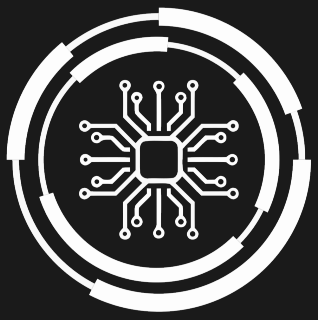
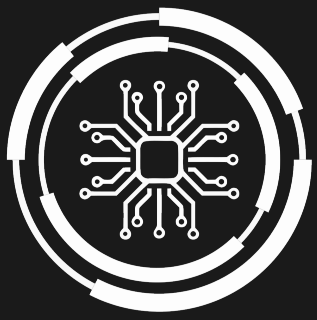


Manual & Security Audit for Train

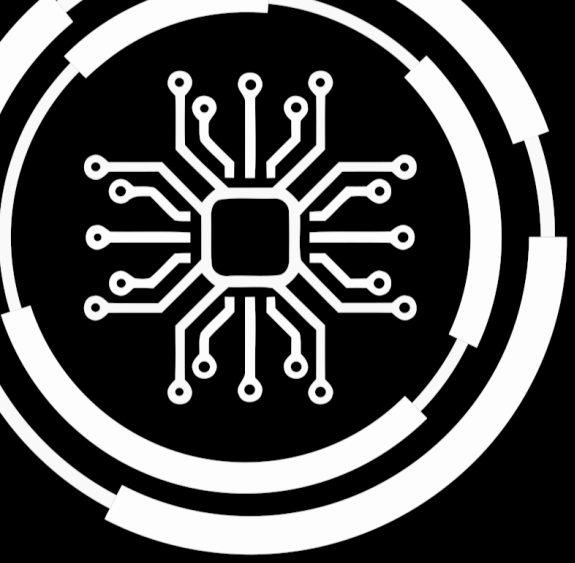
ImageAnalysis

Karl Kindermann



PADME-ANALYTICS.DE

First printing, February 1, 2024



Contents

1. Train Summary

1.1 Overview

- **Train name:** ImageAnalysis
- **Creator of the train:** Karl Kindermann
- **Location:** `https://git.rwth-aachen.de/padme-development/padme-train-depot/-/archive/main/padme-train-depot-main.zip?path=ImageAnalysis`

1.2 Image Building File

Listing 1.1: Image building file

```
FROM python:3.10.0a7-buster

WORKDIR /usr/src/app

# LABEL
LABEL "envs"="[{\"name\": \"DB_NAME\",\"type\": \"text\",\"
   required\": true},{\"name\": \"DATA_SOURCE_USERNAME\",\"
   type\": \"text\",\"required\": true},{\"name\": \"
   DATA_SOURCE_HOST\",\"type\": \"text\",\"required\": true
   },{\"name\": \"DATA_SOURCE_PORT\",\"type\": \"number\",\"
   required\": true},{\"name\": \"DATA_SOURCE_PASSWORD\",\"
   type\": \"password\",\"required\": true},{\"name\": \"
   STATION_NAME\",\"type\": \"text\",\"required\": true}]"

COPY . .

CMD [ "python", "main.py" ]
```

1.3 Requirements & Dependencies

No requirements.txt found

1.4 Code Base

Legend: env query retrieve_previous_results execute_analysis save log

```
1 print("Hello World!")
```

Listing 1.2: main.py

1.5 Connection Parameters

Overall, 6 connection parameters have been found in the train:

Name	Type	Required?
DB_NAME	text	True
DATA_SOURCE_USERNAME	text	True
DATA_SOURCE_HOST	text	True
DATA_SOURCE_PORT	number	True
DATA_SOURCE_PASSWORD	password	True
STATION_NAME	text	True

2. Static Train Analysis

Summary 2.1

- **Number of Lines:** 223820
- **Vulnerabilities per Line:** 0.0
- **Analysis Score:** 1.0

Total

Summary: Low: 0 Medium: 0 High: 0

2.1 SAST

Summary: Low: 0 Medium: 0 High: 0

Detailed Vulnerabilities:

2.2 Secret Detection

Summary: Low: 0 Medium: 0 High: 0

Detailed Secret Detection:

2.3 Dependency Analysis

Summary: Low: 0 Medium: 0 High: 0

Detailed Dependency Analysis:

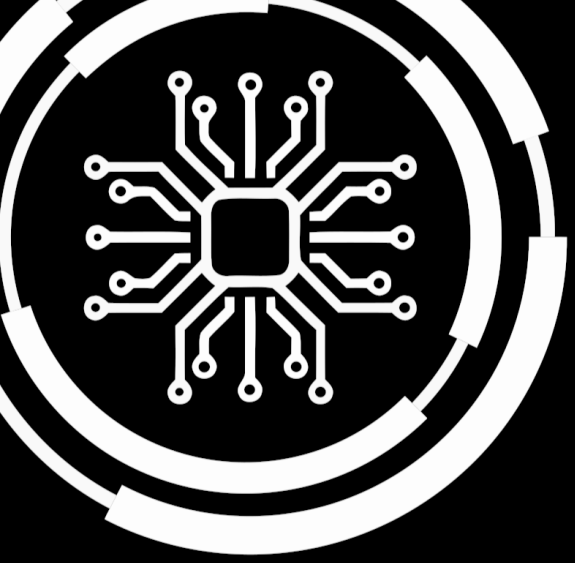
2.4 Blacklist Detection

The following patterns have been configured:

`\bPOST\b`

The following matches have been found:

None



3. Train Image Analysis

3.1 Vulnerabilities

Summary: Low: 395 Medium: 246 High: 169 Critical: 49

Detailed Vulnerabilities:

Critical:

Vulnerability 3.1

Test-specific ID: SNYK-DEBIAN10-BLUEZ-1911955 **Severity:** critical
Identifiers: **Message**:Use After Free

Vulnerability 3.2

Test-specific ID: SNYK-DEBIAN10-CURL-3065760 **Severity:** critical
Identifiers: **Message**:Exposure of Resource to Wrong Sphere

Vulnerability 3.3

Test-specific ID: SNYK-DEBIAN10-DB53-2825169 **Severity:** critical
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.4

Test-specific ID: SNYK-DEBIAN10-DPKG-2847944 **Severity:** critical
Identifiers: **Message**:Directory Traversal

Vulnerability 3.5

Test-specific ID: SNYK-DEBIAN10-EXPAT-2331803 **Severity:** critical
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.6

Test-specific ID: SNYK-DEBIAN10-EXPAT-2331813 **Severity:** critical
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.7

Test-specific ID: SNYK-DEBIAN10-EXPAT-2331818 **Severity:** critical
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.8

Test-specific ID: SNYK-DEBIAN10-EXPAT-2359258 **Severity:** critical
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.9

Test-specific ID: SNYK-DEBIAN10-EXPAT-2403513 **Severity:** critical
Identifiers: **Message**:Improper Encoding or Escaping of Output

Vulnerability 3.10

Test-specific ID: SNYK-DEBIAN10-EXPAT-2403518 **Severity:** critical
Identifiers: **Message**:Exposure of Resource to Wrong Sphere

Vulnerability 3.11

Test-specific ID: SNYK-DEBIAN10-EXPAT-2406128 **Severity:** critical

Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.12

Test-specific ID: SNYK-DEBIAN10-FREETYPE-2774655 **Severity:** critical
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.13

Test-specific ID: SNYK-DEBIAN10-GIT-3232718 **Severity:** critical
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.14

Test-specific ID: SNYK-DEBIAN10-GIT-3232719 **Severity:** critical
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.15

Test-specific ID: SNYK-DEBIAN10-GLIBC-1296899 **Severity:** critical
Identifiers: **Message**:Use After Free

Vulnerability 3.16

Test-specific ID: SNYK-DEBIAN10-GLIBC-1315333 **Severity:** critical
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.17

Test-specific ID: SNYK-DEBIAN10-GLIBC-2340915 **Severity:** critical
Identifiers: **Message**:Buffer Overflow

Vulnerability 3.18

Test-specific ID: SNYK-DEBIAN10-GLIBC-2340923 **Severity:** critical
Identifiers: **Message**:Buffer Overflow

Vulnerability 3.19

Test-specific ID: SNYK-DEBIAN10-GNUTLS28-1085094 **Severity:** critical
Identifiers: **Message**:Use After Free

Vulnerability 3.20

Test-specific ID: SNYK-DEBIAN10-GNUTLS28-1085097 **Severity:** critical
Identifiers: **Message**:Use After Free

Vulnerability 3.21

Test-specific ID: SNYK-DEBIAN10-LIBKSBA-3050754 **Severity:** critical
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.22

Test-specific ID: SNYK-DEBIAN10-LIBKSBA-3179190 **Severity:** critical
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.23

Test-specific ID: SNYK-DEBIAN10-LIBTASN16-3061094 **Severity:** critical
Identifiers: **Message**:Off-by-one Error

Vulnerability 3.24

Test-specific ID: SNYK-DEBIAN10-LIBWEBP-1289553 **Severity:** critical
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.25

Test-specific ID: SNYK-DEBIAN10-LIBWEBP-1289561 **Severity:** critical
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.26
Test-specific ID: SNYK-DEBIAN10-LIBWEBP-1289573 **Severity:** critical
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.27
Test-specific ID: SNYK-DEBIAN10-LIBWEBP-1289576 **Severity:** critical
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.28
Test-specific ID: SNYK-DEBIAN10-LIBWEBP-1289584 **Severity:** critical
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.29
Test-specific ID: SNYK-DEBIAN10-LIBWEBP-1289586 **Severity:** critical
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.30
Test-specific ID: SNYK-DEBIAN10-LIBWEBP-1289591 **Severity:** critical
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.31
Test-specific ID: SNYK-DEBIAN10-LIBWEBP-1289592 **Severity:** critical
Identifiers: **Message**:Use After Free

Vulnerability 3.32
Test-specific ID: SNYK-DEBIAN10-LIBWEBP-1289593 **Severity:** critical
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.33
Test-specific ID: SNYK-DEBIAN10-LIBWEBP-1290149 **Severity:** critical
Identifiers: **Message**:Use of Uninitialized Resource

Vulnerability 3.34
Test-specific ID: SNYK-DEBIAN10-LIBX11-1293573 **Severity:** critical
Identifiers: **Message**:Buffer Overflow

Vulnerability 3.35
Test-specific ID: SNYK-DEBIAN10-LZ4-1277601 **Severity:** critical
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.36
Test-specific ID: SNYK-DEBIAN10-OPENLDAP-2808412 **Severity:** critical
Identifiers: **Message**:SQL Injection

Vulnerability 3.37
Test-specific ID: SNYK-DEBIAN10-OPENSSH-5788320 **Severity:** critical
Identifiers: **Message**:Unquoted Search Path or Element

Vulnerability 3.38
Test-specific ID: SNYK-DEBIAN10-OPENSSL-1569403 **Severity:** critical
Identifiers: **Message**:Buffer Overflow

Vulnerability 3.39
Test-specific ID: SNYK-DEBIAN10-OPENSSL-2807585 **Severity:** critical
Identifiers: **Message**:OS Command Injection

Vulnerability 3.40

Test-specific ID: SNYK-DEBIAN10-OPENSSL-2933515 **Severity:** critical
Identifiers: **Message**:OS Command Injection

Vulnerability 3.41

Test-specific ID: SNYK-DEBIAN10-PCRE2-2808696 **Severity:** critical
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.42

Test-specific ID: SNYK-DEBIAN10-PCRE2-2808698 **Severity:** critical
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.43

Test-specific ID: SNYK-DEBIAN10-PYTHON27-1063178 **Severity:** critical
Identifiers: **Message**:Buffer Overflow

Vulnerability 3.44

Test-specific ID: SNYK-DEBIAN10-PYTHON27-5853772 **Severity:** critical
Identifiers: **Message**:XML External Entity (XXE) Injection

Vulnerability 3.45

Test-specific ID: SNYK-DEBIAN10-PYTHON37-3090928 **Severity:** critical
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.46

Test-specific ID: SNYK-DEBIAN10-PYTHON37-5851336 **Severity:** critical
Identifiers: **Message**:XML External Entity (XXE) Injection

Vulnerability 3.47
Test-specific ID: SNYK-DEBIAN10-SQLITE3-3011634 **Severity:** critical
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.48
Test-specific ID: SNYK-DEBIAN10-ZLIB-2976149 **Severity:** critical
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.49
Test-specific ID: SNYK-DEBIAN10-ZLIB-6008964 **Severity:** critical
Identifiers: **Message**:Integer Overflow or Wraparound

High:

Vulnerability 3.50
Test-specific ID: SNYK-DEBIAN10-BLUEZ-1018718 **Severity:** high
Identifiers: **Message**:Double Free

Vulnerability 3.51
Test-specific ID: SNYK-DEBIAN10-BLUEZ-1926134 **Severity:** high
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.52
Test-specific ID: SNYK-DEBIAN10-BLUEZ-2340898 **Severity:** high
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.53
Test-specific ID: SNYK-DEBIAN10-BLUEZ-3014387 **Severity:** high
Identifiers: **Message**:CVE-2022-39176

Vulnerability 3.54
Test-specific ID: SNYK-DEBIAN10-BLUEZ-3014393 **Severity:** high
Identifiers: **Message**:CVE-2022-39177

Vulnerability 3.55
Test-specific ID: SNYK-DEBIAN10-CURL-1585139 **Severity:** high
Identifiers: **Message**:Cleartext Transmission of Sensitive Information

Vulnerability 3.56
Test-specific ID: SNYK-DEBIAN10-CURL-2805484 **Severity:** high
Identifiers: **Message**:Missing Authentication for Critical Function

Vulnerability 3.57
Test-specific ID: SNYK-DEBIAN10-CURL-2813757 **Severity:** high
Identifiers: **Message**:Improper Certificate Validation

Vulnerability 3.58
Test-specific ID: SNYK-DEBIAN10-CURL-2813772 **Severity:** high
Identifiers: **Message**:Loop with Unreachable Exit Condition (’Infinite Loop’)

Vulnerability 3.59
Test-specific ID: SNYK-DEBIAN10-CURL-3366771 **Severity:** high
Identifiers: **Message**:Arbitrary Code Injection

Vulnerability 3.60
Test-specific ID: SNYK-DEBIAN10-CYRUSSASL2-2412041 **Severity:** high
Identifiers: **Message**:SQL Injection

Vulnerability 3.61

Test-specific ID: SNYK-DEBIAN10-DJVULIBRE-1278421 **Severity:** high
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.62

Test-specific ID: SNYK-DEBIAN10-DJVULIBRE-1290628 **Severity:** high
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.63

Test-specific ID: SNYK-DEBIAN10-DJVULIBRE-1290629 **Severity:** high
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.64

Test-specific ID: SNYK-DEBIAN10-DJVULIBRE-1290633 **Severity:** high
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.65

Test-specific ID: SNYK-DEBIAN10-DJVULIBRE-1290638 **Severity:** high
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.66

Test-specific ID: SNYK-DEBIAN10-DJVULIBRE-481572 **Severity:** high
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.67

Test-specific ID: SNYK-DEBIAN10-EXPAT-2329087 **Severity:** high
Identifiers: **Message**:Incorrect Calculation

Vulnerability 3.68
Test-specific ID: SNYK-DEBIAN10-EXPAT-2330888 **Severity:** high
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.69
Test-specific ID: SNYK-DEBIAN10-EXPAT-2331795 **Severity:** high
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.70
Test-specific ID: SNYK-DEBIAN10-EXPAT-2331796 **Severity:** high
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.71
Test-specific ID: SNYK-DEBIAN10-EXPAT-2331820 **Severity:** high
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.72
Test-specific ID: SNYK-DEBIAN10-EXPAT-2384929 **Severity:** high
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.73
Test-specific ID: SNYK-DEBIAN10-EXPAT-2406126 **Severity:** high
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.74
Test-specific ID: SNYK-DEBIAN10-EXPAT-3023032 **Severity:** high
Identifiers: **Message**:Use After Free

