Docker Security Scan Report

Scan Information

Image:	python:3.9-slim
Dockerfile:	.\testfiles\1\Dockerfile
Scan Date:	2025-03-01 22:42:09

Dockerfile Scan Results

Dockerfile linting issues:

```
.\testfiles\1\Dockerfile:81 SC3037  [1m [93mwarning [0m: In POSIX sh, echo flags are undefined.
.\testfiles\1\Dockerfile:81  DL3059  [92minfo [0m: Multiple consecutive `RUN` instructions. Consider
consolidation.
.\testfiles\1\Dockerfile:83 DL4006  [1m [93mwarning [0m: Set the SHELL option -o pipefail before RUN with a
pipe in it. If you are using /bin/sh in an alpine image or if your shell is symlinked to busybox then consider
explicitly setting your SHELL to /bin/ash, or disable this check
.\testfiles\1\Dockerfile:83 DL3008  [1m [93mwarning [0m: Pin versions in apt get install. Instead of `apt-get
install <package>` use `apt-get install <package>=<version>`
.\testfiles\1\Dockerfile:108 DL3013  [1m [93mwarning [0m: Pin versions in pip. Instead of `pip install
<package>` use `pip install <package>==<version>` or `pip install --requirement <requirements file>`
.\testfiles\1\Dockerfile:108 DL3042  [1m [93mwarning [0m: Avoid use of cache directory with pip. Use `pip
install --no-cache-dir <package>`
```

Vulnerability Scan Summary

Total vulnerabilities: 74

LOW: 70

HIGH: 3

CRITICAL: 1

Vulnerability Details

Vulnerability ID	Severity	Package	Version	Title/Description
CVE-2011-3374	LOW	apt	2.6.1	It was found that apt-key in apt, all versions, do not correctly valid ...
TEMP-0841856-B18BAF	LOW	bash	5.2.15-2+b7	[Privilege escalation possible to other user than root]
CVE-2022-0563	LOW	bsdutils	1:2.38.1-5+deb12u3	util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled with libreadline
CVE-2016-2781	LOW	coreutils	9.1-1	coreutils: Non-privileged session can escape to the parent session in chroot

CVE-2017-18018	LOW	coreutils	9.1-1	coreutils: race condition vulnerability in chown and chgrp
CVE-2022-27943	LOW	gcc-12-base	12.2.0-14	binutils: libiberty/rust-demangle.c in GNU GCC 11.2 allows stack exhaustion in demangle_const
CVE-2023-4039	LOW	gcc-12-base	12.2.0-14	gcc: -fstack-protector fails to guard dynamic stack allocations on ARM64
CVE-2022-3219	LOW	gpgv	2.2.40-1.1	gnupg: denial of service issue (resource consumption) using compressed packets
CVE-2011-3374	LOW	libapt-pkg6.0	2.6.1	It was found that apt-key in apt, all versions, do not correctly valid ...
CVE-2022-0563	LOW	libblkid1	2.38.1-5+deb12u3	util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled with libreadline
CVE-2010-4756	LOW	libc-bin	2.36-9+deb12u9	glibc: glob implementation can cause excessive CPU and memory consumption due to crafted glob expressions
CVE-2018-20796	LOW	libc-bin	2.36-9+deb12u9	glibc: uncontrolled recursion in function check_dst_limits_calc_pos_1 in posix/regexec.c
CVE-2019-1010022	LOW	libc-bin	2.36-9+deb12u9	glibc: stack guard protection bypass
CVE-2019-1010023	LOW	libc-bin	2.36-9+deb12u9	glibc: running ldd on malicious ELF leads to code execution because of wrong size computation
CVE-2019-1010024	LOW	libc-bin	2.36-9+deb12u9	glibc: ASLR bypass using cache of thread stack and heap
CVE-2019-1010025	LOW	libc-bin	2.36-9+deb12u9	glibc: information disclosure of heap addresses of pthread_created thread
CVE-2019-9192	LOW	libc-bin	2.36-9+deb12u9	glibc: uncontrolled recursion in function check_dst_limits_calc_pos_1 in posix/regexec.c
CVE-2010-4756	LOW	libc6	2.36-9+deb12u9	glibc: glob implementation can cause excessive CPU and memory consumption due to crafted glob expressions
CVE-2018-20796	LOW	libc6	2.36-9+deb12u9	glibc: uncontrolled recursion in function check_dst_limits_calc_pos_1 in posix/regexec.c
CVE-2019-1010022	LOW	libc6	2.36-9+deb12u9	glibc: stack guard protection bypass
CVE-2019-1010023	LOW	libc6	2.36-9+deb12u9	glibc: running ldd on malicious ELF leads to code execution because of wrong size computation
CVE-2019-1010024	LOW	libc6	2.36-9+deb12u9	glibc: ASLR bypass using cache of thread stack and heap
CVE-2019-1010025	LOW	libc6	2.36-9+deb12u9	glibc: information disclosure of heap addresses of pthread_created thread
CVE-2019-9192	LOW	libc6	2.36-9+deb12u9	glibc: uncontrolled recursion in function check_dst_limits_calc_pos_1 in posix/regexec.c

