MALDET · STATIC SECURITY REPORT

cadence

github.com/cadence-workflow/cadence

Scanned 30 October 2026 at 03:12 · Report generated 30 October 2026 · Go · 9,529 stars

OVERALL ASSESSMENT

Critical

Combined score 580 · 267 findings after filtering

Summary

202 findings likely need attention, 3 look like noise. Most notable: Missing mutex unlock (`a.mut` variable) before returning from a function. This could r... (99% 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

Critical (578)

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

MALICIOUS PATTERN

Low (2)

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	13	249	0	**262**
yara	Signatures of malicious behaviour in source files	0	0	3	**3**
guarddog	Malicious package and install-time behaviour	0	0	2	**2**

202 of 267 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	Missing mutex unlock (`a.mut` variable) before returning from a function. This could result in panics resulting from double lock operations	4	`/common/quotas/global/algorithm/requestweighted.go:476`
HIGH	semgrep	Missing mutex unlock (`r.mut` variable) before returning from a function. This could result in panics resulting from double lock operations	2	`/common/clock/ratelimiter.go:241`
HIGH	semgrep	Missing mutex unlock (`c.mut` variable) before returning from a function. This could result in panics resulting from double lock operations	1	`/common/cache/lru.go:141`
HIGH	semgrep	Detected non-static command inside Command. Audit the input to 'exec.Command'. If unverified user data can reach this call site, this is a code injection vulnerability. A malicious actor can inject a malicious script to execute arbitrary code.	4	`/common/scripting/exec.go:33`
HIGH	semgrep	Private Key detected. This is a sensitive credential and should not be hardcoded here. Instead, store this in a separate, private file.	2	`/config/credentials/client.key:1`
MEDIUM	semgrep	Variable `details` is likely modified and later used on error. In some cases this could result in panics due to a nil dereference	8	`/common/dynamicconfig/openfeatureclient/client.go:285`
MEDIUM	semgrep	Service 'kafka' is running with a writable root filesystem. This may allow malicious applications to download and run additional payloads, or modify container files. If an application inside a container has to save something temporarily consider using a tmpfs. Add 'read_only: true' to this service t	6	`/docker/dev/mongo-esv7-kafka.yml:27`

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
MEDIUM	semgrep	Service 'cassandra' is running with a writable root filesystem. This may allow malicious applications to download and run additional payloads, or modify container files. If an application inside a container has to save something temporarily consider using a tmpfs. Add 'read_only: true' to this servi	5	`/docker/docker-compose-multiclusters-cass-mysql-es.yaml:3`
MEDIUM	semgrep	Variable `profile` is likely modified and later used on error. In some cases this could result in panics due to a nil dereference	2	`/canary/cancellation.go:220`
MEDIUM	semgrep	Variable `resp` is likely modified and later used on error. In some cases this could result in panics due to a nil dereference	1	`/service/history/handler/handler.go:1153`
MEDIUM	semgrep	Service 'zookeeper' is running with a writable root filesystem. This may allow malicious applications to download and run additional payloads, or modify container files. If an application inside a container has to save something temporarily consider using a tmpfs. Add 'read_only: true' to this servi	1	`/docker/dev/cassandra-pinot-kafka.yml:10`
MEDIUM	semgrep	Service 'pinot-broker' is running with a writable root filesystem. This may allow malicious applications to download and run additional payloads, or modify container files. If an application inside a container has to save something temporarily consider using a tmpfs. Add 'read_only: true' to this se	1	`/docker/dev/cassandra-pinot-kafka.yml:29`
MEDIUM	semgrep	Service 'cadence' is running with a writable root filesystem. This may allow malicious applications to download and run additional payloads, or modify container files. If an application inside a container has to save something temporarily consider using a tmpfs. Add 'read_only: true' to this service	1	`/docker/docker-compose-multiclusters-cass-mysql-es.yaml:54`

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
MEDIUM	semgrep	Service 'opensearch-dashboards' is running with a writable root filesystem. This may allow malicious applications to download and run additional payloads, or modify container files. If an application inside a container has to save something temporarily consider using a tmpfs. Add 'read_only: true' t	1	`/docker/dev/cassandra-opensearch-kafka-migration.yml:28`
MEDIUM	semgrep	Service 'cadence-secondary' is running with a writable root filesystem. This may allow malicious applications to download and run additional payloads, or modify container files. If an application inside a container has to save something temporarily consider using a tmpfs. Add 'read_only: true' to th	1	`/docker/docker-compose-multiclusters-cass-mysql-es.yaml:96`
MEDIUM	semgrep	Service 'mongo' is running with a writable root filesystem. This may allow malicious applications to download and run additional payloads, or modify container files. If an application inside a container has to save something temporarily consider using a tmpfs. Add 'read_only: true' to this service t	1	`/docker/dev/mongo-esv7-kafka.yml:3`
MEDIUM	semgrep	Service 'cadence-web' is running with a writable root filesystem. This may allow malicious applications to download and run additional payloads, or modify container files. If an application inside a container has to save something temporarily consider using a tmpfs. Add 'read_only: true' to this ser	1	`/docker/docker-compose-multiclusters-cass-mysql-es.yaml:136`
MEDIUM	semgrep	Service 'opensearch' is running with a writable root filesystem. This may allow malicious applications to download and run additional payloads, or modify container files. If an application inside a container has to save something temporarily consider using a tmpfs. Add 'read_only: true' to this serv	1	`/docker/dev/cassandra-opensearch-kafka-migration.yml:10`