Vulnerability 3.75
Test-specific ID: SNYK-DEBIAN10-EXPAT-3061092 **Severity:** high
Identifiers: **Message**:Use After Free

Vulnerability 3.76
Test-specific ID: SNYK-DEBIAN10-FREETYPE-2774652 **Severity:** high
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.77
Test-specific ID: SNYK-DEBIAN10-FREETYPE-2774657 **Severity:** high
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.78
Test-specific ID: SNYK-DEBIAN10-FRIBIDI-2433113 **Severity:** high
Identifiers: **Message**:Stack-based Buffer Overflow

Vulnerability 3.79
Test-specific ID: SNYK-DEBIAN10-GCC8-347558 **Severity:** high
Identifiers: **Message**:Information Exposure

Vulnerability 3.80
Test-specific ID: SNYK-DEBIAN10-GIT-1083853 **Severity:** high
Identifiers: **Message**:Link Following

Vulnerability 3.81
Test-specific ID: SNYK-DEBIAN10-GIT-1577271 **Severity:** high
Identifiers: **Message**:CVE-2021-40330

Vulnerability 3.82
Test-specific ID: SNYK-DEBIAN10-GIT-2635966 **Severity:** high
Identifiers: **Message**:Uncontrolled Search Path Element

Vulnerability 3.83
Test-specific ID: SNYK-DEBIAN10-GIT-2949147 **Severity:** high
Identifiers: **Message**:Improper Ownership Management

Vulnerability 3.84
Test-specific ID: SNYK-DEBIAN10-GIT-3051708 **Severity:** high
Identifiers: **Message**:Heap-based Buffer Overflow

Vulnerability 3.85
Test-specific ID: SNYK-DEBIAN10-GIT-3319755 **Severity:** high
Identifiers: **Message**:Directory Traversal

Vulnerability 3.86
Test-specific ID: SNYK-DEBIAN10-GLIB20-1075023 **Severity:** high
Identifiers: **Message**:Incorrect Conversion between Numeric Types

Vulnerability 3.87
Test-specific ID: SNYK-DEBIAN10-GLIB20-1075027 **Severity:** high
Identifiers: **Message**:Incorrect Conversion between Numeric Types

Vulnerability 3.88
Test-specific ID: SNYK-DEBIAN10-GLIB20-5670985 **Severity:** high
Identifiers: **Message**:Resource Exhaustion

Vulnerability 3.89
Test-specific ID: SNYK-DEBIAN10-GLIBC-1065768 **Severity:** high
Identifiers: **Message**:Reachable Assertion

Vulnerability 3.90
Test-specific ID: SNYK-DEBIAN10-GLIBC-2340921 **Severity:** high
Identifiers: **Message**:Off-by-one Error

Vulnerability 3.91
Test-specific ID: SNYK-DEBIAN10-GLIBC-559488 **Severity:** high
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.92
Test-specific ID: SNYK-DEBIAN10-GLIBC-559493 **Severity:** high
Identifiers: **Message**:Use After Free

Vulnerability 3.93
Test-specific ID: SNYK-DEBIAN10-GLIBC-564233 **Severity:** high
Identifiers: **Message**:Integer Underflow

Vulnerability 3.94
Test-specific ID: SNYK-DEBIAN10-GMP-1920939 **Severity:** high
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.95
Test-specific ID: SNYK-DEBIAN10-GNUTLS28-2964217 **Severity:** high
Identifiers: **Message**:Double Free

Vulnerability 3.96

Test-specific ID: SNYK-DEBIAN10-GNUTLS28-3318300 **Severity:** high
Identifiers: **Message**:Information Exposure

Vulnerability 3.97

Test-specific ID: SNYK-DEBIAN10-GNUTLS28-609778 **Severity:** high
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.98

Test-specific ID: SNYK-DEBIAN10-GNUTLS28-6159414 **Severity:** high
Identifiers: **Message**:Information Exposure

Vulnerability 3.99

Test-specific ID: SNYK-DEBIAN10-GZIP-2444259 **Severity:** high
Identifiers: **Message**:Improper Input Validation

Vulnerability 3.100

Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-1042774 **Severity:** high
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.101

Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-1048022 **Severity:** high
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.102

Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-1049976 **Severity:** high
Identifiers: **Message**:XML Injection

Vulnerability 3.103
Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-1244105 **Severity:** high
Identifiers: **Message**:Divide By Zero

Vulnerability 3.104
Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-1246263 **Severity:** high
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.105
Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-1246512 **Severity:** high
Identifiers: **Message**:Information Exposure

Vulnerability 3.106
Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-2812516 **Severity:** high
Identifiers: **Message**:Buffer Overflow

Vulnerability 3.107
Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-2928986 **Severity:** high
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.108
Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-2928990 **Severity:** high
Identifiers: **Message**:Incorrect Type Conversion or Cast

Vulnerability 3.109
Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-2928992 **Severity:** high
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.110
Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-5850024 **Severity:** high
Identifiers: **Message**:Memory Leak

Vulnerability 3.111
Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-5858554 **Severity:** high
Identifiers: **Message**:Divide By Zero

Vulnerability 3.112
Test-specific ID: SNYK-DEBIAN10-KRB5-1320094 **Severity:** high
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.113
Test-specific ID: SNYK-DEBIAN10-KRB5-3120879 **Severity:** high
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.114
Test-specific ID: SNYK-DEBIAN10-LIBDE265-1585971 **Severity:** high
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.115
Test-specific ID: SNYK-DEBIAN10-LIBDE265-2359233 **Severity:** high
Identifiers: **Message**:Reachable Assertion

Vulnerability 3.116
Test-specific ID: SNYK-DEBIAN10-LIBDE265-3227415 **Severity:** high
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.117
Test-specific ID: SNYK-DEBIAN10-LIBDE265-3336915 **Severity:** high
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.118
Test-specific ID: SNYK-DEBIAN10-LIBDE265-3342947 **Severity:** high
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.119
Test-specific ID: SNYK-DEBIAN10-LIBDE265-3342950 **Severity:** high
Identifiers: **Message**:Buffer Overflow

Vulnerability 3.120
Test-specific ID: SNYK-DEBIAN10-LIBDE265-3361566 **Severity:** high
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.121
Test-specific ID: SNYK-DEBIAN10-LIBDE265-6070697 **Severity:** high
Identifiers: **Message**:Buffer Overflow

Vulnerability 3.122
Test-specific ID: SNYK-DEBIAN10-LIBDE265-6105345 **Severity:** high
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.123
Test-specific ID: SNYK-DEBIAN10-LIBDE265-6105350 **Severity:** high
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.124
Test-specific ID: SNYK-DEBIAN10-LIBDE265-6105363 **Severity:** high
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.125
Test-specific ID: SNYK-DEBIAN10-LIBSSH2-452460 **Severity:** high
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.126
Test-specific ID: SNYK-DEBIAN10-LIBSSH2-474372 **Severity:** high
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.127
Test-specific ID: SNYK-DEBIAN10-LIBSSH2-5861759 **Severity:** high
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.128
Test-specific ID: SNYK-DEBIAN10-LIBWEBP-1289557 **Severity:** high
Identifiers: **Message**:Improper Input Validation

Vulnerability 3.129
Test-specific ID: SNYK-DEBIAN10-LIBWEBP-5489178 **Severity:** high
Identifiers: **Message**:Double Free

Vulnerability 3.130
Test-specific ID: SNYK-DEBIAN10-LIBWEBP-5893093 **Severity:** high
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.131
Test-specific ID: SNYK-DEBIAN10-LIBX11-5710890 **Severity:** high
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.132
Test-specific ID: SNYK-DEBIAN10-LIBX11-5927157 **Severity:** high
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.133
Test-specific ID: SNYK-DEBIAN10-LIBXML2-1277346 **Severity:** high
Identifiers: **Message**:Use After Free

Vulnerability 3.134
Test-specific ID: SNYK-DEBIAN10-LIBXML2-1277349 **Severity:** high
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.135
Test-specific ID: SNYK-DEBIAN10-LIBXML2-1277350 **Severity:** high
Identifiers: **Message**:Use After Free

Vulnerability 3.136
Test-specific ID: SNYK-DEBIAN10-LIBXML2-2413976 **Severity:** high
Identifiers: **Message**:Use After Free

Vulnerability 3.137
Test-specific ID: SNYK-DEBIAN10-LIBXML2-3059798 **Severity:** high
Identifiers: **Message**:Double Free

Vulnerability 3.138
Test-specific ID: SNYK-DEBIAN10-LIBXML2-3059802 **Severity:** high
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.139
Test-specific ID: SNYK-DEBIAN10-LIBXSLT-2964221 **Severity:** high
Identifiers: **Message**:Use After Free

Vulnerability 3.140
Test-specific ID: SNYK-DEBIAN10-LIBXSLT-2964226 **Severity:** high
Identifiers: **Message**:Access of Resource Using Incompatible Type (’Type Confusion’)

Vulnerability 3.141
Test-specific ID: SNYK-DEBIAN10-MARIADB103-1087462 **Severity:** high
Identifiers: **Message**:OS Command Injection

Vulnerability 3.142
Test-specific ID: SNYK-DEBIAN10-MARIADB103-2389282 **Severity:** high
Identifiers: **Message**:Use After Free

Vulnerability 3.143
Test-specific ID: SNYK-DEBIAN10-MARIADB103-2396505 **Severity:** high
Identifiers: **Message**:Heap-based Buffer Overflow

Vulnerability 3.144
Test-specific ID: SNYK-DEBIAN10-MARIADB103-2396511 **Severity:** high
Identifiers: **Message**:Use of Externally-Controlled Format String

Vulnerability 3.145
Test-specific ID: SNYK-DEBIAN10-MARIADB103-2396512 **Severity:** high
Identifiers: **Message**:Use After Free

Vulnerability 3.146
Test-specific ID: SNYK-DEBIAN10-MARIADB103-2396513 **Severity:** high
Identifiers: **Message**:Stack-based Buffer Overflow

Vulnerability 3.147
Test-specific ID: SNYK-DEBIAN10-MARIADB103-2766279 **Severity:** high
Identifiers: **Message**:CVE-2022-27445

Vulnerability 3.148
Test-specific ID: SNYK-DEBIAN10-MARIADB103-2766287 **Severity:** high
Identifiers: **Message**:CVE-2022-27452

Vulnerability 3.149
Test-specific ID: SNYK-DEBIAN10-MARIADB103-2766300 **Severity:** high
Identifiers: **Message**:CVE-2022-27449

Vulnerability 3.150
Test-specific ID: SNYK-DEBIAN10-MARIADB103-2766301 **Severity:** high
Identifiers: **Message**:Reachable Assertion

Vulnerability 3.151
Test-specific ID: SNYK-DEBIAN10-MARIADB103-2766314 **Severity:** high
Identifiers: **Message**:Use After Free

Vulnerability 3.152
Test-specific ID: SNYK-DEBIAN10-MARIADB103-2766360 **Severity:** high
Identifiers: **Message**:SQL Injection

Vulnerability 3.153
Test-specific ID: SNYK-DEBIAN10-MARIADB103-2766361 **Severity:** high
Identifiers: **Message**:SQL Injection

Vulnerability 3.154
Test-specific ID: SNYK-DEBIAN10-MARIADB103-2766367 **Severity:** high
Identifiers: **Message**:SQL Injection

Vulnerability 3.155
Test-specific ID: SNYK-DEBIAN10-MARIADB103-2766369 **Severity:** high
Identifiers: **Message**:Use After Free

Vulnerability 3.156
Test-specific ID: SNYK-DEBIAN10-MARIADB103-2766377 **Severity:** high
Identifiers: **Message**:Use After Free

Vulnerability 3.157
Test-specific ID: SNYK-DEBIAN10-MARIADB103-2766378 **Severity:** high
Identifiers: **Message**:SQL Injection

Vulnerability 3.158
Test-specific ID: SNYK-DEBIAN10-MARIADB103-2766380 **Severity:** high
Identifiers: **Message**:Use After Free

Vulnerability 3.159
Test-specific ID: SNYK-DEBIAN10-MARIADB103-2766401 **Severity:** high
Identifiers: **Message**:Use After Free

Vulnerability 3.160
Test-specific ID: SNYK-DEBIAN10-MARIADB103-2766402 **Severity:** high
Identifiers: **Message**:SQL Injection

Vulnerability 3.161
Test-specific ID: SNYK-DEBIAN10-MARIADB103-2766403 **Severity:** high
Identifiers: **Message**:SQL Injection

Vulnerability 3.162
Test-specific ID: SNYK-DEBIAN10-MARIADB103-2766414 **Severity:** high
Identifiers: **Message**:Use After Free

Vulnerability 3.163
Test-specific ID: SNYK-DEBIAN10-MARIADB103-2766430 **Severity:** high
Identifiers: **Message**:Buffer Overflow

Vulnerability 3.164
Test-specific ID: SNYK-DEBIAN10-MARIADB103-2940554 **Severity:** high
Identifiers: **Message**:Use After Free

Vulnerability 3.165
Test-specific ID: SNYK-DEBIAN10-MARIADB103-2940558 **Severity:** high
Identifiers: **Message**:CVE-2022-32084

Vulnerability 3.166
Test-specific ID: SNYK-DEBIAN10-MARIADB103-2940560 **Severity:** high
Identifiers: **Message**:CVE-2022-32085

Vulnerability 3.167
Test-specific ID: SNYK-DEBIAN10-MARIADB103-2940568 **Severity:** high
Identifiers: **Message**:CVE-2022-32087

Vulnerability 3.168
Test-specific ID: SNYK-DEBIAN10-MARIADB103-2940573 **Severity:** high
Identifiers: **Message**:CVE-2022-32088

Vulnerability 3.169
Test-specific ID: SNYK-DEBIAN10-MARIADB103-2940586 **Severity:** high
Identifiers: **Message**:CVE-2022-32083

Vulnerability 3.170
Test-specific ID: SNYK-DEBIAN10-NCURSES-1655739 **Severity:** high
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.171
Test-specific ID: SNYK-DEBIAN10-NCURSES-2767192 **Severity:** high
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.172
Test-specific ID: SNYK-DEBIAN10-NCURSES-5421196 **Severity:** high
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.173
Test-specific ID: SNYK-DEBIAN10-NETTLE-1090205 **Severity:** high
Identifiers: **Message**:Use of a Broken or Risky Cryptographic Algorithm

Vulnerability 3.174
Test-specific ID: SNYK-DEBIAN10-NETTLE-1301269 **Severity:** high
Identifiers: **Message**:Improper Input Validation

Vulnerability 3.175
Test-specific ID: SNYK-DEBIAN10-NGHTTP2-1584531 **Severity:** high
Identifiers: **Message**:Improper Enforcement of Message or Data Structure

Vulnerability 3.176
Test-specific ID: SNYK-DEBIAN10-NGHTTP2-5953390 **Severity:** high
Identifiers: **Message**:Resource Exhaustion

Vulnerability 3.177
Test-specific ID: SNYK-DEBIAN10-OPENEXR-1318910 **Severity:** high
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.178
Test-specific ID: SNYK-DEBIAN10-OPENEXR-1320028 **Severity:** high
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.179
Test-specific ID: SNYK-DEBIAN10-OPENSSH-1660419 **Severity:** high
Identifiers: **Message**:Improper Privilege Management

Vulnerability 3.180
Test-specific ID: SNYK-DEBIAN10-OPENSSH-6139207 **Severity:** high
Identifiers: **Message**:CVE-2023-51767

