

# FAQS download: How to improve security with Docker Bench

## 1

## How does Docker Bench for Security work?

```

# -----
# Docker Bench for Security v1.3.5
#
# Docker, Inc. (c) 2015-2021
#
# Checks for dozens of common best-practices around deploying Docker containers in production.
# Inspired by the CIS Docker Benchmark v1.2.0.
# -----

Initializing 2021-03-10T12:03:38+02:00

Section A - Checks result

[INFO] 1 - Host Configuration
[INFO] 1.1 - General Configuration
[NOTE] 1.1.1 - Ensure the container host has been Hardened (Not Scored)
[INFO] 1.1.2 - Ensure that the version of Docker is up to date (Not Scored)
[INFO] * Using 19.03.8, verify it is up to date as deemed necessary
[INFO] * Your operating system vendor may provide support and security maintenance for Docker
[INFO] 1.2 - Linux Hosts Specific Configuration
[WARN] 1.2.1 - Ensure a separate partition for containers has been created (Scored)
[INFO] 1.2.2 - Ensure only trusted users are allowed to control Docker daemon (Scored)
[INFO] * docker:x:998:mhail
[WARN] 1.2.3 - Ensure auditing is configured for the Docker daemon (Scored)
[WARN] 1.2.4 - Ensure auditing is configured for Docker files and directories - /var/lib/docker (Scored)
[WARN] 1.2.5 - Ensure auditing is configured for Docker files and directories - /etc/docker (Scored)
[WARN] 1.2.6 - Ensure auditing is configured for Docker files and directories - docker.service (Scored)
[WARN] 1.2.7 - Ensure auditing is configured for Docker files and directories - docker.socket (Scored)
[INFO] 1.2.8 - Ensure auditing is configured for Docker files and directories - /etc/default/docker (Scored)
[INFO] * File not found
[INFO] 1.2.9 - Ensure auditing is configured for Docker files and directories - /etc/sysconfig/docker (Scored)
[INFO] * File not found
[INFO] 1.2.10 - Ensure auditing is configured for Docker files and directories - /etc/docker/daemon.json (Scored)
[INFO] * File not found
[WARN] 1.2.11 - Ensure auditing is configured for Docker files and directories - /usr/bin/containerd (Scored)
[WARN] 1.2.12 - Ensure auditing is configured for Docker files and directories - /usr/sbin/runc (Scored)

[INFO] 2 - Docker daemon configuration
[WARN] 2.1 - Ensure network traffic is restricted between containers on the default bridge (Scored)
[PASS] 2.2 - Ensure the logging level is set to 'info' (Scored)
[PASS] 2.3 - Ensure Docker is allowed to make changes to iptables (Scored)
[PASS] 2.4 - Ensure insecure registries are not used (Scored)
[PASS] 2.5 - Ensure aufs storage driver is not used (Scored)

```

## 2

## How do I run Docker bench for a particular docker image?

Output:

```

macpro$ ./docker-bench-security.sh -i hello-world
# -----
# Docker Bench for Security v1.3.6
#
# Docker, Inc. (c) 2015-2022
#
# Checks for dozens of common best-practices around deploying Docker containers in production.
# Based on the CIS Docker Benchmark 1.3.1.
# -----[WARN] Some tests might require root to run
Initializing
2022-01-17T15:08:21:z
Section A - Check results[INFO] 1 - Host Configuration
[INFO] 1.1 - Linux Hosts Specific Configuration
[WARN] 1.1.1 - Ensure a separate partition for containers has been created (Automated)
[INFO] 1.1.2 - Ensure only trusted users are allowed to control Docker daemon (Automated)
[INFO] * Users:
[WARN] 1.1.3 - Ensure auditing is configured for the Docker daemon (Automated)
[WARN] 1.1.4 - Ensure auditing is configured for Docker files and directories - /run/containerd (Automated)
[INFO] 1.1.5 - Ensure auditing is configured for Docker files and directories - /var/lib/docker (Automated)
[INFO] * Directory not found
[INFO] 1.1.6 - Ensure auditing is configured for Docker files and directories - /etc/docker (Automated)
[INFO] * Directory not found
[INFO] 1.1.7 - Ensure auditing is configured for Docker files and directories - docker.service (Automated)
[INFO] * File not found
[INFO] 1.1.8 - Ensure auditing is configured for Docker files and directories - containerd.sock (Automated)

