

Cequence UAP Release version:7.7.0 - Image Vulnerability Scan Summary

Image	Severity	Vuln count
registry.gitlab.com/cequence/releases/platform/api-gateway:7.7.0	N/A	Pass
registry.gitlab.com/cequence/releases/platform/integration-executor:7.7.0	N/A	Pass
registry.gitlab.com/cequence/releases/platform/upgrade-init:7.7.0	N/A	Pass
registry.gitlab.com/cequence/releases/third-party/pause:3.2	N/A	Pass
registry.gitlab.com/cequence/releases/cqai/stats-streams:7.7.0	N/A	Pass
registry.gitlab.com/cequence/releases/cqai/bot-analyzer:7.7.0	N/A	Pass
registry.gitlab.com/cequence/releases/platform/component-configuration:7.7.0	N/A	Pass
registry.gitlab.com/cequence/releases/platform/api-edge:7.7.0	N/A	Pass
registry.gitlab.com/cequence/releases/api-spyder-portal:7.7.0	N/A	Pass
registry.gitlab.com/cequence/releases/dataplane/sensorbridge:7.7.0	N/A	Pass
registry.gitlab.com/cequence/releases/platform/ui:7.7.0	N/A	Pass
registry.gitlab.com/cequence/releases/api-testing/cloud-updates:7.7.0	N/A	Pass
registry.gitlab.com/cequence/releases/platform/distribution-service:7.7.0	N/A	Pass
registry.gitlab.com/cequence/releases/platform/docs/user-guide:7.7.0	N/A	Pass
registry.gitlab.com/cequence/releases/api-testing/fury-runner:1.6.0	High	1
registry.gitlab.com/cequence/releases/cqai/data-science/cequence-airflow:7.7.0	Critical	1
registry.gitlab.com/cequence/releases/cqai/data-science/cequence-airflow:7.7.0	High	20
registry.gitlab.com/cequence/releases/cqai/policy-engine:7.7.0	Critical	1
registry.gitlab.com/cequence/releases/cqai/policy-engine:7.7.0	High	2
registry.gitlab.com/cequence/releases/platform/defender-configuration:7.7.0	High	4
registry.gitlab.com/cequence/releases/platform/resource-discovery:7.7.0	High	1
registry.gitlab.com/cequence/releases/platform/strimzi-kafka-connect:7.7.0	Critical	2
registry.gitlab.com/cequence/releases/platform/strimzi-kafka-connect:7.7.0	High	35
registry.gitlab.com/cequence/releases/third-party/bitnami/keycloak:26.0.5-debian-12-r0	High	5
registry.gitlab.com/cequence/releases/third-party/bitnami/postgresql:16.1.0-debian-11-r15	Critical	10
registry.gitlab.com/cequence/releases/third-party/bitnami/postgresql:16.1.0-debian-11-r15	High	27
registry.gitlab.com/cequence/releases/third-party/bitnami/postgresql:17.0.0-debian-12-r1	High	3
registry.gitlab.com/cequence/releases/third-party/bitnami/redis:7.4.1-debian-12-r2	High	2
registry.gitlab.com/cequence/releases/third-party/eck/eck-operator:2.11.0	Critical	1
registry.gitlab.com/cequence/releases/third-party/eck/eck-operator:2.11.0	High	14
registry.gitlab.com/cequence/releases/third-party/elasticsearch/elasticsearch:7.17.21	Critical	1
registry.gitlab.com/cequence/releases/third-party/elasticsearch/elasticsearch:7.17.21	High	9
registry.gitlab.com/cequence/releases/third-party/grafana/grafana:11.3.0	High	5
registry.gitlab.com/cequence/releases/third-party/kube-state-metrics/kube-state-metrics:v2.13.0	High	7
registry.gitlab.com/cequence/releases/third-party/prometheus-operator/prometheus-config-reloader:v0.77.2	High	4
registry.gitlab.com/cequence/releases/third-party/prometheus-operator/prometheus-operator:v0.77.2	High	3
registry.gitlab.com/cequence/releases/third-party/prometheus/node-exporter:v1.8.2	High	7
registry.gitlab.com/cequence/releases/third-party/prometheus/prometheus:v2.55.0	High	4

registry.gitlab.com/cequence/releases/third-party/prometheuscommunity/elasticsearch-exporter:v1.7.0	Critical	1
registry.gitlab.com/cequence/releases/third-party/prometheuscommunity/elasticsearch-exporter:v1.7.0	High	14
registry.gitlab.com/cequence/releases/third-party/strimzi/kafka:0.41.0-kafka-3.7.0	Critical	1
registry.gitlab.com/cequence/releases/third-party/strimzi/kafka:0.41.0-kafka-3.7.0	High	29
registry.gitlab.com/cequence/releases/third-party/strimzi/operator:0.41.0	High	5