Vulnerability 3.181
Test-specific ID: SNYK-DEBIAN10-OPENSSL-1569406 **Severity:** high
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.182
Test-specific ID: SNYK-DEBIAN10-OPENSSL-2426310 **Severity:** high
Identifiers: **Message**:Loop with Unreachable Exit Condition (’Infinite Loop’)

Vulnerability 3.183
Test-specific ID: SNYK-DEBIAN10-OPENSSL-3314585 **Severity:** high
Identifiers: **Message**:Access of Resource Using Incompatible Type (’Type Confusion’)

Vulnerability 3.184
Test-specific ID: SNYK-DEBIAN10-OPENSSL-3314606 **Severity:** high
Identifiers: **Message**:Use After Free

Vulnerability 3.185
Test-specific ID: SNYK-DEBIAN10-OPENSSL-3314607 **Severity:** high
Identifiers: **Message**:Double Free

Vulnerability 3.186
Test-specific ID: SNYK-DEBIAN10-OPENSSL-3368736 **Severity:** high
Identifiers: **Message**:Improper Certificate Validation

Vulnerability 3.187

Test-specific ID: SNYK-DEBIAN10-PCRE2-548863 **Severity:** high
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.188

Test-specific ID: SNYK-DEBIAN10-PIXMAN-3099046 **Severity:** high
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.189

Test-specific ID: SNYK-DEBIAN10-POSTGRESQL11-1292094 **Severity:** high
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.190

Test-specific ID: SNYK-DEBIAN10-POSTGRESQL11-1920111 **Severity:** high
Identifiers: **Message**:SQL Injection

Vulnerability 3.191

Test-specific ID: SNYK-DEBIAN10-POSTGRESQL11-2824083 **Severity:** high
Identifiers: **Message**:Incomplete Cleanup

Vulnerability 3.192

Test-specific ID: SNYK-DEBIAN10-POSTGRESQL11-2980115 **Severity:** high
Identifiers: **Message**:Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')

Vulnerability 3.193

Test-specific ID: SNYK-DEBIAN10-POSTGRESQL11-5519355 **Severity:** high
Identifiers: **Message**:CVE-2023-2454

Vulnerability 3.194
Test-specific ID: SNYK-DEBIAN10-POSTGRESQL11-5838230 **Severity:** high
Identifiers: **Message**:SQL Injection

Vulnerability 3.195
Test-specific ID: SNYK-DEBIAN10-POSTGRESQL11-6055646 **Severity:** high
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.196
Test-specific ID: SNYK-DEBIAN10-PYTHON27-2764959 **Severity:** high
Identifiers: **Message**:Arbitrary Command Injection

Vulnerability 3.197
Test-specific ID: SNYK-DEBIAN10-PYTHON27-5423193 **Severity:** high
Identifiers: **Message**:Improper Encoding or Escaping of Output

Vulnerability 3.198
Test-specific ID: SNYK-DEBIAN10-PYTHON27-5423201 **Severity:** high
Identifiers: **Message**:Arbitrary Code Injection

Vulnerability 3.199
Test-specific ID: SNYK-DEBIAN10-PYTHON27-5423202 **Severity:** high
Identifiers: **Message**:Algorithmic Complexity

Vulnerability 3.200
Test-specific ID: SNYK-DEBIAN10-PYTHON27-5423207 **Severity:** high
Identifiers: **Message**:Improper Input Validation

Vulnerability 3.201
Test-specific ID: SNYK-DEBIAN10-PYTHON27-5423210 **Severity:** high
Identifiers: **Message**:Resource Exhaustion

Vulnerability 3.202
Test-specific ID: SNYK-DEBIAN10-PYTHON27-584372 **Severity:** high
Identifiers: **Message**:Improper Input Validation

Vulnerability 3.203
Test-specific ID: SNYK-DEBIAN10-PYTHON27-5853784 **Severity:** high
Identifiers: **Message**:Use After Free

Vulnerability 3.204
Test-specific ID: SNYK-DEBIAN10-PYTHON37-1570178 **Severity:** high
Identifiers: **Message**:Resource Exhaustion

Vulnerability 3.205
Test-specific ID: SNYK-DEBIAN10-PYTHON37-2764966 **Severity:** high
Identifiers: **Message**:Arbitrary Command Injection

Vulnerability 3.206
Test-specific ID: SNYK-DEBIAN10-PYTHON37-3017604 **Severity:** high
Identifiers: **Message**:Incorrect Type Conversion or Cast

Vulnerability 3.207
Test-specific ID: SNYK-DEBIAN10-PYTHON37-3111114 **Severity:** high
Identifiers: **Message**:Algorithmic Complexity

Vulnerability 3.208
Test-specific ID: SNYK-DEBIAN10-PYTHON37-3325305 **Severity:** high
Identifiers: **Message**:Improper Input Validation

Vulnerability 3.209
Test-specific ID: SNYK-DEBIAN10-PYTHON37-5851338 **Severity:** high
Identifiers: **Message**:Use After Free

Vulnerability 3.210
Test-specific ID: SNYK-DEBIAN10-SQLITE3-3011631 **Severity:** high
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.211
Test-specific ID: SNYK-DEBIAN10-SUBVERSION-2635642 **Severity:** high
Identifiers: **Message**:Use After Free

Vulnerability 3.212
Test-specific ID: SNYK-DEBIAN10-SYSTEMD-3339153 **Severity:** high
Identifiers: **Message**:CVE-2023-26604

Vulnerability 3.213
Test-specific ID: SNYK-DEBIAN10-TIFF-2420604 **Severity:** high
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.214
Test-specific ID: SNYK-DEBIAN10-TIFF-3113870 **Severity:** high
Identifiers: **Message**:Numeric Errors

Vulnerability 3.215

Test-specific ID: SNYK-DEBIAN10-TIFF-5747604 **Severity:** high
Identifiers: **Message**:Buffer Overflow

Vulnerability 3.216

Test-specific ID: SNYK-DEBIAN10-UNBOUND-3028989 **Severity:** high
Identifiers: **Message**:Resource Exhaustion

Vulnerability 3.217

Test-specific ID: SNYK-DEBIAN10-XZUTILS-2444279 **Severity:** high
Identifiers: **Message**:Improper Input Validation

Vulnerability 3.218

Test-specific ID: SNYK-DEBIAN10-ZLIB-2433934 **Severity:** high
Identifiers: **Message**:Out-of-bounds Write

Medium:

Vulnerability 3.219

Test-specific ID: SNYK-DEBIAN10-APRUTIL-3261253 **Severity:** medium
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.220

Test-specific ID: SNYK-DEBIAN10-BLUEZ-1300772 **Severity:** medium
Identifiers: **Message**:Incorrect Authorization

Vulnerability 3.221

Test-specific ID: SNYK-DEBIAN10-BLUEZ-1300777 **Severity:** medium
Identifiers: **Message**:Improper Authentication

Vulnerability 3.222

Test-specific ID: SNYK-DEBIAN10-BLUEZ-1920809 **Severity:** medium
Identifiers: **Message**:Resource Exhaustion

Vulnerability 3.223

Test-specific ID: SNYK-DEBIAN10-BLUEZ-1926136 **Severity:** medium
Identifiers: **Message**:Insufficient Verification of Data Authenticity

Vulnerability 3.224

Test-specific ID: SNYK-DEBIAN10-BLUEZ-6112469 **Severity:** medium
Identifiers: **Message**:Improper Authentication

Vulnerability 3.225

Test-specific ID: SNYK-DEBIAN10-CURL-1585143 **Severity:** medium
Identifiers: **Message**:Insufficient Verification of Data Authenticity

Vulnerability 3.226

Test-specific ID: SNYK-DEBIAN10-CURL-2804161 **Severity:** medium
Identifiers: **Message**:Insufficiently Protected Credentials

Vulnerability 3.227

Test-specific ID: SNYK-DEBIAN10-CURL-2804168 **Severity:** medium
Identifiers: **Message**:Insufficiently Protected Credentials

Vulnerability 3.228

Test-specific ID: SNYK-DEBIAN10-CURL-2936224 **Severity:** medium
Identifiers: **Message**:Allocation of Resources Without Limits or Throttling

Vulnerability 3.229
Test-specific ID: SNYK-DEBIAN10-CURL-2936239 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.230
Test-specific ID: SNYK-DEBIAN10-CURL-3179185 **Severity:** medium
Identifiers: **Message**:Use After Free

Vulnerability 3.231
Test-specific ID: SNYK-DEBIAN10-CURL-3320497 **Severity:** medium
Identifiers: **Message**:Allocation of Resources Without Limits or Throttling

Vulnerability 3.232
Test-specific ID: SNYK-DEBIAN10-CURL-3366759 **Severity:** medium
Identifiers: **Message**:Improper Authentication

Vulnerability 3.233
Test-specific ID: SNYK-DEBIAN10-CURL-3366770 **Severity:** medium
Identifiers: **Message**:Improper Authentication

Vulnerability 3.234
Test-specific ID: SNYK-DEBIAN10-CURL-3366778 **Severity:** medium
Identifiers: **Message**:Improper Authentication

Vulnerability 3.235
Test-specific ID: SNYK-DEBIAN10-CURL-5561870 **Severity:** medium
Identifiers: **Message**:Improper Certificate Validation

Vulnerability 3.236
Test-specific ID: SNYK-DEBIAN10-CURL-6100971 **Severity:** medium
Identifiers: **Message**:CVE-2023-46218

Vulnerability 3.237
Test-specific ID: SNYK-DEBIAN10-DJVULIBRE-1315331 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.238
Test-specific ID: SNYK-DEBIAN10-DJVULIBRE-459736 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.239
Test-specific ID: SNYK-DEBIAN10-DJVULIBRE-459739 **Severity:** medium
Identifiers: **Message**:Uncontrolled Recursion

Vulnerability 3.240
Test-specific ID: SNYK-DEBIAN10-DJVULIBRE-459740 **Severity:** medium
Identifiers: **Message**:Loop with Unreachable Exit Condition (’Infinite Loop’)

Vulnerability 3.241
Test-specific ID: SNYK-DEBIAN10-DJVULIBRE-459743 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.242
Test-specific ID: SNYK-DEBIAN10-ELFUTILS-5862078 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.243
Test-specific ID: SNYK-DEBIAN10-EXPAT-2405942 **Severity:** medium
Identifiers: **Message**:Uncontrolled Recursion

Vulnerability 3.244
Test-specific ID: SNYK-DEBIAN10-FRIBIDI-2433111 **Severity:** medium
Identifiers: **Message**:Heap-based Buffer Overflow

Vulnerability 3.245
Test-specific ID: SNYK-DEBIAN10-FRIBIDI-2433119 **Severity:** medium
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.246
Test-specific ID: SNYK-DEBIAN10-GIT-3051728 **Severity:** medium
Identifiers: **Message**:Link Following

Vulnerability 3.247
Test-specific ID: SNYK-DEBIAN10-GIT-3319751 **Severity:** medium
Identifiers: **Message**:Link Following

Vulnerability 3.248
Test-specific ID: SNYK-DEBIAN10-GLIB20-1085371 **Severity:** medium
Identifiers: **Message**:Link Following

Vulnerability 3.249
Test-specific ID: SNYK-DEBIAN10-GLIB20-2993046 **Severity:** medium
Identifiers: **Message**:Information Exposure

Vulnerability 3.250

Test-specific ID: SNYK-DEBIAN10-GLIB20-5670991 **Severity:** medium
Identifiers: **Message**:Deserialization of Untrusted Data

Vulnerability 3.251

Test-specific ID: SNYK-DEBIAN10-GLIB20-5670993 **Severity:** medium
Identifiers: **Message**:Resource Exhaustion

Vulnerability 3.252

Test-specific ID: SNYK-DEBIAN10-GLIBC-1035462 **Severity:** medium
Identifiers: **Message**:Loop with Unreachable Exit Condition ('Infinite Loop')

Vulnerability 3.253

Test-specific ID: SNYK-DEBIAN10-GLIBC-1055403 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.254

Test-specific ID: SNYK-DEBIAN10-GLIBC-356371 **Severity:** medium
Identifiers: **Message**:Improper Input Validation

Vulnerability 3.255

Test-specific ID: SNYK-DEBIAN10-GLIBC-559181 **Severity:** medium
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.256

Test-specific ID: SNYK-DEBIAN10-GNUPG2-2939852 **Severity:** medium
Identifiers: **Message**:Arbitrary Code Injection

Vulnerability 3.257
Test-specific ID: SNYK-DEBIAN10-GNUTLS28-2419146 **Severity:** medium
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.258
Test-specific ID: SNYK-DEBIAN10-GNUTLS28-6062099 **Severity:** medium
Identifiers: **Message**:Information Exposure

Vulnerability 3.259
Test-specific ID: SNYK-DEBIAN10-ICU-1730331 **Severity:** medium
Identifiers: **Message**:Use After Free

Vulnerability 3.260
Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-1045661 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.261
Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-1045688 **Severity:** medium
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.262
Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-1045711 **Severity:** medium
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.263
Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-1045713 **Severity:** medium
Identifiers: **Message**:Divide By Zero

Vulnerability 3.264
Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-1045717 **Severity:** medium
Identifiers: **Message**:Divide By Zero

Vulnerability 3.265
Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-1045733 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.266
Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-1045745 **Severity:** medium
Identifiers: **Message**:Divide By Zero

Vulnerability 3.267
Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-1045786 **Severity:** medium
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.268
Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-1070303 **Severity:** medium
Identifiers: **Message**:Divide By Zero

Vulnerability 3.269
Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-1075502 **Severity:** medium
Identifiers: **Message**:Divide By Zero

Vulnerability 3.270
Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-1075507 **Severity:** medium
Identifiers: **Message**:Divide By Zero

Vulnerability 3.271

Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-1075510 **Severity:** medium
Identifiers: **Message**:Divide By Zero

Vulnerability 3.272

Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-1078457 **Severity:** medium
Identifiers: **Message**:Divide By Zero

Vulnerability 3.273

Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-1085783 **Severity:** medium
Identifiers: **Message**:Divide By Zero

Vulnerability 3.274

Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-2403734 **Severity:** medium
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.275

Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-3008101 **Severity:** medium
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.276

Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-3314438 **Severity:** medium
Identifiers: **Message**:Improper Resource Shutdown or Release

Vulnerability 3.277

Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-3314443 **Severity:** medium
Identifiers: **Message**:CVE-2022-44268

Vulnerability 3.278

Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-3358957 **Severity:** medium
Identifiers: **Message**:Improper Input Validation

Vulnerability 3.279

Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-5746985 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.280

Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-5788311 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.281

Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-5933303 **Severity:** medium
Identifiers: **Message**:Use After Free

Vulnerability 3.282

Test-specific ID: SNYK-DEBIAN10-KRB5-1568498 **Severity:** medium
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.283

Test-specific ID: SNYK-DEBIAN10-KRB5-5825658 **Severity:** medium
Identifiers: **Message**:Access of Uninitialized Pointer

Vulnerability 3.284

Test-specific ID: SNYK-DEBIAN10-LIBDE265-1585965 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.285

Test-specific ID: SNYK-DEBIAN10-LIBDE265-1585970 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.286

Test-specific ID: SNYK-DEBIAN10-LIBDE265-1585978 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.287

Test-specific ID: SNYK-DEBIAN10-LIBDE265-1585979 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.288

Test-specific ID: SNYK-DEBIAN10-LIBDE265-1585982 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.289

Test-specific ID: SNYK-DEBIAN10-LIBDE265-1585986 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.290

Test-specific ID: SNYK-DEBIAN10-LIBDE265-1585992 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.291

Test-specific ID: SNYK-DEBIAN10-LIBDE265-1585994 **Severity:** medium
Identifiers: **Message**:CVE-2020-21605