CVE-2022-27943	LOW	libgcc-s1	12.2.0-14	binutils: libiberty/rust-demangle.c in GNU GCC 11.2 allows stack exhaustion in demangle_const
CVE-2023-4039	LOW	libgcc-s1	12.2.0-14	gcc: -fstack-protector fails to guard dynamic stack allocations on ARM64
CVE-2018-6829	LOW	libgcrypt20	1.10.1-3	libgcrypt: ElGamal implementation doesn't have semantic security due to incorrectly encoded plaintexts possibly allowing to obtain sensitive information
CVE-2011-3389	LOW	libgnutls30	3.7.9-2+deb12u3	HTTPS: block-wise chosen-plaintext attack against SSL/TLS (BEAST)
CVE-2018-5709	LOW	libgssapi-krb5-2	1.20.1-2+deb12u2	krb5: integer overflow in dbentry->n_key_data in
CVE-2024-26458	LOW	libgssapi-krb5-2	1.20.1-2+deb12u2	krb5: Memory leak at /krb5/src/lib/rpc/pmap_rmt.c
CVE-2024-26461	LOW	libgssapi-krb5-2	1.20.1-2+deb12u2	krb5: Memory leak at /krb5/src/lib/gssapi/krb5/k5sealv3.c
CVE-2018-5709	LOW	libk5crypto3	1.20.1-2+deb12u2	krb5: integer overflow in dbentry->n_key_data in
CVE-2024-26458	LOW	libk5crypto3	1.20.1-2+deb12u2	krb5: Memory leak at /krb5/src/lib/rpc/pmap_rmt.c
CVE-2024-26461	LOW	libk5crypto3	1.20.1-2+deb12u2	krb5: Memory leak at /krb5/src/lib/gssapi/krb5/k5sealv3.c
CVE-2018-5709	LOW	libkrb5-3	1.20.1-2+deb12u2	krb5: integer overflow in dbentry->n_key_data in
CVE-2024-26458	LOW	libkrb5-3	1.20.1-2+deb12u2	krb5: Memory leak at /krb5/src/lib/rpc/pmap_rmt.c
CVE-2024-26461	LOW	libkrb5-3	1.20.1-2+deb12u2	krb5: Memory leak at /krb5/src/lib/gssapi/krb5/k5sealv3.c
CVE-2018-5709	LOW	libkrb5support0	1.20.1-2+deb12u2	krb5: integer overflow in dbentry->n_key_data in
CVE-2024-26458	LOW	libkrb5support0	1.20.1-2+deb12u2	krb5: Memory leak at /krb5/src/lib/rpc/pmap_rmt.c
CVE-2024-26461	LOW	libkrb5support0	1.20.1-2+deb12u2	krb5: Memory leak at /krb5/src/lib/gssapi/krb5/k5sealv3.c
CVE-2022-0563	LOW	libmount1	2.38.1-5+deb12u3	util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled with libreadline
CVE-2022-0563	LOW	libsmartcols1	2.38.1-5+deb12u3	util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled with libreadline
CVE-2021-45346	LOW	libsqlite3-0	3.40.1-2+deb12u1	sqlite: crafted SQL query allows a malicious user to obtain sensitive information
CVE-2022-27943	LOW	libstdc++6	12.2.0-14	binutils: libiberty/rust-demangle.c in GNU GCC 11.2 allows stack exhaustion in demangle_const
CVE-2023-4039	LOW	libstdc++6	12.2.0-14	gcc: -fstack-protector fails to guard dynamic stack allocations on ARM64
CVE-2013-4392	LOW	libsystemd0	252.33-1~deb12u1	systemd: TOCTOU race condition when updating file permissions and SELinux security contexts

CVE-2023-31437	LOW	libsystemd0	252.33-1~deb12u1	An issue was discovered in systemd 253. An attacker can modify a seale ...
CVE-2023-31438	LOW	libsystemd0	252.33-1~deb12u1	An issue was discovered in systemd 253. An attacker can truncate a sea ...
CVE-2023-31439	LOW	libsystemd0	252.33-1~deb12u1	An issue was discovered in systemd 253. An attacker can modify the con ...
CVE-2013-4392	LOW	libudev1	252.33-1~deb12u1	systemd: TOCTOU race condition when updating file permissions and SELinux security contexts

Note: Only showing 50 of 74 vulnerabilities. See CSV for complete list.