Vulnerability Details per Image

Image	Severity	Vulnerability_Id	FixStatus
registry.gitlab.com/cequence/releases/api-sentinel/resource-dictionary:7.7.0	Critical	CVE-2025-24813	New vulnerability
registry.gitlab.com/cequence/releases/api-sentinel/spec-parser:7.7.0	High	CVE-2025-27152	New vulnerability
registry.gitlab.com/cequence/releases/api-sentinel/spec-parser:7.7.0	High	CVE-2025-27789	New vulnerability
registry.gitlab.com/cequence/releases/api-sentinel/traffic-analyzer:7.7.0	Critical	CVE-2025-24813	New vulnerability
registry.gitlab.com/cequence/releases/api-testing/fury-runner:1.6.0	High	CVE-2024-12797	New vulnerability
registry.gitlab.com/cequence/releases/api-testing/fury-runner:1.6.0	High	CVE-2024-12905	Fix in Next Release
registry.gitlab.com/cequence/releases/api-testing/fury-runner:1.6.0	High	CVE-2025-27152	New vulnerability
registry.gitlab.com/cequence/releases/cqai/data-science/cequence-airflow:7.7.0	Critical	CVE-2024-12084	Fix not available
registry.gitlab.com/cequence/releases/cqai/data-science/cequence-airflow:7.7.0	Critical	CVE-2024-55549	New vulnerability
registry.gitlab.com/cequence/releases/cqai/data-science/cequence-airflow:7.7.0	Critical	CVE-2024-56406	New vulnerability
registry.gitlab.com/cequence/releases/cqai/data-science/cequence-airflow:7.7.0	Critical	CVE-2025-24855	New vulnerability
registry.gitlab.com/cequence/releases/cqai/data-science/cequence-airflow:7.7.0	Critical	CVE-2025-27018	New vulnerability
registry.gitlab.com/cequence/releases/cqai/data-science/cequence-airflow:7.7.0	High	CVE-2023-46136	Fix not available
registry.gitlab.com/cequence/releases/cqai/data-science/cequence-airflow:7.7.0	High	CVE-2023-7104	Fix not available
registry.gitlab.com/cequence/releases/cqai/data-science/cequence-airflow:7.7.0	High	CVE-2024-12797	New vulnerability
registry.gitlab.com/cequence/releases/cqai/data-science/cequence-airflow:7.7.0	High	CVE-2024-21096	Fix not available
registry.gitlab.com/cequence/releases/cqai/data-science/cequence-airflow:7.7.0	High	CVE-2024-34069	Fix not available
registry.gitlab.com/cequence/releases/cqai/data-science/cequence-airflow:7.7.0	High	CVE-2024-45033	Fix not available
registry.gitlab.com/cequence/releases/cqai/data-science/cequence-airflow:7.7.0	High	CVE-2024-45336	Fix not available
registry.gitlab.com/cequence/releases/cqai/data-science/cequence-airflow:7.7.0	High	CVE-2024-45341	Fix not available
registry.gitlab.com/cequence/releases/cqai/data-science/cequence-airflow:7.7.0	High	CVE-2024-49767	Fix not available
registry.gitlab.com/cequence/releases/cqai/data-science/cequence-airflow:7.7.0	High	CVE-2024-52303	Fix not available
registry.gitlab.com/cequence/releases/cqai/data-science/cequence-airflow:7.7.0	High	CVE-2024-52804	Fix not available
registry.gitlab.com/cequence/releases/cqai/data-science/cequence-airflow:7.7.0	High	CVE-2024-5535	Fix not available
registry.gitlab.com/cequence/releases/cqai/data-science/cequence-airflow:7.7.0	High	CVE-2024-56201	Fix not available
registry.gitlab.com/cequence/releases/cqai/data-science/cequence-airflow:7.7.0	High	CVE-2024-56326	Fix not available
registry.gitlab.com/cequence/releases/cqai/data-science/cequence-airflow:7.7.0	High	CVE-2025-0395	New vulnerability
registry.gitlab.com/cequence/releases/cqai/data-science/cequence-airflow:7.7.0	High	CVE-2025-24793	New vulnerability
registry.gitlab.com/cequence/releases/cqai/data-science/cequence-airflow:7.7.0	High	CVE-2025-27516	New vulnerability
registry.gitlab.com/cequence/releases/cqai/data-science/cequence-airflow:7.7.0	High	CVE-2025-30473	New vulnerability
registry.gitlab.com/cequence/releases/cqai/data-science/cequence-airflow:7.7.0	High	CVE-2025-31115	New vulnerability
registry.gitlab.com/cequence/releases/cqai/policy-engine:7.7.0	Critical	CVE-2016-1000027	Fix in Next Release
registry.gitlab.com/cequence/releases/cqai/policy-engine:7.7.0	Critical	CVE-2025-24813	New vulnerability
registry.gitlab.com/cequence/releases/cqai/policy-engine:7.7.0	High	CVE-2024-38816	Fix not available
registry.gitlab.com/cequence/releases/cqai/policy-engine:7.7.0	High	CVE-2024-38819	Fix not available
registry.gitlab.com/cequence/releases/cqai/policy-engine:7.7.0	High	CVE-2025-22228	New vulnerability