Vulnerability 3.292

Test-specific ID: SNYK-DEBIAN10-LIBDE265-1585999 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.293

Test-specific ID: SNYK-DEBIAN10-LIBDE265-1586001 **Severity:** medium
Identifiers: **Message**:Buffer Overflow

Vulnerability 3.294

Test-specific ID: SNYK-DEBIAN10-LIBDE265-1586006 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.295

Test-specific ID: SNYK-DEBIAN10-LIBDE265-2359231 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.296

Test-specific ID: SNYK-DEBIAN10-LIBDE265-2359232 **Severity:** medium
Identifiers: **Message**:Use After Free

Vulnerability 3.297

Test-specific ID: SNYK-DEBIAN10-LIBDE265-2359238 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.298

Test-specific ID: SNYK-DEBIAN10-LIBDE265-2359247 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.299

Test-specific ID: SNYK-DEBIAN10-LIBDE265-3098972 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.300

Test-specific ID: SNYK-DEBIAN10-LIBDE265-3098974 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.301

Test-specific ID: SNYK-DEBIAN10-LIBDE265-3098977 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.302

Test-specific ID: SNYK-DEBIAN10-LIBDE265-3098980 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.303

Test-specific ID: SNYK-DEBIAN10-LIBDE265-3098982 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.304

Test-specific ID: SNYK-DEBIAN10-LIBDE265-3098987 **Severity:** medium
Identifiers: **Message**:CVE-2022-43245

Vulnerability 3.305

Test-specific ID: SNYK-DEBIAN10-LIBDE265-3098989 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.306
Test-specific ID: SNYK-DEBIAN10-LIBDE265-3098992 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.307
Test-specific ID: SNYK-DEBIAN10-LIBDE265-3098998 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.308
Test-specific ID: SNYK-DEBIAN10-LIBDE265-3099004 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.309
Test-specific ID: SNYK-DEBIAN10-LIBDE265-3099014 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.310
Test-specific ID: SNYK-DEBIAN10-LIBDE265-3099016 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.311
Test-specific ID: SNYK-DEBIAN10-LIBDE265-3099017 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.312
Test-specific ID: SNYK-DEBIAN10-LIBDE265-3099023 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.313
Test-specific ID: SNYK-DEBIAN10-LIBDE265-3099024 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.314
Test-specific ID: SNYK-DEBIAN10-LIBDE265-3099025 **Severity:** medium
Identifiers: **Message**:CVE-2022-43238

Vulnerability 3.315
Test-specific ID: SNYK-DEBIAN10-LIBDE265-3336897 **Severity:** medium
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.316
Test-specific ID: SNYK-DEBIAN10-LIBDE265-3336906 **Severity:** medium
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.317
Test-specific ID: SNYK-DEBIAN10-LIBDE265-3336907 **Severity:** medium
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.318
Test-specific ID: SNYK-DEBIAN10-LIBDE265-3336910 **Severity:** medium
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.319
Test-specific ID: SNYK-DEBIAN10-LIBDE265-3336911 **Severity:** medium
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.320
Test-specific ID: SNYK-DEBIAN10-LIBDE265-3336914 **Severity:** medium
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.321
Test-specific ID: SNYK-DEBIAN10-LIBDE265-3336918 **Severity:** medium
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.322
Test-specific ID: SNYK-DEBIAN10-LIBDE265-3361569 **Severity:** medium
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.323
Test-specific ID: SNYK-DEBIAN10-LIBDE265-6062371 **Severity:** medium
Identifiers: **Message**:Buffer Overflow

Vulnerability 3.324
Test-specific ID: SNYK-DEBIAN10-LIBGCRYPT20-1582894 **Severity:** medium
Identifiers: **Message**:Use of a Broken or Risky Cryptographic Algorithm

Vulnerability 3.325
Test-specific ID: SNYK-DEBIAN10-LIBRSVG-543970 **Severity:** medium
Identifiers: **Message**:Resource Exhaustion

Vulnerability 3.326
Test-specific ID: SNYK-DEBIAN10-LIBX11-5927153 **Severity:** medium
Identifiers: **Message**:Loop with Unreachable Exit Condition (’Infinite Loop’)

Vulnerability 3.327

Test-specific ID: SNYK-DEBIAN10-LIBX11-5927158 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.328

Test-specific ID: SNYK-DEBIAN10-LIBXML2-1290152 **Severity:** medium
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.329

Test-specific ID: SNYK-DEBIAN10-LIBXML2-1293202 **Severity:** medium
Identifiers: **Message**:Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')

Vulnerability 3.330

Test-specific ID: SNYK-DEBIAN10-LIBXML2-2806809 **Severity:** medium
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.331

Test-specific ID: SNYK-DEBIAN10-LIBXML2-5423818 **Severity:** medium
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.332

Test-specific ID: SNYK-DEBIAN10-LIBXML2-5423823 **Severity:** medium
Identifiers: **Message**:Double Free

Vulnerability 3.333

Test-specific ID: SNYK-DEBIAN10-LIBXML2-609787 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.334
Test-specific ID: SNYK-DEBIAN10-MARIADB103-1291032 **Severity:** medium
Identifiers: **Message**:CVE-2021-2154

Vulnerability 3.335
Test-specific ID: SNYK-DEBIAN10-MARIADB103-1291033 **Severity:** medium
Identifiers: **Message**:CVE-2021-2166

Vulnerability 3.336
Test-specific ID: SNYK-DEBIAN10-MARIADB103-1537595 **Severity:** medium
Identifiers: **Message**:CVE-2021-2389

Vulnerability 3.337
Test-specific ID: SNYK-DEBIAN10-MARIADB103-1537596 **Severity:** medium
Identifiers: **Message**:CVE-2021-2372

Vulnerability 3.338
Test-specific ID: SNYK-DEBIAN10-MARIADB103-1924615 **Severity:** medium
Identifiers: **Message**:CVE-2021-35604

Vulnerability 3.339
Test-specific ID: SNYK-DEBIAN10-MARIADB103-2388602 **Severity:** medium
Identifiers: **Message**:CVE-2021-46657

Vulnerability 3.340
Test-specific ID: SNYK-DEBIAN10-MARIADB103-2388603 **Severity:** medium
Identifiers: **Message**:CVE-2021-46658

Vulnerability 3.341

Test-specific ID: SNYK-DEBIAN10-MARIADB103-2388612 **Severity:** medium
Identifiers: **Message**:CVE-2021-46659

Vulnerability 3.342

Test-specific ID: SNYK-DEBIAN10-MARIADB103-2389254 **Severity:** medium
Identifiers: **Message**:CVE-2021-46661

Vulnerability 3.343

Test-specific ID: SNYK-DEBIAN10-MARIADB103-2389274 **Severity:** medium
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.344

Test-specific ID: SNYK-DEBIAN10-MARIADB103-2389275 **Severity:** medium
Identifiers: **Message**:CVE-2021-46665

Vulnerability 3.345

Test-specific ID: SNYK-DEBIAN10-MARIADB103-2389283 **Severity:** medium
Identifiers: **Message**:CVE-2021-46662

Vulnerability 3.346

Test-specific ID: SNYK-DEBIAN10-MARIADB103-2389286 **Severity:** medium
Identifiers: **Message**:CVE-2021-46663

Vulnerability 3.347

Test-specific ID: SNYK-DEBIAN10-MARIADB103-2389287 **Severity:** medium
Identifiers: **Message**:Resource Exhaustion

Vulnerability 3.348
Test-specific ID: SNYK-DEBIAN10-MARIADB103-2389295 **Severity:** medium
Identifiers: **Message**:Reachable Assertion

Vulnerability 3.349
Test-specific ID: SNYK-DEBIAN10-MARIADB103-2389296 **Severity:** medium
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.350
Test-specific ID: SNYK-DEBIAN10-MARIADB103-2848382 **Severity:** medium
Identifiers: **Message**:Improper Locking

Vulnerability 3.351
Test-specific ID: SNYK-DEBIAN10-MARIADB103-2848387 **Severity:** medium
Identifiers: **Message**:Improper Locking

Vulnerability 3.352
Test-specific ID: SNYK-DEBIAN10-MARIADB103-2848390 **Severity:** medium
Identifiers: **Message**:Improper Locking

Vulnerability 3.353
Test-specific ID: SNYK-DEBIAN10-MARIADB103-2848391 **Severity:** medium
Identifiers: **Message**:Improper Locking

Vulnerability 3.354
Test-specific ID: SNYK-DEBIAN10-MARIADB103-2994373 **Severity:** medium
Identifiers: **Message**:Improper Locking

Vulnerability 3.355
Test-specific ID: SNYK-DEBIAN10-MARIADB103-3025437 **Severity:** medium
Identifiers: **Message**:CVE-2022-21427

Vulnerability 3.356
Test-specific ID: SNYK-DEBIAN10-MARIADB103-3325556 **Severity:** medium
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.357
Test-specific ID: SNYK-DEBIAN10-MARIADB103-6091683 **Severity:** medium
Identifiers: **Message**:CVE-2023-22084

Vulnerability 3.358
Test-specific ID: SNYK-DEBIAN10-NCURSES-5862705 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.359
Test-specific ID: SNYK-DEBIAN10-OPENEXR-1050304 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.360
Test-specific ID: SNYK-DEBIAN10-OPENEXR-1050309 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.361
Test-specific ID: SNYK-DEBIAN10-OPENEXR-1050313 **Severity:** medium
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.362
Test-specific ID: SNYK-DEBIAN10-OPENEXR-1089996 **Severity:** medium
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.363
Test-specific ID: SNYK-DEBIAN10-OPENEXR-1089998 **Severity:** medium
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.364
Test-specific ID: SNYK-DEBIAN10-OPENEXR-1090000 **Severity:** medium
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.365
Test-specific ID: SNYK-DEBIAN10-OPENEXR-1090002 **Severity:** medium
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.366
Test-specific ID: SNYK-DEBIAN10-OPENEXR-1090006 **Severity:** medium
Identifiers: **Message**:Resource Exhaustion

Vulnerability 3.367
Test-specific ID: SNYK-DEBIAN10-OPENEXR-1090124 **Severity:** medium
Identifiers: **Message**:Resource Exhaustion

Vulnerability 3.368
Test-specific ID: SNYK-DEBIAN10-OPENEXR-1090128 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.369
Test-specific ID: SNYK-DEBIAN10-OPENEXR-1300563 **Severity:** medium
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.370
Test-specific ID: SNYK-DEBIAN10-OPENEXR-1300566 **Severity:** medium
Identifiers: **Message**:Integer Underflow

Vulnerability 3.371
Test-specific ID: SNYK-DEBIAN10-OPENEXR-1304910 **Severity:** medium
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.372
Test-specific ID: SNYK-DEBIAN10-OPENEXR-1310952 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.373
Test-specific ID: SNYK-DEBIAN10-OPENEXR-1318903 **Severity:** medium
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.374
Test-specific ID: SNYK-DEBIAN10-OPENEXR-1318904 **Severity:** medium
Identifiers: **Message**:CVE-2021-20302

Vulnerability 3.375
Test-specific ID: SNYK-DEBIAN10-OPENEXR-1318913 **Severity:** medium
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.376

Test-specific ID: SNYK-DEBIAN10-OPENEXR-1913909 **Severity:** medium
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.377

Test-specific ID: SNYK-DEBIAN10-OPENEXR-1913916 **Severity:** medium
Identifiers: **Message**:Divide By Zero

Vulnerability 3.378

Test-specific ID: SNYK-DEBIAN10-OPENEXR-2329540 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.379

Test-specific ID: SNYK-DEBIAN10-OPENSSH-6130524 **Severity:** medium
Identifiers: **Message**:OS Command Injection

Vulnerability 3.380

Test-specific ID: SNYK-DEBIAN10-OPENSSH-6130526 **Severity:** medium
Identifiers: **Message**:Improper Validation of Integrity Check Value

Vulnerability 3.381

Test-specific ID: SNYK-DEBIAN10-OPENSSL-2388381 **Severity:** medium
Identifiers: **Message**:CVE-2021-4160

Vulnerability 3.382

Test-specific ID: SNYK-DEBIAN10-OPENSSL-2941248 **Severity:** medium
Identifiers: **Message**:Use of a Broken or Risky Cryptographic Algorithm

Vulnerability 3.383

Test-specific ID: SNYK-DEBIAN10-OPENSSL-3314590 **Severity:** medium
Identifiers: **Message**:Information Exposure

Vulnerability 3.384

Test-specific ID: SNYK-DEBIAN10-OPENSSL-5291770 **Severity:** medium
Identifiers: **Message**:Improper Certificate Validation

Vulnerability 3.385

Test-specific ID: SNYK-DEBIAN10-OPENSSL-5291775 **Severity:** medium
Identifiers: **Message**:Improper Certificate Validation

Vulnerability 3.386

Test-specific ID: SNYK-DEBIAN10-OPENSSL-5661563 **Severity:** medium
Identifiers: **Message**:Allocation of Resources Without Limits or Throttling

Vulnerability 3.387

Test-specific ID: SNYK-DEBIAN10-OPENSSL-5788323 **Severity:** medium
Identifiers: **Message**:Inefficient Regular Expression Complexity

Vulnerability 3.388

Test-specific ID: SNYK-DEBIAN10-OPENSSL-5812635 **Severity:** medium
Identifiers: **Message**:Excessive Iteration

Vulnerability 3.389

Test-specific ID: SNYK-DEBIAN10-POSTGRESQL11-1292093 **Severity:** medium
Identifiers: **Message**:CVE-2021-32029

Vulnerability 3.390

Test-specific ID: SNYK-DEBIAN10-POSTGRESQL11-1292095 **Severity:** medium
Identifiers: **Message**:Information Exposure

Vulnerability 3.391

Test-specific ID: SNYK-DEBIAN10-POSTGRESQL11-1540905 **Severity:** medium
Identifiers: **Message**:Information Exposure

Vulnerability 3.392

Test-specific ID: SNYK-DEBIAN10-POSTGRESQL11-1920112 **Severity:** medium
Identifiers: **Message**:Insufficiently Protected Credentials

Vulnerability 3.393

Test-specific ID: SNYK-DEBIAN10-POSTGRESQL11-5519356 **Severity:** medium
Identifiers: **Message**:CVE-2023-2455

Vulnerability 3.394

Test-specific ID: SNYK-DEBIAN10-POSTGRESQL11-6055645 **Severity:** medium
Identifiers: **Message**:CVE-2023-5868

Vulnerability 3.395

Test-specific ID: SNYK-DEBIAN10-POSTGRESQL11-6055657 **Severity:** medium
Identifiers: **Message**:CVE-2023-5870

Vulnerability 3.396

Test-specific ID: SNYK-DEBIAN10-PYTHON27-1085863 **Severity:** medium
Identifiers: **Message**:HTTP Request Smuggling

Vulnerability 3.397

Test-specific ID: SNYK-DEBIAN10-PYTHON27-2329040 **Severity:** medium
Identifiers: **Message**:Unchecked Return Value

Vulnerability 3.398

Test-specific ID: SNYK-DEBIAN10-PYTHON27-5423192 **Severity:** medium
Identifiers: **Message**:Resource Exhaustion

Vulnerability 3.399

Test-specific ID: SNYK-DEBIAN10-PYTHON27-543815 **Severity:** medium
Identifiers: **Message**:Resource Exhaustion

Vulnerability 3.400

Test-specific ID: SNYK-DEBIAN10-PYTHON27-5853778 **Severity:** medium
Identifiers: **Message**:Race Condition

Vulnerability 3.401

Test-specific ID: SNYK-DEBIAN10-PYTHON27-5861800 **Severity:** medium
Identifiers: **Message**:CVE-2023-40217

Vulnerability 3.402

Test-specific ID: SNYK-DEBIAN10-PYTHON37-1075120 **Severity:** medium
Identifiers: **Message**:HTTP Request Smuggling

