Manual & Security Audit for Train

ISIC2019I

Karl Kindermann

PADME-ANALYTICS.DE

First printing, January 31, 2024

Contents

1. Train Summary

1.1 Overview

- **Train name:** ISIC2019I
- **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=ISIC2019I

1.2 Image Building File

Listing 1.1: Image building file

```
FROM python:3.6

WORKDIR /

# LABEL
LABEL "envs"="[{\"name\":\"FHIR_SERVER\",\"type\":\"string
   \",\"required\":true},{\"name\":\"FHIR_PORT\",\"type\":\"
   number\",\"required\":true}]"

COPY requirements.txt ./
RUN pip install --no-cache-dir -r requirements.txt

COPY . .

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

1.3 Requirements & Dependencies

Listing 1.2: List of all Requirements

```
pandas
numpy
fhirpy
datetime
matplotlib
```

1.4 Code Base

Legend: env query retrieve_previous_results execute_analysis save log

```python
import os
import os.path as osp
import numpy as np
import pandas as pd
import matplotlib.pyplot as plt
import glob

from fhirpy import SyncFHIRClient

## Define directory of output
here = osp.dirname(osp.abspath(__file__))
out_dir = osp.join(here, ’output’)
if not os.path.exists(out_dir):
    os.makedirs(out_dir)
runs = sorted(glob.glob(os.path.join(out_dir, ’run_*’)))
run_id = int(runs[-1].split(’_’)[-1]) + 1 if runs else 0
experiment_dir = os.path.join(out_dir, ’run_{}’.format(str(run_id)))
if not os.path.exists(experiment_dir):
    os.makedirs(experiment_dir)

## Define (output) file formats
if not osp.exists(osp.join(experiment_dir, ’report.txt’)):
    with open(osp.join(experiment_dir, ’report.txt’), ’w’) as f:
        pass

## Define (input) variables from Docker Container environment variables
fhir_server = str(os.environ[’FHIR_SERVER’])
fhir_port = str(os.environ[’FHIR_PORT’])

## Load aggregated results from previous stations
# if run_id > 0:
#     prev_experiment_dir = osp.join(out_dir, ’run_{}’.format(str(run_id -
    1)))
#     if osp.exists(osp.join(prev_experiment_dir, ’’)):
#         pass
#     else:
#         pass
# else:
#     pass

## Collect Data Statistic
# Create an instance
client = SyncFHIRClient(’http://{}:{}/fhir’.format(fhir_server, fhir_port))
# Search for patients
patients = client.resources(’Patient’)  # Return lazy search set
patients_data = []
for patient in patients:
    patient_birthDate = None
    try:
        patient_birthDate = patient.birthDate
    except:
        pass
    # patinet_id, gender, birthDate
    patients_data.append([patient.id, patient.gender, patient_birthDate])
patients_df = pd.DataFrame(patients_data, columns=["patient_id", "gender", "birthDate"])
# Search for media
media_list = client.resources('Media').include('Patient', 'subject')
media_data = []
for media in media_list:
    media_bodySite = None
    media_reasonCode = None
    media_note = None
    try:
        media_bodySite = media.bodySite.text
    except:
        pass
    try:
        media_reasonCode = media.reasonCode[0].text
    except:
        pass
    try:
        media_note = media.note[0].text
    except:
        pass
    media_data.append([media.subject.id, media.id, media_bodySite, media_reasonCode, media_note, media.content.url])
media_df = pd.DataFrame(media_data, columns=["patient_id", "media_id", "bodySite", "reasonCode", "note", "image_url"])
data_df = pd.merge(patients_df, media_df, on='patient_id', how='outer')

# Python3 code to  calculate age in years
import datetime
from datetime import date
def calculateAge(born):
    if born is None:
        return None
    born = datetime.datetime.strptime(born, '%Y-%m-%d').date()
    today = date.today()
    try:
        birthday = born.replace(year=today.year)
    except ValueError:
        birthday = born.replace(year=today.year,
                                month=born.month + 1, day=1)
    if birthday > today:
        return today.year - born.year - 1
    else:
        return today.year - born.year

data_df['age'] = data_df['birthDate'].map(lambda x: calculateAge(x))

with open(osp.join(experiment_dir, 'report.txt'), 'a') as f:
    f.write('Stations have {} instances with complete attributes \n'.format(data_df[(data_df['age'].notna()) & (data_df['note'].notna()) & (data_df['gender'].notna())].shape[0]))
    f.write('Station has {} instances whose attribute \"age\" is missing\n'.format(data_df['age'].isna().sum()))
    f.write('Station has {} instances whose attribute \"gender\" is missing\n'.format(data_df['gender'].isna().sum()))
    f.write(’Station has {} instances whose attribute \"bodySite\" is
    missing\n’.format(data_df[’bodySite’].isna().sum()))

