ZETA-Guard Bewertung von potenziellen Schwachstellen

Betrachtet werden CVEs der Schwere CRITICAL und HIGH

Images

PDP / Keycloak

Image: ".../zeta/zeta-guard/keycloak-zeta:main"

Analysis

netty-transport-4.1.119.Final.jar	CVE-2025-58057 CVE-2025-55163 CVE-2025-58056	HIGH	Wird serverseitig nicht verwendet Nur im Infinispan-Client enthalten für SASL-Option die wir nicht nutzen
protobuf-java-3.25.1.jar	CVE-2024-7254	HIGH	Wird nicht verwendet
java-21-openjdk-headless	CVE-2025-64720 CVE-2025-65018 CVE-2025-66293	HIGH	Wird nicht verwendet Image-Processing wird nicht genutzt
om.googlecode.owasp-java-html-sanitizer:owasp-java-html-sanitizer	CVE-2025-66021	HIGH	Wird nicht verwendet Keine HTML Seiten nach aussen
com.microsoft.sqlserver:mssql-jdbc	CVE-2025-59250	HIGH	Wird nicht verwendet MSSQL wird verwendet

Keycloak-DB / Postgres

Wird nicht ausgeliefert, ist eine Voraussetzung

Image: Official Image “Postgres Operator 1.11”

Latest image: https://opensource.zalando.com/postgres-operator/

```
trivy --severity=CRITICAL,HIGH image ghcr.io/zalando/postgres-operator:v
```

http://golang.org/x/crypto	CVE-2024-45337	CRITICAL / HIGH	SSH Funktionalität von x/crypto wird nicht genutzt.

	CVE-2025-22869		
stdlib	CVE-2024-24790 CVE-2023-45288 CVE-2024-34156 CVE-2025-47907 CVE-2025-58183 CVE-2025-58186 CVE-2025-58187 CVE-2025-61729	CRITICAL / HIGH	• CVE-2024-24790: Neubewertung im eingesetzen Kontext ist MEDIUM: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/MAV:L/MAC:H/MPR:H • CVE-2023-45288: Neubewertung im eingesetzten Kontext ist MEDIUM: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/MAV:A • CVE-2024-34156: Neubewertung im eingesetzten Kontext ist MEDIUM: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/MAV:A • CVE-2025-47907: Neubewertung im eingesetzten Kontext ist MEDIUM: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L/MAV:A • CVE-2025-58183 Neubewertung im eingesetzten Kontext ist MEDIUM: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/MAV:A • CVE-2025-58186: Bewertung bei NVD ist MEDIUM und die Neubewertung im eingesetzten Kontext ist: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/MAV:A • CVE-2025-58187: Neubewertung im eingesetzten Kontext ist MEDIUM: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/MAV:A • CVE-2025-61729 Neubewertung im eingesetzten Kontext ist MEDIUM: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/MAV:A
http://golang.org/x/oauth2	CVE-2025-22868	HIGH	Neubewertung im eingesetzten Kontext ist MEDIUM: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:N/CR:L/IR:M/AR:L/MAV:A/MAC:H/MPR:H/MUI:N
http://github.com/dgrijalva/jwt-go	CVE-2020-26160	HIGH	Version wird hochgezogen Nicht mehr vorhanden in Version 1.14
http://github.com/golang-jwt/jwt	CVE-2025-30204	HIGH	Version wird hochgezogen Nicht mehr vorhanden in Version 1.14
http://github.com/jackc/pgproto3/v2	GHSA-7jwh-3vrq-q3m8	HIGH	Version wird hochgezogen Nicht mehr vorhanden in Version 1.14
http://github.com/jackc/pgx	CVE-2024-27289 CVE-2024-27304	HIGH	Version wird hochgezogen Nicht mehr vorhanden in Version 1.14

http://golang.org/x/net	CVE-2022-27664 CVE-2022-41723 CVE-2023-39325	HIGH	Version wird hochgezogen Nicht mehr vorhanden in Version 1.14
http://golang.org/x/text	CVE-2022-32149	HIGH	Version wird hochgezogen Nicht mehr vorhanden in Version 1.14
http://google.golang.org/grpc	GHSA-m425-mq94-257g	HIGH	Version wird hochgezogen Nicht mehr vorhanden in Version 1.14
http://gopkg.in/yaml.v3	CVE-2022-28948	HIGH	Version wird hochgezogen Nicht mehr vorhanden in Version 1.14

PEP / NGINX

Image: “.../zeta/zeta-guard/ngx_pep:main"

Analysis

libaom3	CVE-2023-6879 CVE-2023-39616	CRITICAL / HIGH	Wird nicht verwendet Videocodec wird nicht genutzt
zlib1g	CVE-2023-45853	CRITICAL	nginx verwendet zlib für den gzip filter - Das CVE bezieht sich auf ein Problem im nicht verwendeten minizip Verfahren.
libldap-2.5-0, libpam-modules, libpam-modules-bin, libpam-runtime, libpam0g	CVE-2023-2953 CVE-2025-6020	HIGH	Wird nicht verwendet Pam wird nicht genutzt
libpng16-16, libtiff6	CVE-2025-64720 CVE-2025-65018 CVE-2025-66293 CVE-2023-52355	HIGH	Wird nicht verwendet Image-Processing wird nicht genutzt
libxslt1.1	CVE-2025-7425	HIGH	Wird nicht verwendet Kein XSLT

Telemetrie

Image: "http://ghcr.io/open-telemetry/opentelemetry-collector-releases/opentelemetry-collector-k8s:0.105.0 "