Vulnerability 3.403

Test-specific ID: SNYK-DEBIAN10-PYTHON37-1085111 **Severity:** medium
Identifiers: **Message**:Information Exposure

Vulnerability 3.404

Test-specific ID: SNYK-DEBIAN10-PYTHON37-1579740 **Severity:** medium
Identifiers: **Message**:Resource Exhaustion

Vulnerability 3.405

Test-specific ID: SNYK-DEBIAN10-PYTHON37-2329041 **Severity:** medium
Identifiers: **Message**:Unchecked Return Value

Vulnerability 3.406

Test-specific ID: SNYK-DEBIAN10-PYTHON37-5851337 **Severity:** medium
Identifiers: **Message**:Resource Exhaustion

Vulnerability 3.407

Test-specific ID: SNYK-DEBIAN10-PYTHON37-5851354 **Severity:** medium
Identifiers: **Message**:Race Condition

Vulnerability 3.408

Test-specific ID: SNYK-DEBIAN10-PYTHON37-5861798 **Severity:** medium
Identifiers: **Message**:CVE-2023-40217

Vulnerability 3.409

Test-specific ID: SNYK-DEBIAN10-SUBVERSION-2635650 **Severity:** medium
Identifiers: **Message**:Information Exposure

Vulnerability 3.410

Test-specific ID: SNYK-DEBIAN10-SYSTEMD-1320245 **Severity:** medium
Identifiers: **Message**:Allocation of Resources Without Limits or Throttling

Vulnerability 3.411
Test-specific ID: SNYK-DEBIAN10-SYSTEMD-3111121 **Severity:** medium
Identifiers: **Message**:Off-by-one Error

Vulnerability 3.412
Test-specific ID: SNYK-DEBIAN10-SYSTEMD-3177744 **Severity:** medium
Identifiers: **Message**:CVE-2022-4415

Vulnerability 3.413
Test-specific ID: SNYK-DEBIAN10-TIFF-1584014 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.414
Test-specific ID: SNYK-DEBIAN10-TIFF-2331934 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.415
Test-specific ID: SNYK-DEBIAN10-TIFF-2399968 **Severity:** medium
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.416
Test-specific ID: SNYK-DEBIAN10-TIFF-2399971 **Severity:** medium
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.417
Test-specific ID: SNYK-DEBIAN10-TIFF-2419112 **Severity:** medium
Identifiers: **Message**:Reachable Assertion

Vulnerability 3.418

Test-specific ID: SNYK-DEBIAN10-TIFF-2421377 **Severity:** medium
Identifiers: **Message**:Unchecked Return Value

Vulnerability 3.419

Test-specific ID: SNYK-DEBIAN10-TIFF-2421382 **Severity:** medium
Identifiers: **Message**:Divide By Zero

Vulnerability 3.420

Test-specific ID: SNYK-DEBIAN10-TIFF-2421383 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.421

Test-specific ID: SNYK-DEBIAN10-TIFF-2421394 **Severity:** medium
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.422

Test-specific ID: SNYK-DEBIAN10-TIFF-2774163 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.423

Test-specific ID: SNYK-DEBIAN10-TIFF-2774168 **Severity:** medium
Identifiers: **Message**:Stack-based Buffer Overflow

Vulnerability 3.424

Test-specific ID: SNYK-DEBIAN10-TIFF-2938515 **Severity:** medium
Identifiers: **Message**:Divide By Zero

Vulnerability 3.425

Test-specific ID: SNYK-DEBIAN10-TIFF-2938517 **Severity:** medium
Identifiers: **Message**:Divide By Zero

Vulnerability 3.426

Test-specific ID: SNYK-DEBIAN10-TIFF-2938524 **Severity:** medium
Identifiers: **Message**:Divide By Zero

Vulnerability 3.427

Test-specific ID: SNYK-DEBIAN10-TIFF-2964238 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.428

Test-specific ID: SNYK-DEBIAN10-TIFF-2987008 **Severity:** medium
Identifiers: **Message**:Integer Underflow

Vulnerability 3.429

Test-specific ID: SNYK-DEBIAN10-TIFF-2987016 **Severity:** medium
Identifiers: **Message**:Improper Validation of Specified Quantity in Input

Vulnerability 3.430

Test-specific ID: SNYK-DEBIAN10-TIFF-2987018 **Severity:** medium
Identifiers: **Message**:Integer Underflow

Vulnerability 3.431

Test-specific ID: SNYK-DEBIAN10-TIFF-3058770 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.432
Test-specific ID: SNYK-DEBIAN10-TIFF-3058773 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.433
Test-specific ID: SNYK-DEBIAN10-TIFF-3058776 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.434
Test-specific ID: SNYK-DEBIAN10-TIFF-3058781 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.435
Test-specific ID: SNYK-DEBIAN10-TIFF-3058788 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.436
Test-specific ID: SNYK-DEBIAN10-TIFF-3058793 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.437
Test-specific ID: SNYK-DEBIAN10-TIFF-3244451 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.438
Test-specific ID: SNYK-DEBIAN10-TIFF-3319792 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.439

Test-specific ID: SNYK-DEBIAN10-TIFF-3319793 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.440

Test-specific ID: SNYK-DEBIAN10-TIFF-3319794 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.441

Test-specific ID: SNYK-DEBIAN10-TIFF-3319797 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.442

Test-specific ID: SNYK-DEBIAN10-TIFF-3319799 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.443

Test-specific ID: SNYK-DEBIAN10-TIFF-3319802 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.444

Test-specific ID: SNYK-DEBIAN10-TIFF-3319807 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.445

Test-specific ID: SNYK-DEBIAN10-TIFF-3319809 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.446

Test-specific ID: SNYK-DEBIAN10-TIFF-3319815 **Severity:** medium
Identifiers: **Message**:Use After Free

Vulnerability 3.447

Test-specific ID: SNYK-DEBIAN10-TIFF-3319819 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.448

Test-specific ID: SNYK-DEBIAN10-TIFF-3339159 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.449

Test-specific ID: SNYK-DEBIAN10-TIFF-5425899 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.450

Test-specific ID: SNYK-DEBIAN10-TIFF-5518069 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.451

Test-specific ID: SNYK-DEBIAN10-TIFF-5724638 **Severity:** medium
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.452

Test-specific ID: SNYK-DEBIAN10-TIFF-5747605 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.453
Test-specific ID: SNYK-DEBIAN10-TIFF-5747609 **Severity:** medium
Identifiers: **Message**:Buffer Overflow

Vulnerability 3.454
Test-specific ID: SNYK-DEBIAN10-TIFF-5749341 **Severity:** medium
Identifiers: **Message**:Buffer Overflow

Vulnerability 3.455
Test-specific ID: SNYK-DEBIAN10-TIFF-5750146 **Severity:** medium
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.456
Test-specific ID: SNYK-DEBIAN10-TIFF-5767898 **Severity:** medium
Identifiers: **Message**:Buffer Overflow

Vulnerability 3.457
Test-specific ID: SNYK-DEBIAN10-TIFF-5773191 **Severity:** medium
Identifiers: **Message**:Buffer Overflow

Vulnerability 3.458
Test-specific ID: SNYK-DEBIAN10-TIFF-5862862 **Severity:** medium
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.459
Test-specific ID: SNYK-DEBIAN10-TIFF-5862867 **Severity:** medium
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.460
Test-specific ID: SNYK-DEBIAN10-UNBOUND-1045777 **Severity:** medium
Identifiers: **Message**:Link Following

Vulnerability 3.461
Test-specific ID: SNYK-DEBIAN10-UNBOUND-2964916 **Severity:** medium
Identifiers: **Message**:Insufficient Session Expiration

Vulnerability 3.462
Test-specific ID: SNYK-DEBIAN10-UNBOUND-2964919 **Severity:** medium
Identifiers: **Message**:Insufficient Session Expiration

Vulnerability 3.463
Test-specific ID: SNYK-DEBIAN10-UNZIP-2396446 **Severity:** medium
Identifiers: **Message**:CVE-2022-0530

Vulnerability 3.464
Test-specific ID: SNYK-DEBIAN10-UNZIP-2396450 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Low:

Vulnerability 3.465
Test-specific ID: SNYK-DEBIAN10-APT-407502 **Severity:** low
Identifiers: **Message**:Improper Verification of Cryptographic Signature

Vulnerability 3.466
Test-specific ID: SNYK-DEBIAN10-BASH-536280 **Severity:** low
Identifiers: **Message**:Improper Check for Dropped Privileges

Vulnerability 3.467

Test-specific ID: SNYK-DEBIAN10-BINUTILS-1050281 **Severity:** low
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.468

Test-specific ID: SNYK-DEBIAN10-BINUTILS-1050286 **Severity:** low
Identifiers: **Message**:Double Free

Vulnerability 3.469

Test-specific ID: SNYK-DEBIAN10-BINUTILS-1050291 **Severity:** low
Identifiers: **Message**:Use After Free

Vulnerability 3.470

Test-specific ID: SNYK-DEBIAN10-BINUTILS-1050295 **Severity:** low
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.471

Test-specific ID: SNYK-DEBIAN10-BINUTILS-1050299 **Severity:** low
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.472

Test-specific ID: SNYK-DEBIAN10-BINUTILS-1054598 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.473

Test-specific ID: SNYK-DEBIAN10-BINUTILS-1055017 **Severity:** low
Identifiers: **Message**:Improper Input Validation

Vulnerability 3.474

Test-specific ID: SNYK-DEBIAN10-BINUTILS-1055021 **Severity:** low
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.475

Test-specific ID: SNYK-DEBIAN10-BINUTILS-1055024 **Severity:** low
Identifiers: **Message**:Use of Uninitialized Resource

Vulnerability 3.476

Test-specific ID: SNYK-DEBIAN10-BINUTILS-1055152 **Severity:** low
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.477

Test-specific ID: SNYK-DEBIAN10-BINUTILS-1055156 **Severity:** low
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.478

Test-specific ID: SNYK-DEBIAN10-BINUTILS-1065550 **Severity:** low
Identifiers: **Message**:Link Following

Vulnerability 3.479

Test-specific ID: SNYK-DEBIAN10-BINUTILS-1086497 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.480

Test-specific ID: SNYK-DEBIAN10-BINUTILS-1089439 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.481
Test-specific ID: SNYK-DEBIAN10-BINUTILS-1292159 **Severity:** low
Identifiers: **Message**:Uncontrolled Recursion

Vulnerability 3.482
Test-specific ID: SNYK-DEBIAN10-BINUTILS-1296882 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.483
Test-specific ID: SNYK-DEBIAN10-BINUTILS-2321368 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.484
Test-specific ID: SNYK-DEBIAN10-BINUTILS-2341554 **Severity:** low
Identifiers: **Message**:Uncontrolled Recursion

Vulnerability 3.485
Test-specific ID: SNYK-DEBIAN10-BINUTILS-2993561 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.486
Test-specific ID: SNYK-DEBIAN10-BINUTILS-3041901 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.487
Test-specific ID: SNYK-DEBIAN10-BINUTILS-3172911 **Severity:** low
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.488
Test-specific ID: SNYK-DEBIAN10-BINUTILS-337986 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.489
Test-specific ID: SNYK-DEBIAN10-BINUTILS-337990 **Severity:** low
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.490
Test-specific ID: SNYK-DEBIAN10-BINUTILS-337992 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.491
Test-specific ID: SNYK-DEBIAN10-BINUTILS-337999 **Severity:** low
Identifiers: **Message**:Allocation of Resources Without Limits or Throttling

Vulnerability 3.492
Test-specific ID: SNYK-DEBIAN10-BINUTILS-338007 **Severity:** low
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.493
Test-specific ID: SNYK-DEBIAN10-BINUTILS-338012 **Severity:** low
Identifiers: **Message**:Uncontrolled Recursion

Vulnerability 3.494
Test-specific ID: SNYK-DEBIAN10-BINUTILS-403696 **Severity:** low
Identifiers: **Message**:Allocation of Resources Without Limits or Throttling

Vulnerability 3.495
Test-specific ID: SNYK-DEBIAN10-BINUTILS-403777 **Severity:** low
Identifiers: **Message**:Uncontrolled Recursion

Vulnerability 3.496
Test-specific ID: SNYK-DEBIAN10-BINUTILS-403817 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.497
Test-specific ID: SNYK-DEBIAN10-BINUTILS-403841 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.498
Test-specific ID: SNYK-DEBIAN10-BINUTILS-403861 **Severity:** low
Identifiers: **Message**:Loop with Unreachable Exit Condition ('Infinite Loop')

Vulnerability 3.499
Test-specific ID: SNYK-DEBIAN10-BINUTILS-403865 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.500
Test-specific ID: SNYK-DEBIAN10-BINUTILS-403873 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.501
Test-specific ID: SNYK-DEBIAN10-BINUTILS-403909 **Severity:** low
Identifiers: **Message**:Use After Free

Vulnerability 3.502
Test-specific ID: SNYK-DEBIAN10-BINUTILS-403933 **Severity:** low
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.503
Test-specific ID: SNYK-DEBIAN10-BINUTILS-403941 **Severity:** low
Identifiers: **Message**:Resource Exhaustion

Vulnerability 3.504
Test-specific ID: SNYK-DEBIAN10-BINUTILS-403945 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.505
Test-specific ID: SNYK-DEBIAN10-BINUTILS-403961 **Severity:** low
Identifiers: **Message**:Uncontrolled Recursion

Vulnerability 3.506
Test-specific ID: SNYK-DEBIAN10-BINUTILS-403977 **Severity:** low
Identifiers: **Message**:CVE-2018-12698

Vulnerability 3.507
Test-specific ID: SNYK-DEBIAN10-BINUTILS-403985 **Severity:** low
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.508
Test-specific ID: SNYK-DEBIAN10-BINUTILS-404005 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.509
Test-specific ID: SNYK-DEBIAN10-BINUTILS-404033 **Severity:** low
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.510
Test-specific ID: SNYK-DEBIAN10-BINUTILS-404041 **Severity:** low
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.511
Test-specific ID: SNYK-DEBIAN10-BINUTILS-404045 **Severity:** low
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.512
Test-specific ID: SNYK-DEBIAN10-BINUTILS-404049 **Severity:** low
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.513
Test-specific ID: SNYK-DEBIAN10-BINUTILS-404130 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.514
Test-specific ID: SNYK-DEBIAN10-BINUTILS-404138 **Severity:** low
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.515
Test-specific ID: SNYK-DEBIAN10-BINUTILS-404150 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.516
Test-specific ID: SNYK-DEBIAN10-BINUTILS-404190 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.517
Test-specific ID: SNYK-DEBIAN10-BINUTILS-404194 **Severity:** low
Identifiers: **Message**:Uncontrolled Recursion

Vulnerability 3.518
Test-specific ID: SNYK-DEBIAN10-BINUTILS-404206 **Severity:** low
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.519
Test-specific ID: SNYK-DEBIAN10-BINUTILS-404210 **Severity:** low
Identifiers: **Message**:Missing Release of Resource after Effective Lifetime

Vulnerability 3.520
Test-specific ID: SNYK-DEBIAN10-BINUTILS-404214 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.521
Test-specific ID: SNYK-DEBIAN10-BINUTILS-404222 **Severity:** low
Identifiers: **Message**:Allocation of Resources Without Limits or Throttling

Vulnerability 3.522
Test-specific ID: SNYK-DEBIAN10-BINUTILS-404270 **Severity:** low
Identifiers: **Message**:Loop with Unreachable Exit Condition (’Infinite Loop’)

Vulnerability 3.523

Test-specific ID: SNYK-DEBIAN10-BINUTILS-451156 **Severity:** low
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.524

