium.yaml:139 51

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
MEDIUM	guarddog	Detects unicode homoglyphs and uncommon characters used for obfuscation [threat-runtime-obfuscation-unicode]	1	/kubernetes/apps/base/network-system/dex-k8s-authenticator/app/resources/html/static/highlight.pack.min.js:1
MEDIUM	semgrep	Found an HTTP server without TLS. Use 'http.ListenAndServeTLS' instead. See https://golang.org/pkg/net/http/#ListenAndServeTLS for more information.	1	/kubernetes/apps/base/network-system/dex-k8s-authenticator/app/resources/main.go:290
MEDIUM	semgrep	In Kubernetes, each pod runs in its own isolated environment with its own set of security policies. However, certain container images may contain `setuid` or `setgid` binaries that could allow an attacker to perform privilege escalation and gain access to sensitive resources. To mitigate this risk,	1	/talos/integrations/cilium/cilium.yaml:13519
MEDIUM	semgrep	In Kubernetes, each pod runs in its own isolated environment with its own set of security policies. However, certain container images may contain `setuid` or `setgid` binaries that could allow an attacker to perform privilege escalation and gain access to sensitive resources. To mitigate this risk,	8	/kubernetes/apps/base/game-servers/cmangos-ptr/app/db-init-job.yaml:27
LOW	guarddog	Detects DLL injection and process injection techniques [threat-process-injection-dll]	2	/kubernetes/apps/base/network-system/dex-k8s-authenticator/app/resources/html/static/highlight.pack.min.js:1

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
LOW	guarddog	Detects memory scraping and credential dumping from process memory [threat-process-memory]	3	/kubernetes/apps/base/network-system/dex-k8s-authenticator/app/resources/html/static/highlight.pack.min.js:1
LOW	semgrep	When running containers in Kubernetes, it's important to ensure that they are properly secured to prevent privilege escalation attacks. One potential vulnerability is when a container is allowed to run applications as the root user, which could allow an attacker to gain access to sensitive resou	5	/kubernetes/apps/base/preview-system/preview-system/app/resourceset.yaml:103
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	/kubernetes/apps/base/network-system/dex-k8s-authenticator/app/resources/html/static/highlight.pack.min.js

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.