```

```

[INFO] * File not found
[INFO] 1.1.9 - Ensure auditing is configured for Docker files and directories - docker.socket (Automated)
[INFO] * File not found
[INFO] 1.1.10 - Ensure auditing is configured for Docker files and directories - /etc/default/docker (Automated)
[INFO] * File not found
[INFO] 1.1.11 - Ensure auditing is configured for Dockerfiles and directories - /etc/docker/daemon.json (Automated)
[INFO] * File not found
[INFO] 1.1.12 - 1.1.12 Ensure auditing is configured for Dockerfiles and directories - /etc/containerd/config.toml (Automated)
[INFO] * File not found
[INFO] 1.1.13 - Ensure auditing is configured for Docker files and directories - /etc/sysconfig/docker (Automated)
[INFO] * File not found
[INFO] 1.1.14 - Ensure auditing is configured for Docker files and directories - /usr/bin/containerd (Automated)
[INFO] * File not found
[INFO] 1.1.15 - Ensure auditing is configured for Docker files and directories - /usr/bin/containerd-shim (Automated)
[INFO] * File not found
[INFO] 1.1.16 - Ensure auditing is configured for Docker files and directories - /usr/bin/containerd-shim-runc-v1 (Automated)
[INFO] * File not found
[INFO] 1.1.17 - Ensure auditing is configured for Docker files and directories - /usr/bin/containerd-shim-runc-v2 (Automated)
[INFO] * File not found
[INFO] 1.1.18 - Ensure auditing is configured for Docker files and directories - /usr/bin/runc (Automated)
[INFO] * File not found
[INFO] 1.2 - General Configuration
[NOTE] 1.2.1 - Ensure the container host has been Hardened (Manual)
date: illegal time format
usage: date [-jnRu] [-d dst] [-r seconds] [-t west] [-v[+|-]val[ymwdHMS]] ...
      [-f fmt date | [[[mm]dd]HH]MM[[cc]yy][.ss]] [+format]
./functions/helper_lib.sh: line 36: [: : integer expression expected
./functions/helper_lib.sh: line 37: [: : integer expression expected
[PASS] 1.2.2 - Ensure that the version of Docker is up to date (Manual)
[INFO] * Using 20.10.12 which is current
[INFO] * Check with your operating system vendor for support and security maintenance for Docker[INFO] 2 - Docker daemon configuration
[NOTE] 2.1 - Run the Docker daemon as a non-root user, if possible (Manual)
[WARN] 2.2 - Ensure network traffic is restricted between containers on the default bridge (Scored)
[PASS] 2.3 - Ensure the logging level is set to 'info' (Scored)
[PASS] 2.4 - Ensure Docker is allowed to make changes to iptables (Scored)
[PASS] 2.5 - Ensure insecure registries are not used (Scored)
[PASS] 2.6 - Ensure aufs storage driver is not used (Scored)
[INFO] 2.7 - Ensure TLS authentication for Docker daemon is configured (Scored)
[INFO] * Docker daemon not listening on TCP
[INFO] 2.8 - Ensure the default ulimit is configured appropriately (Manual)
[INFO] * Default ulimit doesn't appear to be set
[WARN] 2.9 - Enable user namespace support (Scored)
[PASS] 2.10 - Ensure the default cgroup usage has been confirmed (Scored)
[PASS] 2.11 - Ensure base device size is not changed until needed (Scored)
[WARN] 2.12 - Ensure that authorization for Docker client commands is enabled (Scored)
[WARN] 2.13 - Ensure centralized and remote logging is configured (Scored)
[WARN] 2.14 - Ensure containers are restricted from acquiring new privileges (Scored)
[WARN] 2.15 - Ensure live restore is enabled (Scored)
[WARN] 2.16 - Ensure Userland Proxy is Disabled (Scored)
[PASS] 2.17 - Ensure that a daemon-wide custom seccomp profile is applied if appropriate (Manual)
[INFO] Ensure that experimental features are not implemented in production (Scored) (Deprecated)[INFO] 3 - Docker daemon configuration files
[INFO] 3.1 - Ensure that the docker.service file ownership is set to root:root (Automated)
[INFO] * File not found
[INFO] 3.2 - Ensure that docker.service file permissions are appropriately set (Automated)
[INFO] * File not found
[INFO] 3.3 - Ensure that docker.socket file ownership is set to root:root (Automated)
[INFO] * File not found
[INFO] 3.4 - Ensure that docker.socket file permissions are set to 644 or more restrictive (Automated)
[INFO] * File not found
[INFO] 3.5 - Ensure that the /etc/docker directory ownership is set to root:root (Automated)
[INFO] * Directory not found
[INFO] 3.6 - Ensure that /etc/docker directory permissions are set to 755 or more restrictively (Automated)
[INFO] * Directory not found
[INFO] 3.7 - Ensure that registry certificate file ownership is set to root:root (Automated)
[INFO] * Directory not found
[INFO] 3.8 - Ensure that registry certificate file permissions are set to 444 or more restrictively (Automated)
[INFO] * Directory not found
[INFO] 3.9 - Ensure that TLS CA certificate file ownership is set to root:root (Automated)
[INFO] * No TLS CA certificate found

```



```

[INFO] 3.10 - Ensure that TLS CA certificate file permissions are set to 444 or more restrictively (Automated)
[INFO] * No TLS CA certificate found
[INFO] 3.11 - Ensure that Docker server certificate file ownership is set to root:root (Automated)
[INFO] * No TLS Server certificate found
[INFO] 3.12 - Ensure that the Docker server certificate file permissions are set to 444 or more restrictively (Automated)
[INFO] * No TLS Server certificate found
[INFO] 3.13 - Ensure that the Docker server certificate key file ownership is set to root:root (Automated)
[INFO] * No TLS Key found
[INFO] 3.14 - Ensure that the Docker server certificate key file permissions are set to 400 (Automated)
[INFO] * No TLS Key found
stat: illegal option -- c
usage: stat [-FLnqrsx] [-f format] [-t timefmt] [file ...]
[WARN] 3.15 - Ensure that the Docker socket file ownership is set to root:docker (Automated)
[WARN] * Wrong ownership for /var/run/docker.sock
stat: illegal option -- c
usage: stat [-FLnqrsx] [-f format] [-t timefmt] [file ...]
./tests/3_docker_daemon_configuration_files.sh: line 429: [: : integer expression expected
[WARN] 3.16 - Ensure that the Docker socket file permissions are set to 660 or more restrictively (Automated)
[WARN] * Wrong permissions for /var/run/docker.sock
[INFO] 3.17 - Ensure that the daemon.json file ownership is set to root:root (Automated)
[INFO] * File not found
[INFO] 3.18 - Ensure that daemon.json file permissions are set to 644 or more restrictive (Automated)
[INFO] * File not found
[INFO] 3.19 - Ensure that the /etc/default/docker file ownership is set to root:root (Automated)
[INFO] * File not found
[INFO] 3.20 - Ensure that the /etc/sysconfig/docker file permissions are set to 644 or more restrictively (Automated)
[INFO] * File not found
[INFO] 3.21 - Ensure that the /etc/sysconfig/docker file ownership is set to root:root (Automated)
[INFO] * File not found
[INFO] 3.22 - Ensure that the /etc/default/docker file permissions are set to 644 or more restrictively (Automated)
[INFO] * File not found
[INFO] 3.23 - Ensure that the Containerd socket file ownership is set to root:root (Automated)
[INFO] * File not found
[INFO] 3.24 - Ensure that the Containerd socket file permissions are set to 660 or more restrictively (Automated)
[INFO] * File not found[INFO] 4 - Container Images and Build File
[INFO] 4.1 - Ensure that a user for the container has been created (Automated)
[INFO] * No containers running
[NOTE] 4.2 - Ensure that containers use only trusted base images (Manual)
[NOTE] 4.3 - Ensure that unnecessary packages are not installed in the container (Manual)
[NOTE] 4.4 - Ensure images are scanned and rebuilt to include security patches (Manual)
[WARN] 4.5 - Ensure Content trust for Docker is Enabled (Automated)
[WARN] 4.6 - Ensure that HEALTHCHECK instructions have been added to container images (Automated)
[WARN] * No Healthcheck found: [hello-world:latest]
[PASS] 4.7 - Ensure update instructions are not used alone in the Dockerfile (Manual)
[NOTE] 4.8 - Ensure setuid and setgid permissions are removed (Manual)
[PASS] 4.9 - Ensure that COPY is used instead of ADD in Dockerfiles (Manual)
[NOTE] 4.10 - Ensure secrets are not stored in Dockerfiles (Manual)
[NOTE] 4.11 - Ensure only verified packages are installed (Manual)[INFO] 5 - Container Runtime
[INFO] * No containers running, skipping Section 5[INFO] 6 - Docker Security Operations
[INFO] 6.1 - Ensure that image sprawl is avoided (Manual)
[INFO] * There are currently: 19 images
[INFO] * Only 0 out of 19 are in use
[INFO] 6.2 - Ensure that container sprawl is avoided (Manual)
[INFO] * There are currently a total of 35 containers, with 18 of them currently running[INFO] 7 - Docker Swarm Configuration
[PASS] 7.1 - Ensure swarm mode is not Enabled, if not needed (Automated)
[PASS] 7.2 - Ensure that the minimum number of manager nodes have been created in a swarm (Automated) (Swarm mode not enabled)
[PASS] 7.3 - Ensure that swarm services are bound to a specific host interface (Automated) (Swarm mode not enabled)
[PASS] 7.4 - Ensure that all Docker swarm overlay networks are encrypted (Automated)
[PASS] 7.5 - Ensure that Docker's secret management commands are used for managing secrets in a swarm cluster (Manual) (Swarm mode not enabled)
[PASS] 7.6 - Ensure that swarm manager is run in auto-lock mode (Automated) (Swarm mode not enabled)
[PASS] 7.7 - Ensure that the swarm manager auto-lock key is rotated periodically (Manual) (Swarm mode not enabled)
[PASS] 7.8 - Ensure that node certificates are rotated as appropriate (Manual) (Swarm mode not enabled)
[PASS] 7.9 - Ensure that CA certificates are rotated as appropriate (Manual) (Swarm mode not enabled)
[PASS] 7.10 - Ensure that management plane traffic is separated from data plane traffic (Manual) (Swarm mode not enabled)
Section C - Score[INFO] Checks: 85
[INFO] Score: -3