registry.gitlab.com/cequence/releases/platform/bff:7.7.0	High	CVE-2025-22228	New vulnerability
registry.gitlab.com/cequence/releases/platform/defender-configuration:7.7.0	Critical	CVE-2025-24813	New vulnerability
registry.gitlab.com/cequence/releases/platform/defender-configuration:7.7.0	High	CVE-2024-12798	Fix in Next Release
registry.gitlab.com/cequence/releases/platform/defender-configuration:7.7.0	High	CVE-2024-38819	Fix not available
registry.gitlab.com/cequence/releases/platform/defender-configuration:7.7.0	High	CVE-2024-50379	Fix in Next Release
registry.gitlab.com/cequence/releases/platform/defender-configuration:7.7.0	High	CVE-2024-56337	Fix in Next Release
registry.gitlab.com/cequence/releases/platform/elasticsearch-init:7.7.0	High	CVE-2025-27152	New vulnerability
registry.gitlab.com/cequence/releases/platform/elasticsearch-init:7.7.0	High	CVE-2025-27789	New vulnerability
registry.gitlab.com/cequence/releases/platform/keycloak-init:7.7.0	High	CVE-2025-27152	New vulnerability
registry.gitlab.com/cequence/releases/platform/resource-discovery:7.7.0	Critical	CVE-2025-24813	New vulnerability
registry.gitlab.com/cequence/releases/platform/resource-discovery:7.7.0	High	CVE-2025-31672	Fix in Next Release
registry.gitlab.com/cequence/releases/platform/strimzi-kafka-connect:7.7.0	Critical	CVE-2024-24790	Fix not available
registry.gitlab.com/cequence/releases/platform/strimzi-kafka-connect:7.7.0	Critical	CVE-2024-47561	Fix in Next Release
registry.gitlab.com/cequence/releases/platform/strimzi-kafka-connect:7.7.0	Critical	CVE-2025-30065	New vulnerability
registry.gitlab.com/cequence/releases/platform/strimzi-kafka-connect:7.7.0	High	CVE-2023-29403	Fix not available
registry.gitlab.com/cequence/releases/platform/strimzi-kafka-connect:7.7.0	High	CVE-2023-2976	Fix in Next Release
registry.gitlab.com/cequence/releases/platform/strimzi-kafka-connect:7.7.0	High	CVE-2023-39325	Fix not available
registry.gitlab.com/cequence/releases/platform/strimzi-kafka-connect:7.7.0	High	CVE-2023-4043	Fix in Next Release
registry.gitlab.com/cequence/releases/platform/strimzi-kafka-connect:7.7.0	High	CVE-2023-43642	Fix in Next Release
registry.gitlab.com/cequence/releases/platform/strimzi-kafka-connect:7.7.0	High	CVE-2023-44487	Fix in Next Release
registry.gitlab.com/cequence/releases/platform/strimzi-kafka-connect:7.7.0	High	CVE-2023-45283	Fix not available
registry.gitlab.com/cequence/releases/platform/strimzi-kafka-connect:7.7.0	High	CVE-2023-45288	Fix not available
registry.gitlab.com/cequence/releases/platform/strimzi-kafka-connect:7.7.0	High	CVE-2023-45289	Fix not available
registry.gitlab.com/cequence/releases/platform/strimzi-kafka-connect:7.7.0	High	CVE-2023-45290	Fix not available
registry.gitlab.com/cequence/releases/platform/strimzi-kafka-connect:7.7.0	High	CVE-2023-51775	Fix in Next Release
registry.gitlab.com/cequence/releases/platform/strimzi-kafka-connect:7.7.0	High	CVE-2023-52428	Fix in Next Release
registry.gitlab.com/cequence/releases/platform/strimzi-kafka-connect:7.7.0	High	CVE-2023-7272	Fix in Next Release
registry.gitlab.com/cequence/releases/platform/strimzi-kafka-connect:7.7.0	High	CVE-2024-10963	Fix in Next Release
registry.gitlab.com/cequence/releases/platform/strimzi-kafka-connect:7.7.0	High	CVE-2024-21147	Fix in Next Release
registry.gitlab.com/cequence/releases/platform/strimzi-kafka-connect:7.7.0	High	CVE-2024-23444	Fix in Next Release
registry.gitlab.com/cequence/releases/platform/strimzi-kafka-connect:7.7.0	High	CVE-2024-24783	Fix not available
registry.gitlab.com/cequence/releases/platform/strimzi-kafka-connect:7.7.0	High	CVE-2024-24785	Fix not available
registry.gitlab.com/cequence/releases/platform/strimzi-kafka-connect:7.7.0	High	CVE-2024-24786	Fix in Next Release
registry.gitlab.com/cequence/releases/platform/strimzi-kafka-connect:7.7.0	High	CVE-2024-27309	Fix in Next Release
registry.gitlab.com/cequence/releases/platform/strimzi-kafka-connect:7.7.0	High	CVE-2024-29025	Fix in Next Release
registry.gitlab.com/cequence/releases/platform/strimzi-kafka-connect:7.7.0	High	CVE-2024-29857	Fix in Next Release
registry.gitlab.com/cequence/releases/platform/strimzi-kafka-connect:7.7.0	High	CVE-2024-30172	Fix in Next Release
registry.gitlab.com/cequence/releases/platform/strimzi-kafka-connect:7.7.0	High	CVE-2024-34155	Fix not available
registry.gitlab.com/cequence/releases/platform/strimzi-kafka-connect:7.7.0	High	CVE-2024-34156	Fix not available
registry.gitlab.com/cequence/releases/platform/strimzi-kafka-connect:7.7.0	High	CVE-2024-34158	Fix not available
registry.gitlab.com/cequence/releases/platform/strimzi-kafka-connect:7.7.0	High	CVE-2024-3596	Fix in Next Release
registry.gitlab.com/cequence/releases/platform/strimzi-kafka-connect:7.7.0	High	CVE-2024-45336	Fix not available
registry.gitlab.com/cequence/releases/platform/strimzi-kafka-connect:7.7.0	High	CVE-2024-45338	Fix in Next Release
registry.gitlab.com/cequence/releases/platform/strimzi-kafka-connect:7.7.0	High	CVE-2024-45341	Fix not available