CVSS Score Details

Vulnerability ID	CVSS Score	Description
CVE-2011-3374	3.7	It was found that apt-key in apt, all versions, do not correctly validate gpg keys with the master keyring, leading to a potential man-in-the-middle a...
CVE-2022-0563	5.5	A flaw was found in the util-linux chfn and chsh utilities when compiled with Readline support. The Readline library uses an "INPUTRC" environment var...
CVE-2016-2781	6.5	chroot in GNU coreutils, when used with --userspec, allows local users to escape to the parent session via a crafted TIOCSTI ioctl call, which pushes ...
CVE-2017-18018	4.7	In GNU Coreutils through 8.29, chown-core.c in chown and chgrp does not prevent replacement of a plain file with a symlink during use of the POSIX "-R...
CVE-2022-27943	5.5	libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as demonstrated by nm-new.
CVE-2023-4039	4.8	**DISPUTED**A failure in the -fstack-protector feature in GCC-based toolchains that target AArch64 allows an attacker to exploit an existing buffer
CVE-2022-3219	3.3	GnuPG can be made to spin on a relatively small input by (for example) crafting a public key with thousands of signatures attached, compressed down to...
CVE-2011-3374	3.7	It was found that apt-key in apt, all versions, do not correctly validate gpg keys with the master keyring, leading to a potential man-in-the-middle a...
CVE-2022-0563	5.5	A flaw was found in the util-linux chfn and chsh utilities when compiled with Readline support. The Readline library uses an "INPUTRC" environment var...
CVE-2018-20796	7.5	In the GNU C Library (aka glibc or libc6) through 2.29, check_dst_limits_calc_pos_1 in posix/regexec.c has Uncontrolled Recursion, as demonstrated by ...
CVE-2019-1010022	9.8	GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may bypass stack guard protection. The component is: nptl. The attack vect...
CVE-2019-1010023	8.8	GNU Libc current is affected by: Re-mapping current loaded library with malicious ELF file. The impact is: In worst case attacker may evaluate privile...
CVE-2019-1010024	5.3	GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may bypass ASLR using cache of thread stack and heap. The component is: gl...
CVE-2019-1010025	5.3	GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may guess the heap addresses of pthread_created thread. The component is: ...
CVE-2019-9192	7.5	In the GNU C Library (aka glibc or libc6) through 2.29, check_dst_limits_calc_pos_1 in posix/regexec.c has Uncontrolled Recursion, as demonstrated by ...
CVE-2018-20796	7.5	In the GNU C Library (aka glibc or libc6) through 2.29, check_dst_limits_calc_pos_1 in posix/regexec.c has Uncontrolled Recursion, as demonstrated by ...
CVE-2019-1010022	9.8	GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may bypass stack guard protection. The component is: nptl. The attack vect...
CVE-2019-1010023	8.8	GNU Libc current is affected by: Re-mapping current loaded library with malicious ELF file. The impact is: In worst case attacker may evaluate privile...
CVE-2019-1010024	5.3	GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may bypass ASLR using cache of thread stack and heap. The component is: gl...
CVE-2019-1010025	5.3	GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may guess the heap addresses of pthread_created thread. The component is: ...
CVE-2019-9192	7.5	In the GNU C Library (aka glibc or libc6) through 2.29, check_dst_limits_calc_pos_1 in posix/regexec.c has Uncontrolled Recursion, as demonstrated by ...
CVE-2022-27943	5.5	libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as demonstrated by nm-new.
CVE-2023-4039	4.8	**DISPUTED**A failure in the -fstack-protector feature in GCC-based toolchains that target AArch64 allows an attacker to exploit an existing buffer
CVE-2018-6829	7.5	cipher/elgamal.c in Libgcrypt through 1.8.2, when used to encrypt messages directly, improperly encodes plaintexts, which allows attackers to obtain s...
CVE-2018-5709	7.5	An issue was discovered in MIT Kerberos 5 (aka krb5) through 1.16. There is a variable "dbentry->n_key_data" in kadmin/dbutil/dump.c that can store 16...

CVE-2018-5709

7.5

An issue was discovered in MIT Kerberos 5 (aka krb5) through 1.16. There is a variable "dbentry->n_key_data" in kadmin/dbutil/dump.c that can store 16...

CVE-2018-5709

7.5

An issue was discovered in MIT Kerberos 5 (aka krb5) through 1.16. There is a variable "dbentry->n_key_data" in kadmin/dbutil/dump.c that can store 16...

CVE-2018-5709

7.5

An issue was discovered in MIT Kerberos 5 (aka krb5) through 1.16. There is a variable "dbentry->n_key_data" in kadmin/dbutil/dump.c that can store 16...

CVE-2022-0563

5.5

A flaw was found in the util-linux chfn and chsh utilities when compiled with Readline support. The Readline library uses an "INPUTRC" environment var...

CVE-2022-0563

5.5

A flaw was found in the util-linux chfn and chsh utilities when compiled with Readline support. The Readline library uses an "INPUTRC" environment var...

CVE-2021-45346

4.3

A Memory Leak vulnerability exists in SQLite Project SQLite3 3.35.1 and 3.37.0 via maliciously crafted SQL Queries (made via editing the Database File...

CVE-2022-27943

5.5

libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as demonstrated by nm-new.

CVE-2023-4039

4.8

DISPUTEDA failure in the -fstack-protector feature in GCC-based toolchains
that target AArch64 allows an attacker to exploit an existing buffer
...

CVE-2023-31437

5.3

An issue was discovered in systemd 253. An attacker can modify a sealed log file such that, in some views, not all existing and sealed log messages ar...

CVE-2023-31438

5.3

An issue was discovered in systemd 253. An attacker can truncate a sealed log file and then resume log sealing such that checking the integrity shows ...

CVE-2023-31439

5.3

An issue was discovered in systemd 253. An attacker can modify the contents of past events in a sealed log file and then adjust the file such that che...