data_df[’MEL’] = data_df[’note’].map(lambda x: 1 if x == ’MEL’ else 0)
data_df[’NV’] = data_df[’note’].map(lambda x: 1 if x == ’NV’ else 0)
data_df[’BKL’] = data_df[’note’].map(lambda x: 1 if x == ’BKL’ else 0)
data_df[’DF’] = data_df[’note’].map(lambda x: 1 if x == ’DF’ else 0)
data_df[’SCC’] = data_df[’note’].map(lambda x: 1 if x == ’SCC’ else 0)
data_df[’BCC’] = data_df[’note’].map(lambda x: 1 if x == ’BCC’ else 0)
data_df[’VASC’] = data_df[’note’].map(lambda x: 1 if x == ’VASC’ else 0)
data_df[’AK’] = data_df[’note’].map(lambda x: 1 if x == ’AK’ else 0)

age_df = data_df[[’MEL’,’NV’,’BCC’,’AK’,’BKL’,’DF’,’VASC’,’SCC’,’age’]]
def replace_age(row):
    if row[’age’] == np.nan:
        return pd.Series([np.nan, np.nan, np.nan, np.nan, np.nan, np.nan,
    np.nan, np.nan, np.nan])
    elif row[’MEL’] == 1.0:
        return pd.Series([row[’age’], np.nan, np.nan, np.nan, np.nan, np.
    nan, np.nan, np.nan, np.nan])
    elif row[’NV’] == 1.0:
        return pd.Series([np.nan, row[’age’], np.nan, np.nan, np.nan, np.
    nan, np.nan, np.nan, np.nan])
    elif row[’BCC’] == 1.0:
        return pd.Series([np.nan, np.nan, row[’age’], np.nan, np.nan, np.
    nan, np.nan, np.nan, np.nan])
    elif row[’AK’] == 1.0:
        return pd.Series([np.nan, np.nan, np.nan, row[’age’], np.nan, np.
    nan, np.nan, np.nan, np.nan])
    elif row[’BKL’] == 1.0:
        return pd.Series([np.nan, np.nan, np.nan, np.nan, row[’age’], np.
    nan, np.nan, np.nan, np.nan])
    elif row[’DF’] == 1.0:
        return pd.Series([np.nan, np.nan, np.nan, np.nan, np.nan, row[’age’
    ], np.nan, np.nan, np.nan])
    elif row[’VASC’] == 1.0:
        return pd.Series([np.nan, np.nan, np.nan, np.nan, np.nan, np.nan,
    row[’age’], np.nan, np.nan])
    elif row[’SCC’] == 1.0:
        return pd.Series([np.nan, np.nan, np.nan, np.nan, np.nan, np.nan,
    np.nan, row[’age’],  np.nan])

age_df = age_df.apply(lambda row: replace_age(row), axis=1).rename(columns
    ={0:’MEL’, 1:’NV’, 2:’BCC’, 3:’AK’, 4:’BKL’, 5:’DF’, 6:’VASC’, 7:’SCC’,
     8:’age’}).drop([’age’], axis=1)
age_df.boxplot()
plt.savefig(osp.join(experiment_dir,’age_dist.jpg’))
age_quantile = pd.DataFrame([age_df.quantile(0.25), age_df.quantile(0.5),
    age_df.quantile(0.75)], index=[’lower quartile’,  ’median’, ’upper
    quartile’])
age_quantile.to_csv(osp.join(experiment_dir, ’age.csv’), index=True)

sex_df = data_df[[’MEL’,’NV’,’BCC’,’AK’,’BKL’,’DF’,’VASC’,’SCC’,’gender’]]
sex_sum_df = sex_df.groupby(’gender’).sum()
sex_sum_df.T.plot(kind=’bar’)
plt.savefig(osp.join(experiment_dir,’gender_mal.jpg’))
sex_sum_df.to_csv(osp.join(experiment_dir, ’gender.csv’), index=True)

anotom_df = data_df[[’MEL’,’NV’,’BCC’,’AK’,’BKL’,’DF’,’VASC’,’SCC’,’
    bodySite’]]
anotom_sum_df = anotom_df.groupby(’bodySite’).sum()
```

```python
anotom_sum_df.T.plot(kind='bar')
plt.savefig(osp.join(experiment_dir,'anotom_mal.jpg'))
anotom_sum_df.to_csv(osp.join(experiment_dir, 'anotom.csv'), index=True)
```

Listing 1.3: main.py