[illegible]

registry.gitlab.com/cequence/releases/third-party/bitnami/postgresql:17.0.0-debian-12-r1	High	CVE-2025-0395	New vulnerability
registry.gitlab.com/cequence/releases/third-party/bitnami/postgresql:17.0.0-debian-12-r1	High	CVE-2025-31115	New vulnerability
registry.gitlab.com/cequence/releases/third-party/bitnami/redis:7.4.1-debian-12-r2	Critical	CVE-2024-56406	New vulnerability
registry.gitlab.com/cequence/releases/third-party/bitnami/redis:7.4.1-debian-12-r2	High	CVE-2024-45336	Fix not available
registry.gitlab.com/cequence/releases/third-party/bitnami/redis:7.4.1-debian-12-r2	High	CVE-2024-45341	Fix not available
registry.gitlab.com/cequence/releases/third-party/bitnami/redis:7.4.1-debian-12-r2	High	CVE-2025-0395	New vulnerability
registry.gitlab.com/cequence/releases/third-party/bitnami/redis:7.4.1-debian-12-r2	High	CVE-2025-31115	New vulnerability
registry.gitlab.com/cequence/releases/third-party/eck/eck-operator:2.11.0	Critical	CVE-2024-24790	Fix not available
registry.gitlab.com/cequence/releases/third-party/eck/eck-operator:2.11.0	High	CVE-2023-45288	Fix not available
registry.gitlab.com/cequence/releases/third-party/eck/eck-operator:2.11.0	High	CVE-2023-45289	Fix not available
registry.gitlab.com/cequence/releases/third-party/eck/eck-operator:2.11.0	High	CVE-2023-45290	Fix not available
registry.gitlab.com/cequence/releases/third-party/eck/eck-operator:2.11.0	High	CVE-2024-24783	Fix not available
registry.gitlab.com/cequence/releases/third-party/eck/eck-operator:2.11.0	High	CVE-2024-24785	Fix not available
registry.gitlab.com/cequence/releases/third-party/eck/eck-operator:2.11.0	High	CVE-2024-24786	Fix not available
registry.gitlab.com/cequence/releases/third-party/eck/eck-operator:2.11.0	High	CVE-2024-34155	Fix not available
registry.gitlab.com/cequence/releases/third-party/eck/eck-operator:2.11.0	High	CVE-2024-34156	Fix not available
registry.gitlab.com/cequence/releases/third-party/eck/eck-operator:2.11.0	High	CVE-2024-34158	Fix not available
registry.gitlab.com/cequence/releases/third-party/eck/eck-operator:2.11.0	High	CVE-2024-45336	Fix not available
registry.gitlab.com/cequence/releases/third-party/eck/eck-operator:2.11.0	High	CVE-2024-45337	Fix not available
registry.gitlab.com/cequence/releases/third-party/eck/eck-operator:2.11.0	High	CVE-2024-45338	Fix not available
registry.gitlab.com/cequence/releases/third-party/eck/eck-operator:2.11.0	High	CVE-2024-45341	Fix not available
registry.gitlab.com/cequence/releases/third-party/eck/eck-operator:2.11.0	High	CVE-2025-22868	New vulnerability