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
MEDIUM	semgrep	Service 'mongo-express' is running with a writable root filesystem. This may allow malicious applications to download and run additional payloads, or modify container files. If an application inside a container has to save something temporarily consider using a tmpfs. Add 'read_only: true' to this s	1	`/docker/dev/mongo-esv7-kafka.yml:12`
MEDIUM	semgrep	Service 'pinot-server' is running with a writable root filesystem. This may allow malicious applications to download and run additional payloads, or modify container files. If an application inside a container has to save something temporarily consider using a tmpfs. Add 'read_only: true' to this se	1	`/docker/dev/cassandra-pinot-kafka.yml:40`
MEDIUM	semgrep	Service 'pinot-controller' is running with a writable root filesystem. This may allow malicious applications to download and run additional payloads, or modify container files. If an application inside a container has to save something temporarily consider using a tmpfs. Add 'read_only: true' to thi	1	`/docker/dev/cassandra-pinot-kafka.yml:18`
MEDIUM	semgrep	Service 'mysql' is running with a writable root filesystem. This may allow malicious applications to download and run additional payloads, or modify container files. If an application inside a container has to save something temporarily consider using a tmpfs. Add 'read_only: true' to this service t	3	`/docker/dev/mysql.yml:3`
MEDIUM	semgrep	Service 'grafana' is running with a writable root filesystem. This may allow malicious applications to download and run additional payloads, or modify container files. If an application inside a container has to save something temporarily consider using a tmpfs. Add 'read_only: true' to this service	1	`/docker/docker-compose-multiclusters-cass-mysql-es.yaml:148`

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
MEDIUM	semgrep	Service 'prometheus' is running with a writable root filesystem. This may allow malicious applications to download and run additional payloads, or modify container files. If an application inside a container has to save something temporarily consider using a tmpfs. Add 'read_only: true' to this serv	1	`/docker/docker-compose-multiclusters-cass-mysql-es.yaml:21`
MEDIUM	semgrep	Service 'elasticsearch' is running with a writable root filesystem. This may allow malicious applications to download and run additional payloads, or modify container files. If an application inside a container has to save something temporarily consider using a tmpfs. Add 'read_only: true' to this s	5	`/docker/docker-compose-multiclusters-cass-mysql-es.yaml:48`
MEDIUM	semgrep	Service 'mongo-express' allows for privilege escalation via setuid or setgid binaries. Add 'no-new-privileges:true' in 'security_opt' to prevent this.	1	`/docker/dev/mongo-esv7-kafka.yml:12`
MEDIUM	semgrep	Service 'elasticsearch' allows for privilege escalation via setuid or setgid binaries. Add 'no-new-privileges:true' in 'security_opt' to prevent this.	5	`/docker/dev/cassandra-opensearch-kafka-migration.yml:22`
MEDIUM	semgrep	Service 'pinot-controller' allows for privilege escalation via setuid or setgid binaries. Add 'no-new-privileges:true' in 'security_opt' to prevent this.	1	`/docker/dev/cassandra-pinot-kafka.yml:18`
MEDIUM	semgrep	Service 'opensearch-dashboards' allows for privilege escalation via setuid or setgid binaries. Add 'no-new-privileges:true' in 'security_opt' to prevent this.	1	`/docker/dev/cassandra-opensearch-kafka-migration.yml:28`
MEDIUM	semgrep	Service 'cadence-secondary' allows for privilege escalation via setuid or setgid binaries. Add 'no-new-privileges:true' in 'security_opt' to prevent this.	1	`/docker/docker-compose-multiclusters-cass-mysql-es.yaml:96`

