Docker Security Scan Report

Scan Information

Image: python:3.9-slim

Dockerfile: .\testfiles\2\Dockerfile

Scan Date: 2025-03-01 16:13:33

Dockerfile Scan Results

Dockerfile linting issues:

```
.\testfiles\2\Dockerfile:103 SC3037  [1m [93mwarning [0m: In POSIX sh, echo flags are undefined.
.\testfiles\2\Dockerfile:103  DL3059  [92minfo [0m:  Multiple  consecutive  `RUN`  instructions.  Consider consolidation.
.\testfiles\2\Dockerfile:106  DL3059  [92minfo [0m:  Multiple  consecutive  `RUN`  instructions.  Consider consolidation.
.\testfiles\2\Dockerfile:108 DL3008  [1m [93mwarning [0m: Pin versions in apt get install. Instead of `apt-get install <package>` use `apt-get install <package>=<version>`
.\testfiles\2\Dockerfile:108 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\2\Dockerfile:135  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\2\Dockerfile:135  DL3042  [1m [93mwarning [0m:  Avoid  use  of  cache  directory  with  pip.  Use  `pip install --no-cache-dir <package>`
```

Vulnerability Scan Summary

Total vulnerabilities: 4

HIGH: 3

CRITICAL: 1

Vulnerability Details

Vulnerability ID	Severity	Package	Version	Title/Description
CVE-2023-31484	HIGH	perl-base	5.36.0-7+deb12u1	perl: CPAN.pm does not verify TLS certificates when downloading distributions over HTTPS
CVE-2023-45853	CRITICAL	zlib1g	1:1.2.13.dfsg-1	zlib: integer overflow and resultant heap-based buffer overflow in zipOpenNewFileInZip4_6
CVE-2022-40897	HIGH	setuptools	58.1.0	pypa-setuptools: Regular Expression Denial of Service (ReDoS) in package_index.py

CVE-2024-6345	HIGH	setuptools	58.1.0	pypa/setuptools: Remote code execution via download functions in the package_index module in pypa/setuptools

CVSS Score Details

Vulnerability ID	CVSS Score	Description
CVE-2023-31484	8.1	CPAN.pm before 2.35 does not verify TLS certificates when downloading distributions over HTTPS.
CVE-2023-45853	9.8	MiniZip in zlib through 1.3 has an integer overflow and resultant heap-based buffer overflow in zipOpenNewFileInZip4_64 via a long filename, comment, ...
CVE-2022-40897	5.9	Python Packaging Authority (PyPA) setuptools before 65.5.1 allows remote attackers to cause a denial of service via HTML in a crafted package or custo...