```

### 3 How do I enable auditing for Docker Files?

□ Add the following lines to the bottom of the file:

```
-w /etc/default/docker -p wa
-w /etc/docker -p wa
-w /etc/docker/daemon.json -p wa
-w /lib/systemd/system/docker.service -p wa
-w /lib/systemd/system/docker.socket -p wa
-w /usr/bin/docker -p wa
-w /usr/bin/docker-containerd -p wa
-w /usr/bin/docker-runc -p wa
-w /var/lib/docker -p wa
```

### 4 How do I perform vulnerability scanning for Docker local images?

□ Example output from a vulnerability scan:

```
macro$ docker scan --accept-license --version
Version: v0.16.0
Git commit: e135637
Provider: Snyk (1.809.0)macro$ docker scan postgres:12
\ Analyzing container dependencies for postgres:12Testing postgres:12...X Low severity vulnerability found in tar
Description: CVE-2005-2541
Info: https://snyk.io/vuln/SNYK-DEBIAN11-TAR-523480
Introduced through: meta-common-packages@meta
From: meta-common-packages@meta > tar@1.34+dfsg-1X Low severity vulnerability found in systemd/libsystemd0
Description: Authentication Bypass
Info: https://snyk.io/vuln/SNYK-DEBIAN11-SYSTEMD-1291054
Introduced through: postgresql-12@12.9-1.pgdg110+1, util-linux/bsdutils@1:2.36.1-8, util-linux/mount@2.36.1-8
From: postgresql-12@12.9-1.pgdg110+1 > systemd/libsystemd0@247.3-6
From: util-linux/bsdutils@1:2.36.1-8 > systemd/libsystemd0@247.3-6
From: util-linux/mount@2.36.1-8 > util-linux@2.36.1-8 > systemd/libsystemd0@247.3-6
and 4 more...X Low severity vulnerability found in systemd/libsystemd0
Description: CVE-2021-3997
Info: https://snyk.io/vuln/SNYK-DEBIAN11-SYSTEMD-2332025
Introduced through: postgresql-12@12.9-1.pgdg110+1, util-linux/bsdutils@1:2.36.1-8, util-linux/mount@2.36.1-8
From: postgresql-12@12.9-1.pgdg110+1 > systemd/libsystemd0@247.3-6
From: util-linux/bsdutils@1:2.36.1-8 > systemd/libsystemd0@247.3-6
From: util-linux/mount@2.36.1-8 > util-linux@2.36.1-8 > systemd/libsystemd0@247.3-6
and 4 more...X Low severity vulnerability found in systemd/libsystemd0
Description: Link Following
Info: https://snyk.io/vuln/SNYK-DEBIAN11-SYSTEMD-524969
Introduced through: postgresql-12@12.9-1.pgdg110+1, util-linux/bsdutils@1:2.36.1-8, util-linux/mount@2.36.1-8
From: postgresql-12@12.9-1.pgdg110+1 > systemd/libsystemd0@247.3-6
From: util-linux/bsdutils@1:2.36.1-8 > systemd/libsystemd0@247.3-6
From: util-linux/mount@2.36.1-8 > util-linux@2.36.1-8 > systemd/libsystemd0@247.3-6
and 4 more.X Low severity vulnerability found in sqlite3/libsqlite3-0
Description: Out-of-bounds Read
Info: https://snyk.io/vuln/SNYK-DEBIAN11-SQLITE3-1569419
Introduced through: gnupg2/gnupg@2.2.27-2
From: gnupg2/gnupg@2.2.27-2 > gnupg2/gpg@2.2.27-2 > sqlite3/libsqlite3-0@3.34.1-3X Low severity vulnerability found in shadow/passwd
Description: Access Restriction Bypass
Info: https://snyk.io/vuln/SNYK-DEBIAN11-SHADOW-526940
Introduced through: gnupg2/dirmngr@2.2.27-2, shadow/login@1:4.8.1-1, util-linux/mount@2.36.1-8
From: gnupg2/dirmngr@2.2.27-2 > adduser@3.118 > shadow/passwd@1:4.8.1-1
From: shadow/login@1:4.8.1-1
```