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
MEDIUM	semgrep	Service 'kafka' allows for privilege escalation via setuid or setgid binaries. Add 'no-new-privileges:true' in 'security_opt' to prevent this.	6	/docker/dev/cassandra-opensearch-kafka-migration.yml:37
MEDIUM	semgrep	Service 'cassandra' allows for privilege escalation via setuid or setgid binaries. Add 'no-new-privileges:true' in 'security_opt' to prevent this.	5	/docker/dev/cassandra-opensearch-kafka-migration.yml:3
MEDIUM	semgrep	Service 'mongo' allows for privilege escalation via setuid or setgid binaries. Add 'no-new-privileges:true' in 'security_opt' to prevent this.	1	/docker/dev/mongo-esv7-kafka.yml:3
MEDIUM	semgrep	Service 'zookeeper' allows for privilege escalation via setuid or setgid binaries. Add 'no-new-privileges:true' in 'security_opt' to prevent this.	1	/docker/dev/cassandra-pinot-kafka.yml:10
MEDIUM	semgrep	Service 'opensearch' allows for privilege escalation via setuid or setgid binaries. Add 'no-new-privileges:true' in 'security_opt' to prevent this.	1	/docker/dev/cassandra-opensearch-kafka-migration.yml:10
MEDIUM	semgrep	Service 'cadence-web' allows for privilege escalation via setuid or setgid binaries. Add 'no-new-privileges:true' in 'security_opt' to prevent this.	1	/docker/docker-compose-multiclusters-cass-mysql-es.yaml:136
MEDIUM	semgrep	Service 'pinot-broker' allows for privilege escalation via setuid or setgid binaries. Add 'no-new-privileges:true' in 'security_opt' to prevent this.	1	/docker/dev/cassandra-pinot-kafka.yml:29
MEDIUM	semgrep	Service 'cadence' allows for privilege escalation via setuid or setgid binaries. Add 'no-new-privileges:true' in 'security_opt' to prevent this.	1	/docker/docker-compose-multiclusters-cass-mysql-es.yaml:54

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
MEDIUM	semgrep	Service 'mysql' allows for privilege escalation via setuid or setgid binaries. Add 'no-new-privileges:true' in 'security_opt' to prevent this.	3	`/docker/dev/mysql.yml:3`
MEDIUM	semgrep	Service 'prometheus' allows for privilege escalation via setuid or setgid binaries. Add 'no-new-privileges:true' in 'security_opt' to prevent this.	1	`/docker/docker-compose-multiclusters-cass-mysql-es.yaml:21`
MEDIUM	semgrep	Service 'grafana' allows for privilege escalation via setuid or setgid binaries. Add 'no-new-privileges:true' in 'security_opt' to prevent this.	1	`/docker/docker-compose-multiclusters-cass-mysql-es.yaml:148`
MEDIUM	semgrep	Service 'pinot-server' allows for privilege escalation via setuid or setgid binaries. Add 'no-new-privileges:true' in 'security_opt' to prevent this.	1	`/docker/dev/cassandra-pinot-kafka.yml:40`
MEDIUM	semgrep	Downcasting or changing sign of an integer with `int32` method	3	`/common/cache/domainCache.go:997`
MEDIUM	semgrep	Service 'postgres' allows for privilege escalation via setuid or setgid binaries. Add 'no-new-privileges:true' in 'security_opt' to prevent this.	1	`/docker/dev/postgres.yml:3`
MEDIUM	semgrep	Service 'postgres' is running with a writable root filesystem. This may allow malicious applications to download and run additional payloads, or modify container files. If an application inside a container has to save something temporarily consider using a tmpfs. Add 'read_only: true' to this servic	1	`/docker/dev/postgres.yml:3`
MEDIUM	semgrep	Detected MD5 hash algorithm which is considered insecure. MD5 is not collision resistant and is therefore not suitable as a cryptographic signature. Use SHA256 or SHA3 instead.	2	`/schema/common/schema.go:158`

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
MEDIUM	semgrep	String-formatted SQL query detected. This could lead to SQL injection if the string is not sanitized properly. Audit this call to ensure the SQL is not manipulable by external data.	3	`/common/persistence/nosql/nosqlplugin/cassandra/setup.go:44`
MEDIUM	semgrep	`MinVersion` is missing from this TLS configuration. By default, as of Go 1.22, TLS 1.2 is currently used as the minimum. General purpose web applications should default to TLS 1.3 with all other protocols disabled. Only where it is known that a web server must support legacy clients with unsuppor	5	`/common/config/tls.go:69`
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	101	`/.github/workflows/codecov-on-pr.yml:26`
MEDIUM	semgrep	When working with web applications that involve rendering user-generated content, it's important to properly escape any HTML content to prevent Cross-Site Scripting (XSS) attacks. In Go, the `text/template` package does not automatically escape HTML content, which can leave your application vuln	1	`/tools/cli/render.go:31`
MEDIUM	semgrep	Deserializing into `interface{}` allows arbitrary data structures and types, which can lead to security vulnerabilities (CWE-502). Use a concrete struct type instead.	9	`/tools/cli/workflow_commands.go:1421`
MEDIUM	semgrep	Found an HTTP server without TLS. Use 'http.ListenAndServeTLS' instead. See https://golang.org/pkg/net/http/#ListenAndServeTLS for more information.	2	`/simulation/replication/worker/cmd/main.go:114`
MEDIUM	semgrep	Do not use `math/rand`. Use `crypto/rand` instead.	46	`/tools/cli/workflow_commands.go:31`

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
LOW	guarddog	Detects reading of environment variables (credential access, often contains secrets) [threat-runtime-environment-read]	2	`/common/persistence/sql/sqlplugin/postgres/plugin.go:177`
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	3	`/scripts/travis/install-xdc-deps.sh`

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.