Test-specific ID: SNYK-DEBIAN10-BINUTILS-455443 **Severity:** low
Identifiers: **Message**:Improper Input Validation

Vulnerability 3.525

Test-specific ID: SNYK-DEBIAN10-BINUTILS-455454 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.526

Test-specific ID: SNYK-DEBIAN10-BINUTILS-456012 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.527

Test-specific ID: SNYK-DEBIAN10-BINUTILS-456777 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.528

Test-specific ID: SNYK-DEBIAN10-BINUTILS-472909 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.529

Test-specific ID: SNYK-DEBIAN10-BINUTILS-472913 **Severity:** low
Identifiers: **Message**:Uncontrolled Recursion

Vulnerability 3.530

Test-specific ID: SNYK-DEBIAN10-BINUTILS-5416280 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.531

Test-specific ID: SNYK-DEBIAN10-BINUTILS-5422225 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.532

Test-specific ID: SNYK-DEBIAN10-BINUTILS-5803141 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.533

Test-specific ID: SNYK-DEBIAN10-BINUTILS-5853675 **Severity:** low
Identifiers: **Message**:CVE-2022-47695

Vulnerability 3.534

Test-specific ID: SNYK-DEBIAN10-BINUTILS-5853676 **Severity:** low
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.535

Test-specific ID: SNYK-DEBIAN10-BINUTILS-5853678 **Severity:** low
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.536

Test-specific ID: SNYK-DEBIAN10-BINUTILS-5853687 **Severity:** low
Identifiers: **Message**:Reachable Assertion

Vulnerability 3.537

Test-specific ID: SNYK-DEBIAN10-BINUTILS-5853689 **Severity:** low
Identifiers: **Message**:Memory Leak

Vulnerability 3.538

Test-specific ID: SNYK-DEBIAN10-BINUTILS-5853690 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.539

Test-specific ID: SNYK-DEBIAN10-BINUTILS-5853703 **Severity:** low
Identifiers: **Message**:Memory Leak

Vulnerability 3.540

Test-specific ID: SNYK-DEBIAN10-BINUTILS-5853707 **Severity:** low
Identifiers: **Message**:Memory Leak

Vulnerability 3.541

Test-specific ID: SNYK-DEBIAN10-BINUTILS-5853716 **Severity:** low
Identifiers: **Message**:Memory Leak

Vulnerability 3.542

Test-specific ID: SNYK-DEBIAN10-BINUTILS-5853719 **Severity:** low
Identifiers: **Message**:Allocation of Resources Without Limits or Throttling

Vulnerability 3.543

Test-specific ID: SNYK-DEBIAN10-BINUTILS-5853722 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.544

Test-specific ID: SNYK-DEBIAN10-BINUTILS-5853728 **Severity:** low
Identifiers: **Message**:Memory Leak

Vulnerability 3.545

Test-specific ID: SNYK-DEBIAN10-BINUTILS-5853731 **Severity:** low
Identifiers: **Message**:CVE-2022-47696

Vulnerability 3.546

Test-specific ID: SNYK-DEBIAN10-BINUTILS-5853733 **Severity:** low
Identifiers: **Message**:Resource Exhaustion

Vulnerability 3.547

Test-specific ID: SNYK-DEBIAN10-BINUTILS-5858435 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.548

Test-specific ID: SNYK-DEBIAN10-BINUTILS-5858440 **Severity:** low
Identifiers: **Message**:Improper Initialization

Vulnerability 3.549

Test-specific ID: SNYK-DEBIAN10-BINUTILS-5861707 **Severity:** low
Identifiers: **Message**:Memory Leak

Vulnerability 3.550

Test-specific ID: SNYK-DEBIAN10-BINUTILS-5862061 **Severity:** low
Identifiers: **Message**:Memory Leak

Vulnerability 3.551
Test-specific ID: SNYK-DEBIAN10-BINUTILS-5862064 **Severity:** low
Identifiers: **Message**:CVE-2020-19726

Vulnerability 3.552
Test-specific ID: SNYK-DEBIAN10-BINUTILS-5903058 **Severity:** low
Identifiers: **Message**:Use of Uninitialized Resource

Vulnerability 3.553
Test-specific ID: SNYK-DEBIAN10-BINUTILS-5903059 **Severity:** low
Identifiers: **Message**:Use of Uninitialized Resource

Vulnerability 3.554
Test-specific ID: SNYK-DEBIAN10-BINUTILS-5903063 **Severity:** low
Identifiers: **Message**:Use of Uninitialized Resource

Vulnerability 3.555
Test-specific ID: SNYK-DEBIAN10-BINUTILS-5903066 **Severity:** low
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.556
Test-specific ID: SNYK-DEBIAN10-BLUEZ-385898 **Severity:** low
Identifiers: **Message**:Incorrect Authorization

Vulnerability 3.557
Test-specific ID: SNYK-DEBIAN10-BLUEZ-385910 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.558
Test-specific ID: SNYK-DEBIAN10-BLUEZ-385918 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.559
Test-specific ID: SNYK-DEBIAN10-BLUEZ-385926 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.560
Test-specific ID: SNYK-DEBIAN10-BLUEZ-385934 **Severity:** low
Identifiers: **Message**:Use After Free

Vulnerability 3.561
Test-specific ID: SNYK-DEBIAN10-BLUEZ-385942 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.562
Test-specific ID: SNYK-DEBIAN10-BLUEZ-385950 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.563
Test-specific ID: SNYK-DEBIAN10-BLUEZ-385958 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.564
Test-specific ID: SNYK-DEBIAN10-BLUEZ-385977 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.565
Test-specific ID: SNYK-DEBIAN10-BLUEZ-385991 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.566
Test-specific ID: SNYK-DEBIAN10-BLUEZ-385999 **Severity:** low
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.567
Test-specific ID: SNYK-DEBIAN10-CAIRO-344862 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.568
Test-specific ID: SNYK-DEBIAN10-CAIRO-344881 **Severity:** low
Identifiers: **Message**:Reachable Assertion

Vulnerability 3.569
Test-specific ID: SNYK-DEBIAN10-CAIRO-344889 **Severity:** low
Identifiers: **Message**:Loop with Unreachable Exit Condition (’Infinite Loop’)

Vulnerability 3.570
Test-specific ID: SNYK-DEBIAN10-CAIRO-344897 **Severity:** low
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.571
Test-specific ID: SNYK-DEBIAN10-COREUTILS-317465 **Severity:** low
Identifiers: **Message**:Improper Input Validation

Vulnerability 3.572
Test-specific ID: SNYK-DEBIAN10-COREUTILS-317494 **Severity:** low
Identifiers: **Message**:Race Condition

Vulnerability 3.573
Test-specific ID: SNYK-DEBIAN10-CURL-1296892 **Severity:** low
Identifiers: **Message**:Missing Initialization of Resource

Vulnerability 3.574
Test-specific ID: SNYK-DEBIAN10-CURL-1322655 **Severity:** low
Identifiers: **Message**:Improper Validation of Integrity Check Value

Vulnerability 3.575
Test-specific ID: SNYK-DEBIAN10-CURL-1322664 **Severity:** low
Identifiers: **Message**:Use of Incorrectly-Resolved Name or Reference

Vulnerability 3.576
Test-specific ID: SNYK-DEBIAN10-CURL-1322666 **Severity:** low
Identifiers: **Message**:Insufficiently Protected Credentials

Vulnerability 3.577
Test-specific ID: SNYK-DEBIAN10-CURL-3012387 **Severity:** low
Identifiers: **Message**:CVE-2022-35252

Vulnerability 3.578
Test-specific ID: SNYK-DEBIAN10-CURL-3366768 **Severity:** low
Identifiers: **Message**:Directory Traversal

Vulnerability 3.579
Test-specific ID: SNYK-DEBIAN10-CURL-5561874 **Severity:** low
Identifiers: **Message**:CVE-2023-28322

Vulnerability 3.580
Test-specific ID: SNYK-DEBIAN10-CURL-5561878 **Severity:** low
Identifiers: **Message**:Race Condition

Vulnerability 3.581
Test-specific ID: SNYK-DEBIAN10-CURL-5850004 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.582
Test-specific ID: SNYK-DEBIAN10-CURL-5955039 **Severity:** low
Identifiers: **Message**:CVE-2023-38546

Vulnerability 3.583
Test-specific ID: SNYK-DEBIAN10-DJVULIBRE-5858449 **Severity:** low
Identifiers: **Message**:Divide By Zero

Vulnerability 3.584
Test-specific ID: SNYK-DEBIAN10-DJVULIBRE-5858456 **Severity:** low
Identifiers: **Message**:Divide By Zero

Vulnerability 3.585
Test-specific ID: SNYK-DEBIAN10-E2FSPROGS-2628482 **Severity:** low
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.586
Test-specific ID: SNYK-DEBIAN10-ELFUTILS-5803147 **Severity:** low
Identifiers: **Message**:Loop with Unreachable Exit Condition ('Infinite Loop')

Vulnerability 3.587
Test-specific ID: SNYK-DEBIAN10-EXPAT-358079 **Severity:** low
Identifiers: **Message**:XML External Entity (XXE) Injection

Vulnerability 3.588
Test-specific ID: SNYK-DEBIAN10-FREETYPE-2848684 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.589
Test-specific ID: SNYK-DEBIAN10-GCC8-469413 **Severity:** low
Identifiers: **Message**:Insufficient Entropy

Vulnerability 3.590
Test-specific ID: SNYK-DEBIAN10-GCC8-5901315 **Severity:** low
Identifiers: **Message**:CVE-2023-4039

Vulnerability 3.591
Test-specific ID: SNYK-DEBIAN10-GDKPIXBUF-6207390 **Severity:** low
Identifiers: **Message**:CVE-2022-48622

Vulnerability 3.592
Test-specific ID: SNYK-DEBIAN10-GIT-2399905 **Severity:** low
Identifiers: **Message**:Exposure of Resource to Wrong Sphere

Vulnerability 3.593
Test-specific ID: SNYK-DEBIAN10-GIT-340854 **Severity:** low
Identifiers: **Message**:Improper Input Validation

Vulnerability 3.594
Test-specific ID: SNYK-DEBIAN10-GIT-5461944 **Severity:** low
Identifiers: **Message**:Directory Traversal

Vulnerability 3.595
Test-specific ID: SNYK-DEBIAN10-GIT-5461945 **Severity:** low
Identifiers: **Message**:Use of Externally-Controlled Format String

Vulnerability 3.596
Test-specific ID: SNYK-DEBIAN10-GIT-5461946 **Severity:** low
Identifiers: **Message**:Arbitrary Code Injection

Vulnerability 3.597
Test-specific ID: SNYK-DEBIAN10-GLIB20-1051691 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.598
Test-specific ID: SNYK-DEBIAN10-GLIB20-300105 **Severity:** low
Identifiers: **Message**:Cryptographic Issues

Vulnerability 3.599
Test-specific ID: SNYK-DEBIAN10-GLIBC-1078993 **Severity:** low
Identifiers: **Message**:Double Free

Vulnerability 3.600

Test-specific ID: SNYK-DEBIAN10-GLIBC-338106 **Severity:** low
Identifiers: **Message**:Uncontrolled Recursion

Vulnerability 3.601

Test-specific ID: SNYK-DEBIAN10-GLIBC-338163 **Severity:** low
Identifiers: **Message**:Uncontrolled Recursion

Vulnerability 3.602

Test-specific ID: SNYK-DEBIAN10-GLIBC-356735 **Severity:** low
Identifiers: **Message**:Resource Management Errors

Vulnerability 3.603

Test-specific ID: SNYK-DEBIAN10-GLIBC-452228 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.604

Test-specific ID: SNYK-DEBIAN10-GLIBC-452267 **Severity:** low
Identifiers: **Message**:CVE-2019-1010023

Vulnerability 3.605

Test-specific ID: SNYK-DEBIAN10-GLIBC-453375 **Severity:** low
Identifiers: **Message**:Use of Insufficiently Random Values

Vulnerability 3.606

Test-specific ID: SNYK-DEBIAN10-GLIBC-453640 **Severity:** low
Identifiers: **Message**:Information Exposure

Vulnerability 3.607
Test-specific ID: SNYK-DEBIAN10-GLIBC-534995 **Severity:** low
Identifiers: **Message**:Information Exposure

Vulnerability 3.608
Test-specific ID: SNYK-DEBIAN10-GLIBC-5894106 **Severity:** low
Identifiers: **Message**:Use After Free

Vulnerability 3.609
Test-specific ID: SNYK-DEBIAN10-GLIBC-5894107 **Severity:** low
Identifiers: **Message**:Use After Free

Vulnerability 3.610
Test-specific ID: SNYK-DEBIAN10-GNUPG2-3330746 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.611
Test-specific ID: SNYK-DEBIAN10-GNUPG2-535553 **Severity:** low
Identifiers: **Message**:Use of a Broken or Risky Cryptographic Algorithm

Vulnerability 3.612
Test-specific ID: SNYK-DEBIAN10-GNUTLS28-340755 **Severity:** low
Identifiers: **Message**:Improper Input Validation

Vulnerability 3.613
Test-specific ID: SNYK-DEBIAN10-GNUTLS28-6159416 **Severity:** low
Identifiers: **Message**:Improper Verification of Cryptographic Signature

Vulnerability 3.614

Test-specific ID: SNYK-DEBIAN10-HARFBUZZ-2934731 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.615

Test-specific ID: SNYK-DEBIAN10-HARFBUZZ-3311296 **Severity:** low
Identifiers: **Message**:Allocation of Resources Without Limits or Throttling

Vulnerability 3.616

Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-1021142 **Severity:** low
Identifiers: **Message**:Divide By Zero

Vulnerability 3.617

Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-1045665 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.618

Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-1045667 **Severity:** low
Identifiers: **Message**:Memory Leak

Vulnerability 3.619

Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-1045673 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.620

Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-1045675 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.621

Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-1045677 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.622

Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-1045681 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.623

Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-1045685 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.624

Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-1045691 **Severity:** low
Identifiers: **Message**:Memory Leak

Vulnerability 3.625

Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-1045695 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.626

Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-1045699 **Severity:** low
Identifiers: **Message**:Divide By Zero

Vulnerability 3.627

Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-1045707 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.628

Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-1045709 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.629

Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-1045721 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.630

Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-1045725 **Severity:** low
Identifiers: **Message**:Divide By Zero

Vulnerability 3.631

Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-1045727 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.632

Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-1045743 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.633

Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-1045759 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.634

Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-1045762 **Severity:** low
Identifiers: **Message**:Divide By Zero

Vulnerability 3.635
Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-1045769 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.636
Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-1045773 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.637
Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-1045775 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.638
Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-1045782 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.639
Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-1048018 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.640
Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-1048581 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.641
Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-1247326 **Severity:** low
Identifiers: **Message**:Divide By Zero

Vulnerability 3.642

Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-1584524 **Severity:** low
Identifiers: **Message**:Exposure of Resource to Wrong Sphere

Vulnerability 3.643

Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-2441376 **Severity:** low
Identifiers: **Message**:Use After Free

Vulnerability 3.644

Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-3008096 **Severity:** low
Identifiers: **Message**:Memory Leak

Vulnerability 3.645

Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-3027310 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.646

Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-400130 **Severity:** low
Identifiers: **Message**:Resource Exhaustion

Vulnerability 3.647

Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-402740 **Severity:** low
Identifiers: **Message**:Missing Release of Resource after Effective Lifetime

Vulnerability 3.648

Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-402776 **Severity:** low
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.649

Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-402794 **Severity:** low
Identifiers: **Message**:Missing Release of Resource after Effective Lifetime

Vulnerability 3.650

Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-402836 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.651

Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-402879 **Severity:** low
Identifiers: **Message**:CVE-2005-0406

Vulnerability 3.652

Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-402911 **Severity:** low
Identifiers: **Message**:Resource Management Errors