From: util-linux/mount@2.36.1-8 > util-linux@2.36.1-8 > shadow/login@1:4.8.1-1X Low severity vulnerability found in shadow/passwd  
Description: Time-of-check Time-of-use (TOCTOU)  
Info: <https://snyk.io/vuln/SNYK-DEBIAN11-SHADOW-528840>  
Introduced through: gnupg2/dirmngr@2.2.27-2, shadow/login@1:4.8.1-1, util-linux/mount@2.36.1-8  
From: gnupg2/dirmngr@2.2.27-2 > adduser@3.118 > shadow/passwd@1:4.8.1-1  
From: shadow/login@1:4.8.1-1  
From: util-linux/mount@2.36.1-8 > util-linux@2.36.1-8 > shadow/login@1:4.8.1-1X Low severity vulnerability found in shadow/passwd  
Description: Incorrect Permission Assignment for Critical Resource  
Info: <https://snyk.io/vuln/SNYK-DEBIAN11-SHADOW-539870>  
Introduced through: gnupg2/dirmngr@2.2.27-2, shadow/login@1:4.8.1-1, util-linux/mount@2.36.1-8  
From: gnupg2/dirmngr@2.2.27-2 > adduser@3.118 > shadow/passwd@1:4.8.1-1  
From: shadow/login@1:4.8.1-1  
From: util-linux/mount@2.36.1-8 > util-linux@2.36.1-8 > shadow/login@1:4.8.1-1X Low severity vulnerability found in perl/perl-base  
Description: Link Following  
Info: <https://snyk.io/vuln/SNYK-DEBIAN11-PERL-532614>  
Introduced through: meta-common-packages@meta, perl/libperl5.32@5.32.1-4+deb11u2, perl@5.32.1-4+deb11u2, perl/perl-modules-5.32@5.32.1-4+deb11u2  
From: meta-common-packages@meta > perl/perl-base@5.32.1-4+deb11u2  
From: perl/libperl5.32@5.32.1-4+deb11u2  
From: perl@5.32.1-4+deb11u2 > perl/libperl5.32@5.32.1-4+deb11u2  
and 4 more.X Low severity vulnerability found in pcre3/libpcre3  
Description: Out-of-Bounds  
Info: <https://snyk.io/vuln/SNYK-DEBIAN11-PCRE3-523392>  
Introduced through: pcre3/libpcre3@2:8.39-13, grep@3.6-1  
From: pcre3/libpcre3@2:8.39-13  
From: grep@3.6-1 > pcre3/libpcre3@2:8.39-13X Low severity vulnerability found in pcre3/libpcre3  
Description: Out-of-Bounds  
Info: <https://snyk.io/vuln/SNYK-DEBIAN11-PCRE3-525075>  
Introduced through: pcre3/libpcre3@2:8.39-13, grep@3.6-1  
From: pcre3/libpcre3@2:8.39-13  
From: grep@3.6-1 > pcre3/libpcre3@2:8.39-13X Low severity vulnerability found in pcre3/libpcre3  
Description: Uncontrolled Recursion  
Info: <https://snyk.io/vuln/SNYK-DEBIAN11-PCRE3-529298>  
Introduced through: pcre3/libpcre3@2:8.39-13, grep@3.6-1  
From: pcre3/libpcre3@2:8.39-13  
From: grep@3.6-1 > pcre3/libpcre3@2:8.39-13X Low severity vulnerability found in pcre3/libpcre3  
Description: Out-of-Bounds  
Info: <https://snyk.io/vuln/SNYK-DEBIAN11-PCRE3-529490>  
Introduced through: pcre3/libpcre3@2:8.39-13, grep@3.6-1  
From: pcre3/libpcre3@2:8.39-13  
From: grep@3.6-1 > pcre3/libpcre3@2:8.39-13X Low severity vulnerability found in pcre3/libpcre3  
Description: Out-of-bounds Read  
Info: <https://snyk.io/vuln/SNYK-DEBIAN11-PCRE3-572353>  
Introduced through: pcre3/libpcre3@2:8.39-13, grep@3.6-1  
From: pcre3/libpcre3@2:8.39-13  
From: grep@3.6-1 > pcre3/libpcre3@2:8.39-13X Low severity vulnerability found in openssl/libssl1.1  
Description: Cryptographic Issues  
Info: <https://snyk.io/vuln/SNYK-DEBIAN11-OPENSSL-518334>  
Introduced through: postgresql-12@12.9-1.pgdg110+1, gnupg2/dirmngr@2.2.27-2  
From: postgresql-12@12.9-1.pgdg110+1 > openssl/libssl1.1@1.1.1k-1+deb11u1  
From: postgresql-12@12.9-1.pgdg110+1 > postgresql-12/postgresql-client-12@12.9-1.pgdg110+1 > postgresql-14/libpq5@14.1-1.pgdg110+1 > openssl/libssl1.1@1.1.1k-1+deb11u1  
From: postgresql-12@12.9-1.pgdg110+1 > postgresql-common@232.pgdg110+1 > ssl-cert@1.1.0+nmu1 > openssl@1.1.1k-1+deb11u1 > openssl/libssl1.1@1.1.1k-1+deb11u1  
and 2 more.X Low severity vulnerability found in openssl/libssl1.1  
Description: Cryptographic Issues  
Info: <https://snyk.io/vuln/SNYK-DEBIAN11-OPENSSL-525332>  
Introduced through: postgresql-12@12.9-1.pgdg110+1, gnupg2/dirmngr@2.2.27-2  
From: postgresql-12@12.9-1.pgdg110+1 > openssl/libssl1.1@1.1.1k-1+deb11u1  
From: postgresql-12@12.9-1.pgdg110+1 > postgresql-12/postgresql-client-12@12.9-1.pgdg110+1 > postgresql-14/libpq5@14.1-1.pgdg110+1 > openssl/libssl1.1@1.1.1k-1+deb11u1  
From: postgresql-12@12.9-1.pgdg110+1 > postgresql-common@232.pgdg110+1 > ssl-cert@1.1.0+nmu1 > openssl@1.1.1k-1+deb11u1 > openssl/libssl1.1@1.1.1k-1+deb11u1