```json
{"resources":[{"id":"5bce186a-5005-4ca8-878e-9d8d4e0747c0","datasets":[{"id":"3466461a-1e34-11ed-861d-0242ac120002"}]},{"id":"d7b0a9a7-07fd-4a31-b93a-3c946dc82667","datasets":[{"id":"5fc441e6-f160-11ec-8ea0-0242ac120002"}]}],"route":[{"id":"5bce186a-5005-4ca8-878e-9d8d4e0747c0","ownEnvs":[{"name":"FHIR_SERVER","value":"[redacted]"},{"name":"FHIR_PORT","value":"[redacted]"}]},{"id":"d7b0a9a7-07fd-4a31-b93a-3c946dc82667","ownEnvs":[{"name":"FHIR_SERVER","value":"[redacted]"},{"name":"FHIR_PORT","value":"[redacted]"}]}]}
```

Listing 1.4: route.json

1.5 Connection Parameters

Overall, 2 connection parameters have been found in the train:

Name	Type	Required?
FHIR_SERVER	string	True
FHIR_PORT	number	True

2. Static Train Analysis

Summary 2.1

- **Number of Lines:** 223399
- **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: 297 Medium: 168 High: 113 Critical: 35

Detailed Vulnerabilities:

Critical:

Vulnerability 3.1

Test-specific ID: SNYK-DEBIAN11-AOM-1290331 **Severity:** critical
Identifiers: **Message**:Release of Invalid Pointer or Reference

Vulnerability 3.2

Test-specific ID: SNYK-DEBIAN11-AOM-1298721 **Severity:** critical
Identifiers: **Message**:Use After Free

Vulnerability 3.3

Test-specific ID: SNYK-DEBIAN11-AOM-1300249 **Severity:** critical
Identifiers: **Message**:Buffer Overflow

Vulnerability 3.4

Test-specific ID: SNYK-DEBIAN11-APR-3261105 **Severity:** critical
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.5

Test-specific ID: SNYK-DEBIAN11-CURL-1585150 **Severity:** critical
Identifiers: **Message**:Double Free

Vulnerability 3.6

Test-specific ID: SNYK-DEBIAN11-CURL-2936229 **Severity:** critical
Identifiers: **Message**:Incorrect Default Permissions

Vulnerability 3.7

Test-specific ID: SNYK-DEBIAN11-CURL-3065656 **Severity:** critical
Identifiers: **Message**:Exposure of Resource to Wrong Sphere

Vulnerability 3.8

Test-specific ID: SNYK-DEBIAN11-CURL-3320493 **Severity:** critical
Identifiers: **Message**:Cleartext Transmission of Sensitive Information

Vulnerability 3.9

Test-specific ID: SNYK-DEBIAN11-CURL-5955037 **Severity:** critical
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.10

Test-specific ID: SNYK-DEBIAN11-DPKG-2847942 **Severity:** critical
Identifiers: **Message**:Directory Traversal

Vulnerability 3.11

Test-specific ID: SNYK-DEBIAN11-EXPAT-2331802 **Severity:** critical

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

Vulnerability 3.12

Test-specific ID: SNYK-DEBIAN11-EXPAT-2331808 **Severity:** critical
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.13

Test-specific ID: SNYK-DEBIAN11-EXPAT-2331811 **Severity:** critical
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.14

Test-specific ID: SNYK-DEBIAN11-EXPAT-2359255 **Severity:** critical
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.15

Test-specific ID: SNYK-DEBIAN11-EXPAT-2403510 **Severity:** critical
Identifiers: **Message**:Exposure of Resource to Wrong Sphere

Vulnerability 3.16

Test-specific ID: SNYK-DEBIAN11-EXPAT-2403512 **Severity:** critical
Identifiers: **Message**:Improper Encoding or Escaping of Output

Vulnerability 3.17

Test-specific ID: SNYK-DEBIAN11-EXPAT-2406127 **Severity:** critical
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.18

Test-specific ID: SNYK-DEBIAN11-FREETYPE-2774656 **Severity:** critical
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.19

Test-specific ID: SNYK-DEBIAN11-GIT-3232722 **Severity:** critical
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.20

Test-specific ID: SNYK-DEBIAN11-GIT-3232724 **Severity:** critical
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.21

Test-specific ID: SNYK-DEBIAN11-GLIBC-1296898 **Severity:** critical
Identifiers: **Message**:Use After Free

Vulnerability 3.22

Test-specific ID: SNYK-DEBIAN11-GLIBC-2340908 **Severity:** critical
Identifiers: **Message**:Buffer Overflow

Vulnerability 3.23