registry.gitlab.com/cequence/releases/third-party/eck/eck-operator:2.11.0	High	CVE-2025-22869	New vulnerability
registry.gitlab.com/cequence/releases/third-party/eck/eck-operator:2.11.0	High	CVE-2025-22870	New vulnerability
registry.gitlab.com/cequence/releases/third-party/elasticsearch/elasticsearch:7.17.21	Critical	CVE-2022-1471	Fix not available
registry.gitlab.com/cequence/releases/third-party/elasticsearch/elasticsearch:7.17.21	High	CVE-2021-40690	Fix not available
registry.gitlab.com/cequence/releases/third-party/elasticsearch/elasticsearch:7.17.21	High	CVE-2023-1370	Fix not available
registry.gitlab.com/cequence/releases/third-party/elasticsearch/elasticsearch:7.17.21	High	CVE-2023-2976	Fix not available
registry.gitlab.com/cequence/releases/third-party/elasticsearch/elasticsearch:7.17.21	High	CVE-2023-52428	Fix not available
registry.gitlab.com/cequence/releases/third-party/elasticsearch/elasticsearch:7.17.21	High	CVE-2024-23444	Fix not available
registry.gitlab.com/cequence/releases/third-party/elasticsearch/elasticsearch:7.17.21	High	CVE-2024-29025	Fix not available
registry.gitlab.com/cequence/releases/third-party/elasticsearch/elasticsearch:7.17.21	High	CVE-2024-29857	Fix not available
registry.gitlab.com/cequence/releases/third-party/elasticsearch/elasticsearch:7.17.21	High	CVE-2024-30172	Fix not available
registry.gitlab.com/cequence/releases/third-party/elasticsearch/elasticsearch:7.17.21	High	CVE-2025-24970	New vulnerability
registry.gitlab.com/cequence/releases/third-party/grafana/grafana:11.3.0	High	CVE-2024-12797	New vulnerability
registry.gitlab.com/cequence/releases/third-party/grafana/grafana:11.3.0	High	CVE-2024-45336	Fix not available
registry.gitlab.com/cequence/releases/third-party/grafana/grafana:11.3.0	High	CVE-2024-45337	Fix not available
registry.gitlab.com/cequence/releases/third-party/grafana/grafana:11.3.0	High	CVE-2024-45338	Fix not available
registry.gitlab.com/cequence/releases/third-party/grafana/grafana:11.3.0	High	CVE-2024-45341	Fix not available
registry.gitlab.com/cequence/releases/third-party/grafana/grafana:11.3.0	High	CVE-2024-56323	Fix not available
registry.gitlab.com/cequence/releases/third-party/grafana/grafana:11.3.0	High	CVE-2025-0725	New vulnerability
registry.gitlab.com/cequence/releases/third-party/grafana/grafana:11.3.0	High	CVE-2025-22868	New vulnerability
registry.gitlab.com/cequence/releases/third-party/grafana/grafana:11.3.0	High	CVE-2025-22869	New vulnerability
registry.gitlab.com/cequence/releases/third-party/grafana/grafana:11.3.0	High	CVE-2025-22870	New vulnerability