and 2 more. X Low severity vulnerability found in openldap/libldap-2.4-2  
Description: Improper Initialization  
Info: <https://snyk.io/vuln/SNYK-DEBIAN11-OPENLDAP-521320>  
Introduced through: gnupg2/dirmngr@2.2.27-2, postgresql-12@12.9-1.pgdg110+1  
From: gnupg2/dirmngr@2.2.27-2 > openldap/libldap-2.4-2@2.4.57+dfsg-3  
From: postgresql-12@12.9-1.pgdg110+1 > openldap/libldap-2.4-2@2.4.57+dfsg-3  
From: postgresql-12@12.9-1.pgdg110+1 > postgresql-12/postgresql-client-12@12.9-1.pgdg110+1 > postgresql-14/libpq5@14.1-1.pgdg110+1 > openldap/libldap-2.4-2@2.4.57+dfsg-3 X Low severity vulnerability found in openldap/libldap-2.4-2  
Description: Out-of-Bounds  
Info: <https://snyk.io/vuln/SNYK-DEBIAN11-OPENLDAP-531344>  
Introduced through: gnupg2/dirmngr@2.2.27-2, postgresql-12@12.9-1.pgdg110+1  
From: gnupg2/dirmngr@2.2.27-2 > openldap/libldap-2.4-2@2.4.57+dfsg-3  
From: postgresql-12@12.9-1.pgdg110+1 > openldap/libldap-2.4-2@2.4.57+dfsg-3  
From: postgresql-12@12.9-1.pgdg110+1 > postgresql-12/postgresql-client-12@12.9-1.pgdg110+1 > postgresql-14/libpq5@14.1-1.pgdg110+1 > openldap/libldap-2.4-2@2.4.57+dfsg-3 X Low severity vulnerability found in openldap/libldap-2.4-2  
Description: Cryptographic Issues  
Info: <https://snyk.io/vuln/SNYK-DEBIAN11-OPENLDAP-531747>  
Introduced through: gnupg2/dirmngr@2.2.27-2, postgresql-12@12.9-1.pgdg110+1  
From: gnupg2/dirmngr@2.2.27-2 > openldap/libldap-2.4-2@2.4.57+dfsg-3  
From: postgresql-12@12.9-1.pgdg110+1 > openldap/libldap-2.4-2@2.4.57+dfsg-3  
From: postgresql-12@12.9-1.pgdg110+1 > postgresql-12/postgresql-client-12@12.9-1.pgdg110+1 > postgresql-14/libpq5@14.1-1.pgdg110+1 > openldap/libldap-2.4-2@2.4.57+dfsg-3 X Low severity vulnerability found in openldap/libldap-2.4-2  
Description: Improper Certificate Validation  
Info: <https://snyk.io/vuln/SNYK-DEBIAN11-OPENLDAP-584937>  
Introduced through: gnupg2/dirmngr@2.2.27-2, postgresql-12@12.9-1.pgdg110+1  
From: gnupg2/dirmngr@2.2.27-2 > openldap/libldap-2.4-2@2.4.57+dfsg-3  
From: postgresql-12@12.9-1.pgdg110+1 > openldap/libldap-2.4-2@2.4.57+dfsg-3  
From: postgresql-12@12.9-1.pgdg110+1 > postgresql-12/postgresql-client-12@12.9-1.pgdg110+1 > postgresql-14/libpq5@14.1-1.pgdg110+1 > openldap/libldap-2.4-2@2.4.57+dfsg-3 X Low severity vulnerability found in ncurses/libtinfo6  
Description: Out-of-bounds Write  
Info: <https://snyk.io/vuln/SNYK-DEBIAN11-NCURSES-1655741>  
Introduced through: bash/bash@5.1-2+b3, ncurses/ncurses-bin@6.2+20201114-2, postgresql-12@12.9-1.pgdg110+1, util-linux/mount@2.36.1-8, gnupg2/dirmngr@2.2.27-2, gnupg2/gnupg@2.2.27-2, ncurses/ncurses-base@6.2+20201114-2  
From: bash/bash@5.1-2+b3 > ncurses/libtinfo6@6.2+20201114-2  
From: ncurses/ncurses-bin@6.2+20201114-2 > ncurses/libtinfo6@6.2+20201114-2  
From: postgresql-12@12.9-1.pgdg110+1 > llvm-toolchain-11/libllvm11@1:11.0.1-2 > ncurses/libtinfo6@6.2+20201114-2  
and 8 more. X Low severity vulnerability found in libxslt/libxslt1.1  
Description: Use of Insufficiently Random Values  
Info: <https://snyk.io/vuln/SNYK-DEBIAN11-LIBXSLT-514942>  
Introduced through: postgresql-12@12.9-1.pgdg110+1  
From: postgresql-12@12.9-1.pgdg110+1 > libxslt/libxslt1.1@1.1.34-4 X Low severity vulnerability found in libsepol/libsepol1  
Description: Use After Free  
Info: <https://snyk.io/vuln/SNYK-DEBIAN11-LIBSEPOL-1315627>  
Introduced through: gnupg2/dirmngr@2.2.27-2  
From: gnupg2/dirmngr@2.2.27-2 > adduser@3.118 > shadow/passwd@1:4.8.1-1 > libsemanage/libsemanage1@3.1-1+b2 > libsepol/libsepol1@3.1-1 X Low severity vulnerability found in libsepol/libsepol1  
Description: Out-of-bounds Read  
Info: <https://snyk.io/vuln/SNYK-DEBIAN11-LIBSEPOL-1315629>  
Introduced through: gnupg2/dirmngr@2.2.27-2  
From: gnupg2/dirmngr@2.2.27-2 > adduser@3.118 > shadow/passwd@1:4.8.1-1 > libsemanage/libsemanage1@3.1-1+b2 > libsepol/libsepol1@3.1-1 X Low severity vulnerability found in libsepol/libsepol1  
Description: Use After Free  
Info: <https://snyk.io/vuln/SNYK-DEBIAN11-LIBSEPOL-1315635>  
Introduced through: gnupg2/dirmngr@2.2.27-2  
From: gnupg2/dirmngr@2.2.27-2 > adduser@3.118 > shadow/passwd@1:4.8.1-1 > libsemanage/libsemanage1@3.1-1+b2 > libsepol/libsepol1@3.1-1 X Low severity vulnerability found in libsepol/libsepol1  
Description: Use After Free  
Info: <https://snyk.io/vuln/SNYK-DEBIAN11-LIBSEPOL-1315641>  
Introduced through: gnupg2/dirmngr@2.2.27-2  
From: gnupg2/dirmngr@2.2.27-2 > adduser@3.118 > shadow/passwd@1:4.8.1-1 > libsemanage/libsemanage1@3.1-1+b2 > libsepol/libsepol1@3.1-1 X Low severity vulnerability found in gnutls28/libgnutls30  
Description: Improper Input Validation  
Info: <https://snyk.io/vuln/SNYK-DEBIAN11-GNUTLS28-515971>