Analysis

http://github.com/docker/docker	CVE-2024-41110	CRITICAL	Hier so nicht ausnutzbar (kein Docker Daemon verbunden).
http://golang.org/x/crypto	CVE-2024-45337 CVE-2025-22869	CRITICAL / HIGH	SSH Funktionalität von x/crypto wird nicht genutzt.

http://github.com/expr-lang/expr	CVE-2025-29786	HIGH	• CVE-2025-29786 Neubewertung im eingesetzten Kontext ist MEDIUM: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/MAV:A
http://github.com/golang-jwt/jwt/v5	CVE-2025-30204	HIGH	• CVE-2025-30204 Neubewertung im eingesetzten Kontext ist MEDIUM: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/MAV:A/MA:L
http://golang.org/x/oauth2	CVE-2025-22868	HIGH	Neubewertung im eingesetzten Kontext ist MEDIUM CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/MAV:A/MA:L
stdlib	CVE-2024-34156 CVE-2025-47907 CVE-2025-58183 CVE-2025-58186 CVE-2025-58187 CVE-2025-61729	HIGH	• CVE-2024-34156: Neubewertung im eingesetzten Kontext ist MEDIUM: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/MAV:A • CVE-2025-47907: Neubewertung im eingesetzten Kontext ist MEDIUM: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L/MAV:A • CVE-2025-58183 Neubewertung im eingesetzten Kontext ist MEDIUM: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/MAV:A • CVE-2025-58186: Bewertung bei NVD ist MEDIUM und die Neubewertung im eingesetzten Kontext ist: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/MAV:A • CVE-2025-58187: Neubewertung im eingesetzten Kontext ist MEDIUM: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/MAV:A • CVE-2025-61729 Neubewertung im eingesetzten Kontext ist MEDIUM: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/MAV:A

k8s.io/ingress-nginx

Wird nicht ausgeliefert, ist eine Voraussetzung

Image: “registry.k8s.io/ingress-nginx/kube-webhook-certgen:v1.4.4@sha256:a9f03b34a3cbfbb26d103a14046ab2c5130a80c3d69d526ff8063d2b37b9fd3f”

Analysis

http://k8s.io/ingress-nginx	CVE-2025-1974 CVE-2021-25742 CVE-2023-5043 CVE-2023-5044 CVE-2025-1097 CVE-2025-1098	CRITICAL / HIGH	Wir setzen Version 1.11.5 ein (wichtig für die folgende Beurteilung) • CVE-2025-1974 False positive in eingesetzer Version gefixt • CVE-2021-25742: False positive in eingesetzer Version gefixt

	CVE-2025-24514		• CVE-2023-5043: False positive in eingesetzer Version gefixt • CVE-2023-5044: False positive in eingesetzer Version gefixt • CVE-2025-1097 False positive in eingesetzer Version gefixt • CVE-2025-1098 False positive in eingesetzer Version gefixt • CVE-2025-24514 False positive in eingesetzer Version gefixt

zeta-testenv-staging-ingress-nginx-controller

Wird nicht ausgeliefert, ist eine Voraussetzung

Image: “registry.k8s.io/ingress-nginx/controller:v1.11.3@sha256:d56f135b6462cfc476447cfe564b83a45e8bb7da2774963b00d12161112270b7”

Latest image: https://github.com/kubernetes/ingress-nginx/releases

```
trivy --severity=CRITICAL,HIGH image registry.k8s.io/ingress-nginx/contr
```

Analysis

libxml2	CVE-2024-56171 CVE-2025-24928 CVE-2025-27113 CVE-2025-32414 CVE-2025-32415	CRITICAL / HIGH	Wird nicht verwendet, keine XML Verarbeitung.

stdlib	CVE-2025-47907 CVE-2025-58183 CVE-2025-58186 CVE-2025-58187 CVE-2025-61729	HIGH	• CVE-2025-47907: Neubewertung im eingesetzten Kontext ist MEDIUM: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L/MAV:A • CVE-2025-58183 Neubewertung im eingesetzten Kontext ist MEDIUM: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/MAV:A • CVE-2025-58186: Bewertung bei NVD ist MEDIUM und die Neubewertung im eingesetzten Kontext ist: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/MAV:A • CVE-2025-58187: Neubewertung im eingesetzten Kontext ist MEDIUM: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/MAV:A • CVE-2025-61729 Neubewertung im eingesetzten Kontext ist MEDIUM: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/MAV:A
http://golang.org/x/oauth2	CVE-2025-22868	HIGH	Version wird hochgezogen Nicht mehr vorhanden in Version 1.13
http://github.com/opencontainers/runc	CVE-2025-31133 CVE-2025-52565 CVE-2025-52881	HIGH	Version wird hochgezogen Nicht mehr vorhanden in Version 1.13
icu-data-en	CVE-2025-5222	HIGH	Version wird hochgezogen Nicht mehr vorhanden in Version 1.13
icu-libs	CVE-2025-5222	HIGH	Version wird hochgezogen Nicht mehr vorhanden in Version 1.13
libcrypto3	CVE-2024-12797	HIGH	Version wird hochgezogen Nicht mehr vorhanden in Version 1.13
libssl3	CVE-2024-12797	HIGH	Version wird hochgezogen Nicht mehr vorhanden in Version 1.13
openssl	CVE-2024-12797	HIGH	Version wird hochgezogen Nicht mehr vorhanden in Version 1.13
xz-libs	CVE-2025-31115	HIGH	Version wird hochgezogen Nicht mehr vorhanden in Version 1.13

Notes

Check cluster

```
trivy k8s --severity=CRITICAL,HIGH --report=all --include-namespaces zeta-staging
```

CI Jobs

PEP: https://.../zeta/zeta-guard/ngx_pep/-/jobs/21475

PDP: https://.../zeta/zeta-guard/keycloak-zeta/-/jobs/21654