[illegible]

[illegible]

registry.gitlab.com/cequence/releases/third-party/strimzi/kafka:0.41.0-kafka-3.7.0	High	CVE-2024-45338	Fix not available
registry.gitlab.com/cequence/releases/third-party/strimzi/kafka:0.41.0-kafka-3.7.0	High	CVE-2024-45341	Fix not available
registry.gitlab.com/cequence/releases/third-party/strimzi/kafka:0.41.0-kafka-3.7.0	High	CVE-2024-47554	Fix not available
registry.gitlab.com/cequence/releases/third-party/strimzi/kafka:0.41.0-kafka-3.7.0	High	CVE-2024-56171	New vulnerability
registry.gitlab.com/cequence/releases/third-party/strimzi/kafka:0.41.0-kafka-3.7.0	High	CVE-2024-6345	Fix not available
registry.gitlab.com/cequence/releases/third-party/strimzi/kafka:0.41.0-kafka-3.7.0	High	CVE-2025-22870	New vulnerability
registry.gitlab.com/cequence/releases/third-party/strimzi/kafka:0.41.0-kafka-3.7.0	High	CVE-2025-24928	New vulnerability
registry.gitlab.com/cequence/releases/third-party/strimzi/kafka:0.41.0-kafka-3.7.0	High	CVE-2025-24970	New vulnerability
registry.gitlab.com/cequence/releases/third-party/strimzi/operator:0.41.0	High	CVE-2024-21147	Fix not available
registry.gitlab.com/cequence/releases/third-party/strimzi/operator:0.41.0	High	CVE-2024-3596	Fix not available
registry.gitlab.com/cequence/releases/third-party/strimzi/operator:0.41.0	High	CVE-2024-47554	Fix not available
registry.gitlab.com/cequence/releases/third-party/strimzi/operator:0.41.0	High	CVE-2024-56171	New vulnerability
registry.gitlab.com/cequence/releases/third-party/strimzi/operator:0.41.0	High	CVE-2024-6345	Fix not available
registry.gitlab.com/cequence/releases/third-party/strimzi/operator:0.41.0	High	CVE-2025-24928	New vulnerability
registry.gitlab.com/cequence/releases/third-party/strimzi/operator:0.41.0	High	CVE-2025-24970	New vulnerability

Notes for FixStatus column:

1. "New vulnerability" indicates that the vulnerability fix was made available in last 90 days.
2. "Fix in next release" indicates that there is a new version available and we are actively working on fixing it in upcoming release.
3. "Fix not available" indicates one of the following:
 - i. No fix exists for the vulnerability:

In this case, the vulnerability has been identified, but no patch or update has been created to address it yet. This could be because the vulnerability is newly discovered, or because it's particularly challenging to fix.
 - ii. Transitive dependency not actively used:

The vulnerable package is a transitive dependency (i.e., a dependency of a dependency) which is not used anywhere in the product.
 - iii. No updated version available:

This means that while a fix might exist for the transitive dependencies, there isn't an updated version of the package (direct dependency) available that incorporates vulnerability fixes.