Introduced through: gnupg2/dirmngr@2.2.27-2, postgresql-12@12.9-1.pgdg110+1  
 From: gnupg2/dirmngr@2.2.27-2 > gnutls28/libgnutls30@3.7.1-5  
 From: gnupg2/dirmngr@2.2.27-2 > openldap/libldap-2.4-2@2.4.57+dfsg-3 > gnutls28/libgnutls30@3.7.1-5  
 From: postgresql-12@12.9-1.pgdg110+1 > postgresql-12/postgresql-client-12@12.9-1.pgdg110+1 > postgresql-common/postgresql-client-common@232.pgdg110+1 > pgdg-keyring@2018.2 > apt@2.2.4 > gnutls28/libgnutls30@3.7.1-5 X Low severity vulnerability found in apt/libapt-pkg6.0  
 Description: Improper Verification of Cryptographic Signature  
 Info: <https://snyk.io/vuln/SNYK-DEBIAN11-APT-522585>  
 Introduced through: postgresql-12@12.9-1.pgdg110+1  
 From: postgresql-12@12.9-1.pgdg110+1 > postgresql-12/postgresql-client-12@12.9-1.pgdg110+1 > postgresql-common/postgresql-client-common@232.pgdg110+1 > pgdg-keyring@2018.2 > apt@2.2.4 > apt/libapt-pkg6.0@2.2.4  
 From: postgresql-12@12.9-1.pgdg110+1 > postgresql-12/postgresql-client-12@12.9-1.pgdg110+1 > postgresql-common/postgresql-client-common@232.pgdg110+1 > pgdg-keyring@2018.2 > apt@2.2.4 X High severity vulnerability found in perl/perl-base  
 Description: Improper Verification of Cryptographic Signature  
 Info: <https://snyk.io/vuln/SNYK-DEBIAN11-PERL-1925976>  
 Introduced through: meta-common-packages@meta, perl/libperl5.32@5.32.1-4+deb11u2, perl@5.32.1-4+deb11u2, perl/perl-modules-5.32@5.32.1-4+deb11u2  
 From: meta-common-packages@meta > perl/perl-base@5.32.1-4+deb11u2  
 From: perl/libperl5.32@5.32.1-4+deb11u2  
 From: perl@5.32.1-4+deb11u2 > perl/libperl5.32@5.32.1-4+deb11u2  
 and 4 more. X High severity vulnerability found in libgrypt20  
 Description: Information Exposure  
 Info: <https://snyk.io/vuln/SNYK-DEBIAN11-LIBGCRYPT20-1297892>  
 Introduced through: gnupg2/dirmngr@2.2.27-2, gnupg2/gnupg@2.2.27-2, postgresql-12@12.9-1.pgdg110+1  
 From: gnupg2/dirmngr@2.2.27-2 > libgrypt20@1.8.7-6  
 From: gnupg2/dirmngr@2.2.27-2 > gnupg2/gpgconf@2.2.27-2 > libgrypt20@1.8.7-6  
 From: gnupg2/gnupg@2.2.27-2 > gnupg2/gnupg-utils@2.2.27-2 > libgrypt20@1.8.7-6  
 and 9 more. X Critical severity vulnerability found in glibc/libc-bin  
 Description: Use After Free  
 Info: <https://snyk.io/vuln/SNYK-DEBIAN11-GLIBC-1296898>  
 Introduced through: glibc/locales@2.31-13+deb11u2, postgresql-12@12.9-1.pgdg110+1, meta-common-packages@meta  
 From: glibc/locales@2.31-13+deb11u2 > glibc/libc-bin@2.31-13+deb11u2  
 From: glibc/locales@2.31-13+deb11u2 > glibc/libc-l10n@2.31-13+deb11u2  
 From: glibc/locales@2.31-13+deb11u2  
 and 2 more.  
 Package manager: deb  
 Project name: docker-image|postgres  
 Docker image: postgres:12  
 Platform: linux/amd64  
 Base image: postgres:12.9-bullseye Tested 147 dependencies for known vulnerabilities, found 48 vulnerabilities. According to our scan, you are currently using the most secure version of the selected base image For more free scans that keep your images secure, sign up to Snyk at <https://dockr.ly/3ePqVcp>

## 5 How do I install Grype? Recommended:

```
curl -sSfL https://raw.githubusercontent.com/anchore/grype/main/install.sh | sh -s -- -b /usr/local/bin
...or, you can specify a release version and destination directory for the installation: curl -sSfL https://raw.githubusercontent.com/anchore/grype/main/install.sh | sh -s -- -b <DESTINATION_DIR> <RELEASE_VERSION>
```



## 6 How do I install Grype?

Homebrew:

```
brew tap anchore/grype
brew install grype
```

## 7 How do I install Grype?

Example output from a vulnerability scan:

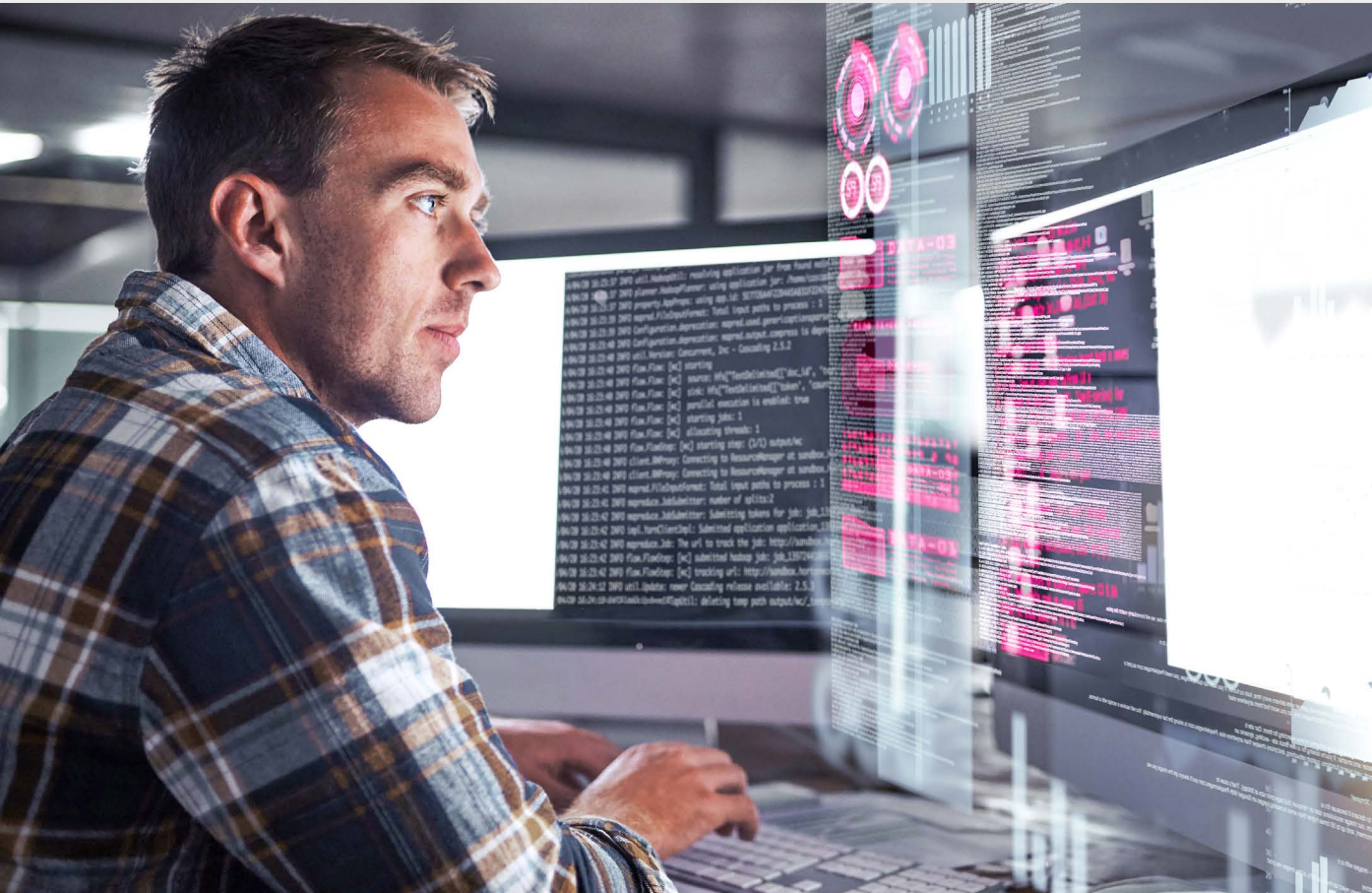
```
macpro$ grype k8s.gcr.io/kube-scheduler:v1.22.5 --scope all-layers
✓ Vulnerability DB [no update available]
✓ Loaded image
✓ Parsed image
✓ Cataloged packages [3 packages]
✓ Scanned image [0 vulnerabilities]No vulnerabilities found
macpro$ grype postgres:12 --scope all-layers
✓ Vulnerability DB [no update available]
✓ Loaded image
✓ Parsed image
✓ Cataloged packages [718 packages]
✓ Scanned image [550 vulnerabilities]
NAME                INSTALLED  FIXED-IN  VULNERABILITY  SEVERITY
apt                  2.2.4      CVE-2011-3374  Negligible
coreutils            8.32-4+b1  (won't fix) CVE-2016-2781  Low
coreutils            8.32-4+b1  CVE-2017-18018  Negligible
github.com/opencontainers/runc v1.0.1    1.0.3    GHSA-v95c-p5hm-xq8f  Medium
libapt-pkg6.0        2.2.4      CVE-2011-3374  Negligible
libc-bin             2.31-13+deb11u2  CVE-2021-43396  Negligible
libc-bin             2.31-13+deb11u2  CVE-2021-3998   Unknown
libc-bin             2.31-13+deb11u2  CVE-2021-3999   Unknown
libc-bin             2.31-13+deb11u2  (won't fix) CVE-2022-23218  Unknown
libc-bin             2.31-13+deb11u2  (won't fix) CVE-2022-23219  Unknown
libc-bin             2.31-13+deb11u2  CVE-2010-4756   Negligible
libc-bin             2.31-13+deb11u2  CVE-2018-20796  Negligible
libc-bin             2.31-13+deb11u2  CVE-2019-1010022  Negligible
libc-bin             2.31-13+deb11u2  CVE-2019-1010023  Negligible
libc-bin             2.31-13+deb11u2  CVE-2019-1010024  Negligible
libc-bin             2.31-13+deb11u2  CVE-2019-1010025  Negligible
libc-bin             2.31-13+deb11u2  CVE-2019-9192   Negligible
libc-bin             2.31-13+deb11u2  (won't fix) CVE-2021-33574  Critical
libc-l10n            2.31-13+deb11u2  CVE-2021-43396  Negligible
libc-l10n            2.31-13+deb11u2  CVE-2021-3998   Unknown
libc-l10n            2.31-13+deb11u2  CVE-2021-3999   Unknown
libc-l10n            2.31-13+deb11u2  (won't fix) CVE-2022-23218  Unknown
libc-l10n            2.31-13+deb11u2  (won't fix) CVE-2022-23219  Unknown
libc-l10n            2.31-13+deb11u2  CVE-2010-4756   Negligible
libc-l10n            2.31-13+deb11u2  CVE-2018-20796  Negligible
libc-l10n            2.31-13+deb11u2  CVE-2019-1010022  Negligible
libc-l10n            2.31-13+deb11u2  CVE-2019-1010023  Negligible
libc-l10n            2.31-13+deb11u2  CVE-2019-1010024  Negligible
libc-l10n            2.31-13+deb11u2  CVE-2019-1010025  Negligible
libc-l10n            2.31-13+deb11u2  CVE-2019-9192   Negligible
libc-l10n            2.31-13+deb11u2  (won't fix) CVE-2021-33574  Critical
libc6                2.31-13+deb11u2  CVE-2021-43396  Negligible
libc6                2.31-13+deb11u2  CVE-2021-3998   Unknown
libc6                2.31-13+deb11u2  CVE-2021-3999   Unknown
```