Vulnerability 3.653

Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-452738 **Severity:** low
Identifiers: **Message**:Memory Leak

Vulnerability 3.654

Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-468936 **Severity:** low
Identifiers: **Message**:Missing Release of Resource after Effective Lifetime

Vulnerability 3.655

Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-5421091 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.656
Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-5591137 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.657
Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-5660571 **Severity:** low
Identifiers: **Message**:OS Command Injection

Vulnerability 3.658
Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-5660606 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.659
Test-specific ID: SNYK-DEBIAN10-IMAGEMAGICK-5707521 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.660
Test-specific ID: SNYK-DEBIAN10-IPROUTE2-568742 **Severity:** low
Identifiers: **Message**:Use After Free

Vulnerability 3.661
Test-specific ID: SNYK-DEBIAN10-IPTABLES-287323 **Severity:** low
Identifiers: **Message**:CVE-2012-2663

Vulnerability 3.662
Test-specific ID: SNYK-DEBIAN10-IPTABLES-451768 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.663

Test-specific ID: SNYK-DEBIAN10-JBIGKIT-289888 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.664

Test-specific ID: SNYK-DEBIAN10-KRB5-395955 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.665

Test-specific ID: SNYK-DEBIAN10-LIBCROCO-300647 **Severity:** low
Identifiers: **Message**:Loop with Unreachable Exit Condition ('Infinite Loop')

Vulnerability 3.666

Test-specific ID: SNYK-DEBIAN10-LIBCROCO-300673 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.667

Test-specific ID: SNYK-DEBIAN10-LIBCROCO-569056 **Severity:** low
Identifiers: **Message**:Uncontrolled Recursion

Vulnerability 3.668

Test-specific ID: SNYK-DEBIAN10-LIBGCRYPT20-1297893 **Severity:** low
Identifiers: **Message**:Information Exposure

Vulnerability 3.669

Test-specific ID: SNYK-DEBIAN10-LIBGCRYPT20-391902 **Severity:** low
Identifiers: **Message**:Use of a Broken or Risky Cryptographic Algorithm

Vulnerability 3.670

Test-specific ID: SNYK-DEBIAN10-LIBGCRYPT20-460489 **Severity:** low
Identifiers: **Message**:Race Condition

Vulnerability 3.671

Test-specific ID: SNYK-DEBIAN10-LIBHEIF-1533480 **Severity:** low
Identifiers: **Message**:CVE-2020-19498

Vulnerability 3.672

Test-specific ID: SNYK-DEBIAN10-LIBHEIF-1533492 **Severity:** low
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.673

Test-specific ID: SNYK-DEBIAN10-LIBHEIF-1910706 **Severity:** low
Identifiers: **Message**:Buffer Overflow

Vulnerability 3.674

Test-specific ID: SNYK-DEBIAN10-LIBHEIF-3331228 **Severity:** low
Identifiers: **Message**:Buffer Overflow

Vulnerability 3.675

Test-specific ID: SNYK-DEBIAN10-LIBHEIF-5498467 **Severity:** low
Identifiers: **Message**:Divide By Zero

Vulnerability 3.676

Test-specific ID: SNYK-DEBIAN10-LIBIDN2-474100 **Severity:** low
Identifiers: **Message**:Improper Input Validation

Vulnerability 3.677
Test-specific ID: SNYK-DEBIAN10-LIBJPEGTURBO-1298595 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.678
Test-specific ID: SNYK-DEBIAN10-LIBJPEGTURBO-2932110 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.679
Test-specific ID: SNYK-DEBIAN10-LIBJPEGTURBO-299879 **Severity:** low
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.680
Test-specific ID: SNYK-DEBIAN10-LIBJPEGTURBO-3016021 **Severity:** low
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.681
Test-specific ID: SNYK-DEBIAN10-LIBJPEGTURBO-572943 **Severity:** low
Identifiers: **Message**:Excessive Iteration

Vulnerability 3.682
Test-specific ID: SNYK-DEBIAN10-LIBPNG16-2363925 **Severity:** low
Identifiers: **Message**:Buffer Overflow

Vulnerability 3.683
Test-specific ID: SNYK-DEBIAN10-LIBPNG16-296440 **Severity:** low
Identifiers: **Message**:CVE-2018-14048

Vulnerability 3.684

Test-specific ID: SNYK-DEBIAN10-LIBPNG16-296468 **Severity:** low
Identifiers: **Message**:Memory Leak

Vulnerability 3.685

Test-specific ID: SNYK-DEBIAN10-LIBPNG16-296471 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.686

Test-specific ID: SNYK-DEBIAN10-LIBSECCOMP-341044 **Severity:** low
Identifiers: **Message**:CVE-2019-9893

Vulnerability 3.687

Test-specific ID: SNYK-DEBIAN10-LIBSEPOL-1315628 **Severity:** low
Identifiers: **Message**:Use After Free

Vulnerability 3.688

Test-specific ID: SNYK-DEBIAN10-LIBSEPOL-1315630 **Severity:** low
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.689

Test-specific ID: SNYK-DEBIAN10-LIBSEPOL-1315636 **Severity:** low
Identifiers: **Message**:Use After Free

Vulnerability 3.690

Test-specific ID: SNYK-DEBIAN10-LIBSEPOL-1315642 **Severity:** low
Identifiers: **Message**:Use After Free

Vulnerability 3.691

Test-specific ID: SNYK-DEBIAN10-LIBTASN16-339585 **Severity:** low
Identifiers: **Message**:CVE-2018-1000654

Vulnerability 3.692

Test-specific ID: SNYK-DEBIAN10-LIBWMF-306336 **Severity:** low
Identifiers: **Message**:Numeric Errors

Vulnerability 3.693

Test-specific ID: SNYK-DEBIAN10-LIBWMF-306344 **Severity:** low
Identifiers: **Message**:Resource Management Errors

Vulnerability 3.694

Test-specific ID: SNYK-DEBIAN10-LIBWMF-306352 **Severity:** low
Identifiers: **Message**:Numeric Errors

Vulnerability 3.695

Test-specific ID: SNYK-DEBIAN10-LIBWMF-306356 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.696

Test-specific ID: SNYK-DEBIAN10-LIBXML2-2964232 **Severity:** low
Identifiers: **Message**:Cross-site Scripting (XSS)

Vulnerability 3.697

Test-specific ID: SNYK-DEBIAN10-LIBXML2-429486 **Severity:** low
Identifiers: **Message**:Loop with Unreachable Exit Condition (’Infinite Loop’)

Vulnerability 3.698

Test-specific ID: SNYK-DEBIAN10-LIBXML2-429496 **Severity:** low
Identifiers: **Message**:XML External Entity (XXE) Injection

Vulnerability 3.699

Test-specific ID: SNYK-DEBIAN10-LIBXML2-5747747 **Severity:** low
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.700

Test-specific ID: SNYK-DEBIAN10-LIBXML2-5871335 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.701

Test-specific ID: SNYK-DEBIAN10-LIBXML2-5947665 **Severity:** low
Identifiers: **Message**:Use After Free

Vulnerability 3.702

Test-specific ID: SNYK-DEBIAN10-LIBXSLT-308013 **Severity:** low
Identifiers: **Message**:Use of Insufficiently Random Values

Vulnerability 3.703

Test-specific ID: SNYK-DEBIAN10-LZ4-473072 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.704

Test-specific ID: SNYK-DEBIAN10-M4-277768 **Severity:** low
Identifiers: **Message**:CVE-2008-1688

Vulnerability 3.705
Test-specific ID: SNYK-DEBIAN10-M4-277772 **Severity:** low
Identifiers: **Message**:CVE-2008-1687

Vulnerability 3.706
Test-specific ID: SNYK-DEBIAN10-NCURSES-6123819 **Severity:** low
Identifiers: **Message**:CVE-2023-50495

Vulnerability 3.707
Test-specific ID: SNYK-DEBIAN10-OPENEXR-1300571 **Severity:** low
Identifiers: **Message**:Integer Underflow

Vulnerability 3.708
Test-specific ID: SNYK-DEBIAN10-OPENEXR-1318917 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.709
Test-specific ID: SNYK-DEBIAN10-OPENEXR-331140 **Severity:** low
Identifiers: **Message**:Missing Release of Resource after Effective Lifetime

Vulnerability 3.710
Test-specific ID: SNYK-DEBIAN10-OPENEXR-331188 **Severity:** low
Identifiers: **Message**:Resource Exhaustion

Vulnerability 3.711
Test-specific ID: SNYK-DEBIAN10-OPENJPEG2-1247330 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.712
Test-specific ID: SNYK-DEBIAN10-OPENJPEG2-1301275 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.713
Test-specific ID: SNYK-DEBIAN10-OPENJPEG2-2434861 **Severity:** low
Identifiers: **Message**:Improper Initialization

Vulnerability 3.714
Test-specific ID: SNYK-DEBIAN10-OPENJPEG2-336268 **Severity:** low
Identifiers: **Message**:Allocation of Resources Without Limits or Throttling

Vulnerability 3.715
Test-specific ID: SNYK-DEBIAN10-OPENJPEG2-345763 **Severity:** low
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.716
Test-specific ID: SNYK-DEBIAN10-OPENJPEG2-345829 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.717
Test-specific ID: SNYK-DEBIAN10-OPENJPEG2-345857 **Severity:** low
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.718
Test-specific ID: SNYK-DEBIAN10-OPENJPEG2-345871 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.719
Test-specific ID: SNYK-DEBIAN10-OPENJPEG2-345885 **Severity:** low
Identifiers: **Message**:Divide By Zero

Vulnerability 3.720
Test-specific ID: SNYK-DEBIAN10-OPENJPEG2-345941 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.721
Test-specific ID: SNYK-DEBIAN10-OPENJPEG2-345945 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.722
Test-specific ID: SNYK-DEBIAN10-OPENJPEG2-345952 **Severity:** low
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.723
Test-specific ID: SNYK-DEBIAN10-OPENJPEG2-345959 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.724
Test-specific ID: SNYK-DEBIAN10-OPENJPEG2-345968 **Severity:** low
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.725
Test-specific ID: SNYK-DEBIAN10-OPENJPEG2-345981 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.726
Test-specific ID: SNYK-DEBIAN10-OPENJPEG2-345985 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.727
Test-specific ID: SNYK-DEBIAN10-OPENJPEG2-345989 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.728
Test-specific ID: SNYK-DEBIAN10-OPENJPEG2-345997 **Severity:** low
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.729
Test-specific ID: SNYK-DEBIAN10-OPENJPEG2-451267 **Severity:** low
Identifiers: **Message**:Improper Input Validation

Vulnerability 3.730
Test-specific ID: SNYK-DEBIAN10-OPENJPEG2-451269 **Severity:** low
Identifiers: **Message**:Divide By Zero

Vulnerability 3.731
Test-specific ID: SNYK-DEBIAN10-OPENJPEG2-451274 **Severity:** low
Identifiers: **Message**:Excessive Iteration

Vulnerability 3.732
Test-specific ID: SNYK-DEBIAN10-OPENLDAP-304601 **Severity:** low
Identifiers: **Message**:Improper Initialization

Vulnerability 3.733

Test-specific ID: SNYK-DEBIAN10-OPENLDAP-304654 **Severity:** low
Identifiers: **Message**:Cryptographic Issues

Vulnerability 3.734

Test-specific ID: SNYK-DEBIAN10-OPENLDAP-304666 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.735

Test-specific ID: SNYK-DEBIAN10-OPENLDAP-5660621 **Severity:** low
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.736

Test-specific ID: SNYK-DEBIAN10-OPENLDAP-584924 **Severity:** low
Identifiers: **Message**:Improper Certificate Validation

Vulnerability 3.737

Test-specific ID: SNYK-DEBIAN10-OPENSSH-1585653 **Severity:** low
Identifiers: **Message**:CVE-2016-20012

Vulnerability 3.738

Test-specific ID: SNYK-DEBIAN10-OPENSSH-2422622 **Severity:** low
Identifiers: **Message**:Improper Authentication

Vulnerability 3.739

Test-specific ID: SNYK-DEBIAN10-OPENSSH-368617 **Severity:** low
Identifiers: **Message**:Information Exposure

Vulnerability 3.740

Test-specific ID: SNYK-DEBIAN10-OPENSSH-368833 **Severity:** low
Identifiers: **Message**:Access Restriction Bypass

Vulnerability 3.741

Test-specific ID: SNYK-DEBIAN10-OPENSSH-368925 **Severity:** low
Identifiers: **Message**:Information Exposure

Vulnerability 3.742

Test-specific ID: SNYK-DEBIAN10-OPENSSH-369016 **Severity:** low
Identifiers: **Message**:Improper Authentication

Vulnerability 3.743

Test-specific ID: SNYK-DEBIAN10-OPENSSH-369020 **Severity:** low
Identifiers: **Message**:Inappropriate Encoding for Output Context

Vulnerability 3.744

Test-specific ID: SNYK-DEBIAN10-OPENSSH-472477 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.745

Test-specific ID: SNYK-DEBIAN10-OPENSSH-570880 **Severity:** low
Identifiers: **Message**:Improper Input Validation

Vulnerability 3.746

Test-specific ID: SNYK-DEBIAN10-OPENSSH-574764 **Severity:** low
Identifiers: **Message**:Information Exposure

Vulnerability 3.747

Test-specific ID: SNYK-DEBIAN10-OPENSSH-590144 **Severity:** low
Identifiers: **Message**:OS Command Injection

Vulnerability 3.748

Test-specific ID: SNYK-DEBIAN10-OPENSSL-374709 **Severity:** low
Identifiers: **Message**:Cryptographic Issues

Vulnerability 3.749

Test-specific ID: SNYK-DEBIAN10-OPENSSL-374996 **Severity:** low
Identifiers: **Message**:Cryptographic Issues

Vulnerability 3.750

Test-specific ID: SNYK-DEBIAN10-OPENSSL-6048818 **Severity:** low
Identifiers: **Message**:Improper Check for Unusual or Exceptional Conditions

Vulnerability 3.751

Test-specific ID: SNYK-DEBIAN10-OPENSSL-6190221 **Severity:** low
Identifiers: **Message**:CVE-2024-0727

Vulnerability 3.752

Test-specific ID: SNYK-DEBIAN10-PAM-6178916 **Severity:** low
Identifiers: **Message**:CVE-2024-22365

Vulnerability 3.753

Test-specific ID: SNYK-DEBIAN10-PATCH-2324790 **Severity:** low
Identifiers: **Message**:Release of Invalid Pointer or Reference

Vulnerability 3.754
Test-specific ID: SNYK-DEBIAN10-PATCH-303854 **Severity:** low
Identifiers: **Message**:Double Free

Vulnerability 3.755
Test-specific ID: SNYK-DEBIAN10-PATCH-303870 **Severity:** low
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.756
Test-specific ID: SNYK-DEBIAN10-PATCH-303893 **Severity:** low
Identifiers: **Message**:Directory Traversal

Vulnerability 3.757
Test-specific ID: SNYK-DEBIAN10-PCRE2-5788328 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.758
Test-specific ID: SNYK-DEBIAN10-PCRE3-345321 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.759
Test-specific ID: SNYK-DEBIAN10-PCRE3-345353 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.760
Test-specific ID: SNYK-DEBIAN10-PCRE3-345502 **Severity:** low
Identifiers: **Message**:Uncontrolled Recursion

Vulnerability 3.761
Test-specific ID: SNYK-DEBIAN10-PCRE3-345530 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.762
Test-specific ID: SNYK-DEBIAN10-PCRE3-572367 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.763
Test-specific ID: SNYK-DEBIAN10-PCRE3-572368 **Severity:** low
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.764
Test-specific ID: SNYK-DEBIAN10-PERL-1925980 **Severity:** low
Identifiers: **Message**:Improper Verification of Cryptographic Signature