libc6	2.31-13+deb11u2	(won't fix) CVE-2022-23218	Unknown
libc6	2.31-13+deb11u2	(won't fix) CVE-2022-23219	Unknown
libc6	2.31-13+deb11u2	CVE-2010-4756	Negligible
libc6	2.31-13+deb11u2	CVE-2018-20796	Negligible
libc6	2.31-13+deb11u2	CVE-2019-1010022	Negligible
libc6	2.31-13+deb11u2	CVE-2019-1010023	Negligible
libc6	2.31-13+deb11u2	CVE-2019-1010024	Negligible
libc6	2.31-13+deb11u2	CVE-2019-1010025	Negligible
libc6	2.31-13+deb11u2	CVE-2019-9192	Negligible
libc6	2.31-13+deb11u2	(won't fix) CVE-2021-33574	Critical
libgcrypt20	1.8.7-6	(won't fix) CVE-2021-33560	High
libgcrypt20	1.8.7-6	CVE-2018-6829	Negligible
libgnutls30	3.7.1-5	CVE-2011-3389	Medium
libgssapi-krb5-2	1.18.3-6+deb11u1	CVE-2004-0971	Negligible
libgssapi-krb5-2	1.18.3-6+deb11u1	CVE-2018-5709	Negligible
libk5crypto3	1.18.3-6+deb11u1	CVE-2004-0971	Negligible
libk5crypto3	1.18.3-6+deb11u1	CVE-2018-5709	Negligible
libkrb5-3	1.18.3-6+deb11u1	CVE-2004-0971	Negligible
libkrb5-3	1.18.3-6+deb11u1	CVE-2018-5709	Negligible
libkrb5support0	1.18.3-6+deb11u1	CVE-2004-0971	Negligible
libkrb5support0	1.18.3-6+deb11u1	CVE-2018-5709	Negligible
libldap-2.4-2	2.4.57+dfsg-3	CVE-2015-3276	Negligible
libldap-2.4-2	2.4.57+dfsg-3	CVE-2017-14159	Negligible
libldap-2.4-2	2.4.57+dfsg-3	CVE-2017-17740	Negligible
libldap-2.4-2	2.4.57+dfsg-3	CVE-2020-15719	Negligible
libncursesw6	6.2+20201114-2	CVE-2021-39537	Negligible
libpcre3	2:8.39-13	CVE-2017-11164	Negligible
libpcre3	2:8.39-13	CVE-2017-16231	Negligible
libpcre3	2:8.39-13	CVE-2017-7245	Negligible
libpcre3	2:8.39-13	CVE-2017-7246	Negligible
libpcre3	2:8.39-13	CVE-2019-20838	Negligible
libperl5.32	5.32.1-4+deb11u2	CVE-2011-4116	Negligible
libperl5.32	5.32.1-4+deb11u2	(won't fix) CVE-2020-16156	High
libsepol1	3.1-1	(won't fix) CVE-2021-36084	Low
libsepol1	3.1-1	(won't fix) CVE-2021-36085	Low
libsepol1	3.1-1	(won't fix) CVE-2021-36086	Low
libsepol1	3.1-1	(won't fix) CVE-2021-36087	Low
libsqlite3-0	3.34.1-3	CVE-2021-36690	Negligible
libssl1.1	1.1.1k-1+deb11u1	CVE-2007-6755	Negligible
libssl1.1	1.1.1k-1+deb11u1	CVE-2010-0928	Negligible
libsystemd0	247.3-6	CVE-2013-4392	Negligible
libsystemd0	247.3-6	CVE-2020-13529	Negligible
libsystemd0	247.3-6	(won't fix) CVE-2021-3997	Unknown
libtinfo6	6.2+20201114-2	CVE-2021-39537	Negligible
libudev1	247.3-6	CVE-2013-4392	Negligible
libudev1	247.3-6	CVE-2020-13529	Negligible
libudev1	247.3-6	(won't fix) CVE-2021-3997	Unknown
libxslt1.1	1.1.34-4	CVE-2015-9019	Negligible
locales	2.31-13+deb11u2	CVE-2021-43396	Negligible
locales	2.31-13+deb11u2	CVE-2021-3998	Unknown
locales	2.31-13+deb11u2	CVE-2021-3999	Unknown
locales	2.31-13+deb11u2	(won't fix) CVE-2022-23218	Unknown
locales	2.31-13+deb11u2	(won't fix) CVE-2022-23219	Unknown
locales	2.31-13+deb11u2	CVE-2010-4756	Negligible
locales	2.31-13+deb11u2	CVE-2018-20796	Negligible
locales	2.31-13+deb11u2	CVE-2019-1010022	Negligible
locales	2.31-13+deb11u2	CVE-2019-1010023	Negligible
locales	2.31-13+deb11u2	CVE-2019-1010024	Negligible
locales	2.31-13+deb11u2	CVE-2019-1010025	Negligible
locales	2.31-13+deb11u2	CVE-2019-9192	Negligible
locales	2.31-13+deb11u2	(won't fix) CVE-2021-33574	Critical
login	1:4.8.1-1	CVE-2007-5686	Negligible



login	1:4.8.1-1	CVE-2013-4235	Negligible
login	1:4.8.1-1	CVE-2019-19882	Negligible
ncurses-base	6.2+20201114-2	CVE-2021-39537	Negligible
ncurses-bin	6.2+20201114-2	CVE-2021-39537	Negligible
openssl	1.1.1k-1+deb11u1	CVE-2007-6755	Negligible
openssl	1.1.1k-1+deb11u1	CVE-2010-0928	Negligible
passwd	1:4.8.1-1	CVE-2007-5686	Negligible
passwd	1:4.8.1-1	CVE-2013-4235	Negligible
passwd	1:4.8.1-1	CVE-2019-19882	Negligible
perl	5.32.1-4+deb11u2	CVE-2011-4116	Negligible
perl	5.32.1-4+deb11u2 (won't fix)	CVE-2020-16156	High
perl-base	5.32.1-4+deb11u2	CVE-2011-4116	Negligible
perl-base	5.32.1-4+deb11u2 (won't fix)	CVE-2020-16156	High
perl-modules-5.32	5.32.1-4+deb11u2	CVE-2011-4116	Negligible
perl-modules-5.32	5.32.1-4+deb11u2 (won't fix)	CVE-2020-16156	High
tar	1.34+dfsg-1	CVE-2005-2541	Negligible



### Your Contact

Email: [info@t-systems.com](mailto:info@t-systems.com)  
Internet: [www.t-systems.com](http://www.t-systems.com)

### Publisher

T-Systems International GmbH  
Hahnstr. 43d  
60528 Frankfurt am Main  
Germany