Vulnerability 3.765
Test-specific ID: SNYK-DEBIAN10-PERL-327793 **Severity:** low
Identifiers: **Message**:Link Following

Vulnerability 3.766
Test-specific ID: SNYK-DEBIAN10-PERL-5489186 **Severity:** low
Identifiers: **Message**:Improper Certificate Validation

Vulnerability 3.767
Test-specific ID: SNYK-DEBIAN10-PERL-5489188 **Severity:** low
Identifiers: **Message**:Improper Certificate Validation

Vulnerability 3.768

Test-specific ID: SNYK-DEBIAN10-PIXMAN-5803157 **Severity:** low
Identifiers: **Message**:Divide By Zero

Vulnerability 3.769

Test-specific ID: SNYK-DEBIAN10-PROCPS-5816469 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.770

Test-specific ID: SNYK-DEBIAN10-PYTHON27-306560 **Severity:** low
Identifiers: **Message**:Cryptographic Issues

Vulnerability 3.771

Test-specific ID: SNYK-DEBIAN10-PYTHON27-306596 **Severity:** low
Identifiers: **Message**:Arbitrary Code Injection

Vulnerability 3.772

Test-specific ID: SNYK-DEBIAN10-PYTHON27-474393 **Severity:** low
Identifiers: **Message**:Arbitrary Code Injection

Vulnerability 3.773

Test-specific ID: SNYK-DEBIAN10-PYTHON27-5423195 **Severity:** low
Identifiers: **Message**:Incorrect Type Conversion or Cast

Vulnerability 3.774

Test-specific ID: SNYK-DEBIAN10-PYTHON27-5423208 **Severity:** low
Identifiers: **Message**:CVE-2020-27619

Vulnerability 3.775

Test-specific ID: SNYK-DEBIAN10-PYTHON27-5423209 **Severity:** low
Identifiers: **Message**:Open Redirect

Vulnerability 3.776

Test-specific ID: SNYK-DEBIAN10-PYTHON27-5430935 **Severity:** low
Identifiers: **Message**:Improper Input Validation

Vulnerability 3.777

Test-specific ID: SNYK-DEBIAN10-PYTHON27-546420 **Severity:** low
Identifiers: **Message**:Resource Exhaustion

Vulnerability 3.778

Test-specific ID: SNYK-DEBIAN10-PYTHON27-5754615 **Severity:** low
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.779

Test-specific ID: SNYK-DEBIAN10-PYTHON37-1021148 **Severity:** low
Identifiers: **Message**:CVE-2020-27619

Vulnerability 3.780

Test-specific ID: SNYK-DEBIAN10-PYTHON37-2394829 **Severity:** low
Identifiers: **Message**:Arbitrary Code Injection

Vulnerability 3.781

Test-specific ID: SNYK-DEBIAN10-PYTHON37-279198 **Severity:** low
Identifiers: **Message**:Arbitrary Code Injection

Vulnerability 3.782
Test-specific ID: SNYK-DEBIAN10-PYTHON37-3032980 **Severity:** low
Identifiers: **Message**:Open Redirect

Vulnerability 3.783
Test-specific ID: SNYK-DEBIAN10-PYTHON37-474392 **Severity:** low
Identifiers: **Message**:Arbitrary Code Injection

Vulnerability 3.784
Test-specific ID: SNYK-DEBIAN10-PYTHON37-5430934 **Severity:** low
Identifiers: **Message**:Improper Input Validation

Vulnerability 3.785
Test-specific ID: SNYK-DEBIAN10-PYTHON37-546419 **Severity:** low
Identifiers: **Message**:Resource Exhaustion

Vulnerability 3.786
Test-specific ID: SNYK-DEBIAN10-PYTHON37-5754663 **Severity:** low
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.787
Test-specific ID: SNYK-DEBIAN10-PYTHONDEFAULTS-269278 **Severity:** low
Identifiers: **Message**:Link Following

Vulnerability 3.788
Test-specific ID: SNYK-DEBIAN10-SHADOW-306205 **Severity:** low
Identifiers: **Message**:Time-of-check Time-of-use (TOCTOU)

Vulnerability 3.789

Test-specific ID: SNYK-DEBIAN10-SHADOW-306230 **Severity:** low
Identifiers: **Message**:Incorrect Permission Assignment for Critical Resource

Vulnerability 3.790

Test-specific ID: SNYK-DEBIAN10-SHADOW-306250 **Severity:** low
Identifiers: **Message**:Access Restriction Bypass

Vulnerability 3.791

Test-specific ID: SNYK-DEBIAN10-SHADOW-539852 **Severity:** low
Identifiers: **Message**:Incorrect Permission Assignment for Critical Resource

Vulnerability 3.792

Test-specific ID: SNYK-DEBIAN10-SHADOW-5423925 **Severity:** low
Identifiers: **Message**:Arbitrary Code Injection

Vulnerability 3.793

Test-specific ID: SNYK-DEBIAN10-SHADOW-5879153 **Severity:** low
Identifiers: **Message**:Improper Authentication

Vulnerability 3.794

Test-specific ID: SNYK-DEBIAN10-SQLITE3-1569415 **Severity:** low
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.795

Test-specific ID: SNYK-DEBIAN10-SQLITE3-2407046 **Severity:** low
Identifiers: **Message**:Memory Leak

Vulnerability 3.796

Test-specific ID: SNYK-DEBIAN10-SQLITE3-2959398 **Severity:** low
Identifiers: **Message**:Improper Validation of Array Index

Vulnerability 3.797

Test-specific ID: SNYK-DEBIAN10-SQLITE3-535712 **Severity:** low
Identifiers: **Message**:CVE-2019-19244

Vulnerability 3.798

Test-specific ID: SNYK-DEBIAN10-SQLITE3-537251 **Severity:** low
Identifiers: **Message**:Uncontrolled Recursion

Vulnerability 3.799

Test-specific ID: SNYK-DEBIAN10-SQLITE3-537598 **Severity:** low
Identifiers: **Message**:CVE-2019-19603

Vulnerability 3.800

Test-specific ID: SNYK-DEBIAN10-SQLITE3-539769 **Severity:** low
Identifiers: **Message**:Improper Handling of Exceptional Conditions

Vulnerability 3.801

Test-specific ID: SNYK-DEBIAN10-SQLITE3-5562379 **Severity:** low
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.802

Test-specific ID: SNYK-DEBIAN10-SQLITE3-565214 **Severity:** low
Identifiers: **Message**:Use After Free

Vulnerability 3.803
Test-specific ID: SNYK-DEBIAN10-SQLITE3-570487 **Severity:** low
Identifiers: **Message**:CVE-2020-13631

Vulnerability 3.804
Test-specific ID: SNYK-DEBIAN10-SQLITE3-6139921 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.805
Test-specific ID: SNYK-DEBIAN10-SYSTEMD-1291056 **Severity:** low
Identifiers: **Message**:Authentication Bypass

Vulnerability 3.806
Test-specific ID: SNYK-DEBIAN10-SYSTEMD-2332026 **Severity:** low
Identifiers: **Message**:Uncontrolled Recursion

Vulnerability 3.807
Test-specific ID: SNYK-DEBIAN10-SYSTEMD-305144 **Severity:** low
Identifiers: **Message**:Link Following

Vulnerability 3.808
Test-specific ID: SNYK-DEBIAN10-SYSTEMD-345386 **Severity:** low
Identifiers: **Message**:Privilege Chaining

Vulnerability 3.809
Test-specific ID: SNYK-DEBIAN10-SYSTEMD-345391 **Severity:** low
Identifiers: **Message**:Incorrect Privilege Assignment

Vulnerability 3.810

Test-specific ID: SNYK-DEBIAN10-SYSTEMD-542807 **Severity:** low
Identifiers: **Message**:Missing Release of Resource after Effective Lifetime

Vulnerability 3.811

Test-specific ID: SNYK-DEBIAN10-SYSTEMD-5733386 **Severity:** low
Identifiers: **Message**:Improper Validation of Integrity Check Value

Vulnerability 3.812

Test-specific ID: SNYK-DEBIAN10-SYSTEMD-5733393 **Severity:** low
Identifiers: **Message**:Improper Validation of Integrity Check Value

Vulnerability 3.813

Test-specific ID: SNYK-DEBIAN10-SYSTEMD-5733397 **Severity:** low
Identifiers: **Message**:Improper Validation of Integrity Check Value

Vulnerability 3.814

Test-specific ID: SNYK-DEBIAN10-SYSTEMD-6137710 **Severity:** low
Identifiers: **Message**:CVE-2023-7008

Vulnerability 3.815

Test-specific ID: SNYK-DEBIAN10-TAR-1063001 **Severity:** low
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.816

Test-specific ID: SNYK-DEBIAN10-TAR-312331 **Severity:** low
Identifiers: **Message**:CVE-2005-2541

Vulnerability 3.817
Test-specific ID: SNYK-DEBIAN10-TAR-3253529 **Severity:** low
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.818
Test-specific ID: SNYK-DEBIAN10-TAR-341203 **Severity:** low
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.819
Test-specific ID: SNYK-DEBIAN10-TAR-6120423 **Severity:** low
Identifiers: **Message**:CVE-2023-39804

Vulnerability 3.820
Test-specific ID: SNYK-DEBIAN10-TCL86-1316210 **Severity:** low
Identifiers: **Message**:Use of Externally-Controlled Format String

Vulnerability 3.821
Test-specific ID: SNYK-DEBIAN10-TIFF-1079067 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.822
Test-specific ID: SNYK-DEBIAN10-TIFF-1079073 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.823
Test-specific ID: SNYK-DEBIAN10-TIFF-2434413 **Severity:** low
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.824
Test-specific ID: SNYK-DEBIAN10-TIFF-2440570 **Severity:** low
Identifiers: **Message**:Improper Resource Shutdown or Release

Vulnerability 3.825
Test-specific ID: SNYK-DEBIAN10-TIFF-3008947 **Severity:** low
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.826
Test-specific ID: SNYK-DEBIAN10-TIFF-3012392 **Severity:** low
Identifiers: **Message**:Double Free

Vulnerability 3.827
Test-specific ID: SNYK-DEBIAN10-TIFF-3012397 **Severity:** low
Identifiers: **Message**:Incorrect Calculation of Buffer Size

Vulnerability 3.828
Test-specific ID: SNYK-DEBIAN10-TIFF-3012400 **Severity:** low
Identifiers: **Message**:Release of Invalid Pointer or Reference

Vulnerability 3.829
Test-specific ID: SNYK-DEBIAN10-TIFF-405264 **Severity:** low
Identifiers: **Message**:Use After Free

Vulnerability 3.830
Test-specific ID: SNYK-DEBIAN10-TIFF-405387 **Severity:** low
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.831
Test-specific ID: SNYK-DEBIAN10-TIFF-405477 **Severity:** low
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.832
Test-specific ID: SNYK-DEBIAN10-TIFF-405858 **Severity:** low
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.833
Test-specific ID: SNYK-DEBIAN10-TIFF-406148 **Severity:** low
Identifiers: **Message**:Missing Release of Resource after Effective Lifetime

Vulnerability 3.834
Test-specific ID: SNYK-DEBIAN10-TIFF-5416361 **Severity:** low
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.835
Test-specific ID: SNYK-DEBIAN10-TIFF-5425906 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.836
Test-specific ID: SNYK-DEBIAN10-TIFF-5673711 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.837
Test-specific ID: SNYK-DEBIAN10-TIFF-5852999 **Severity:** low
Identifiers: **Message**:Loop with Unreachable Exit Condition (’Infinite Loop’)

Vulnerability 3.838

Test-specific ID: SNYK-DEBIAN10-TIFF-5934952 **Severity:** low
Identifiers: **Message**:Memory Leak

Vulnerability 3.839

Test-specific ID: SNYK-DEBIAN10-TIFF-6079921 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.840

Test-specific ID: SNYK-DEBIAN10-TIFF-6084511 **Severity:** low
Identifiers: **Message**:Resource Exhaustion

Vulnerability 3.841

Test-specific ID: SNYK-DEBIAN10-TIFF-6190611 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.842

Test-specific ID: SNYK-DEBIAN10-TIFF-6190612 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.843

Test-specific ID: SNYK-DEBIAN10-UNBOUND-1277126 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.844

Test-specific ID: SNYK-DEBIAN10-UNBOUND-1277133 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.845
Test-specific ID: SNYK-DEBIAN10-UNBOUND-1277135 **Severity:** low
Identifiers: **Message**:Reachable Assertion

Vulnerability 3.846
Test-specific ID: SNYK-DEBIAN10-UNBOUND-1277137 **Severity:** low
Identifiers: **Message**:Arbitrary Code Injection

Vulnerability 3.847
Test-specific ID: SNYK-DEBIAN10-UNBOUND-1277145 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.848
Test-specific ID: SNYK-DEBIAN10-UNBOUND-1277149 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.849
Test-specific ID: SNYK-DEBIAN10-UNBOUND-1277150 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.850
Test-specific ID: SNYK-DEBIAN10-UNBOUND-1277154 **Severity:** low
Identifiers: **Message**:Loop with Unreachable Exit Condition (’Infinite Loop’)

Vulnerability 3.851
Test-specific ID: SNYK-DEBIAN10-UNBOUND-1277159 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.852

Test-specific ID: SNYK-DEBIAN10-UNBOUND-1277161 **Severity:** low
Identifiers: **Message**:Reachable Assertion

Vulnerability 3.853

Test-specific ID: SNYK-DEBIAN10-UNBOUND-1277163 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.854

Test-specific ID: SNYK-DEBIAN10-UNBOUND-1277171 **Severity:** low
Identifiers: **Message**:Reachable Assertion

Vulnerability 3.855

Test-specific ID: SNYK-DEBIAN10-UNBOUND-534899 **Severity:** low
Identifiers: **Message**:Improper Input Validation

Vulnerability 3.856

Test-specific ID: SNYK-DEBIAN10-UNZIP-2387328 **Severity:** low
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.857

Test-specific ID: SNYK-DEBIAN10-UTILLINUX-1534833 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.858

Test-specific ID: SNYK-DEBIAN10-UTILLINUX-2401082 **Severity:** low
Identifiers: **Message**:Information Exposure

Vulnerability 3.859

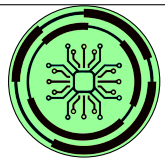
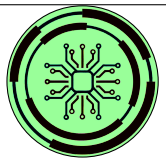
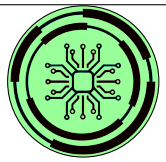
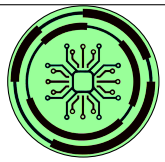
Test-specific ID: SNYK-DEBIAN10-WGET-1277612 **Severity:** low
Identifiers: **Message**:Open Redirect

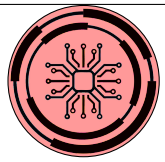
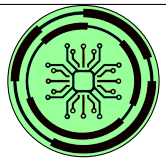
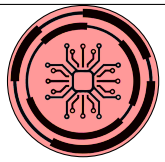
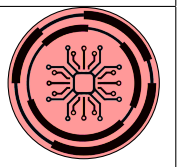
4. Dynamic Train Analysis

No Dynamic Report Available

5. Conclusion

The PADME Security Audit has come to the following conclusion:

Static Complete	SAST	Dependencies	Secret Detection
			

Standard Compliant	Blacklist	Train Image Analysis	DAST
			

Warnings

- Found 1 critical vulnerability in the image.
- Couldn't detect compliance with standards (usage of the python module padme_conductor [https://pypi.org/project/padme-conductor]).
- The reports dynamic_report.json are missing. Acceptance threshold increased from 0.5 to 0.75.

Audit Result

Train Rejected

February 1, 2024