Test-specific ID: SNYK-DEBIAN11-GLIBC-2340922 **Severity:** critical
Identifiers: **Message**:Buffer Overflow

Vulnerability 3.24

Test-specific ID: SNYK-DEBIAN11-LIBDE265-2445047 **Severity:** critical
Identifiers: **Message**:Heap-based Buffer Overflow

Vulnerability 3.25

Test-specific ID: SNYK-DEBIAN11-LIBKSBA-3050753 **Severity:** critical
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.26

Test-specific ID: SNYK-DEBIAN11-LIBKSBA-3179188 **Severity:** critical
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.27

Test-specific ID: SNYK-DEBIAN11-LIBTASN16-3061097 **Severity:** critical
Identifiers: **Message**:Off-by-one Error

Vulnerability 3.28

Test-specific ID: SNYK-DEBIAN11-OPENLDAP-2808413 **Severity:** critical
Identifiers: **Message**:SQL Injection

Vulnerability 3.29

Test-specific ID: SNYK-DEBIAN11-OPENSSH-5788321 **Severity:** critical
Identifiers: **Message**:Unquoted Search Path or Element

Vulnerability 3.30

Test-specific ID: SNYK-DEBIAN11-OPENSSL-2807596 **Severity:** critical
Identifiers: **Message**:OS Command Injection

Vulnerability 3.31

Test-specific ID: SNYK-DEBIAN11-OPENSSL-2933518 **Severity:** critical
Identifiers: **Message**:OS Command Injection

Vulnerability 3.32

Test-specific ID: SNYK-DEBIAN11-PCRE2-2808697 **Severity:** critical
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.33

Test-specific ID: SNYK-DEBIAN11-PCRE2-2808704 **Severity:** critical
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.34

Test-specific ID: SNYK-DEBIAN11-ZLIB-2976151 **Severity:** critical
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.35

Test-specific ID: SNYK-DEBIAN11-ZLIB-6008961 **Severity:** critical
Identifiers: **Message**:Integer Overflow or Wraparound

High:

Vulnerability 3.36

Test-specific ID: SNYK-DEBIAN11-AOM-2309719 **Severity:** high
Identifiers: **Message**:Buffer Overflow

Vulnerability 3.37

Test-specific ID: SNYK-DEBIAN11-AOM-2309736 **Severity:** high
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.38

Test-specific ID: SNYK-DEBIAN11-CURL-1585138 **Severity:** high
Identifiers: **Message**:Cleartext Transmission of Sensitive Information

Vulnerability 3.39

Test-specific ID: SNYK-DEBIAN11-CURL-2804164 **Severity:** high
Identifiers: **Message**:CVE-2022-27775

Vulnerability 3.40

Test-specific ID: SNYK-DEBIAN11-CURL-2805482 **Severity:** high
Identifiers: **Message**:Missing Authentication for Critical Function

Vulnerability 3.41

Test-specific ID: SNYK-DEBIAN11-CURL-2813769 **Severity:** high
Identifiers: **Message**:Improper Certificate Validation

Vulnerability 3.42

Test-specific ID: SNYK-DEBIAN11-CURL-2813773 **Severity:** high
Identifiers: **Message**:Loop with Unreachable Exit Condition ('Infinite Loop')

Vulnerability 3.43

Test-specific ID: SNYK-DEBIAN11-CURL-3066040 **Severity:** high
Identifiers: **Message**:Cleartext Transmission of Sensitive Information

Vulnerability 3.44

Test-specific ID: SNYK-DEBIAN11-CURL-3179181 **Severity:** high
Identifiers: **Message**:Cleartext Transmission of Sensitive Information

Vulnerability 3.45

Test-specific ID: SNYK-DEBIAN11-CURL-3366762 **Severity:** high
Identifiers: **Message**:Directory Traversal

Vulnerability 3.46

Test-specific ID: SNYK-DEBIAN11-CURL-3366772 **Severity:** high
Identifiers: **Message**:Arbitrary Code Injection

Vulnerability 3.47

Test-specific ID: SNYK-DEBIAN11-CYRUSSASL2-2412223 **Severity:** high
Identifiers: **Message**:SQL Injection

Vulnerability 3.48

Test-specific ID: SNYK-DEBIAN11-EXPAT-2329086 **Severity:** high
Identifiers: **Message**:Incorrect Calculation

Vulnerability 3.49

Test-specific ID: SNYK-DEBIAN11-EXPAT-2330887 **Severity:** high
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.50

Test-specific ID: SNYK-DEBIAN11-EXPAT-2331798 **Severity:** high
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.51

Test-specific ID: SNYK-DEBIAN11-EXPAT-2331806 **Severity:** high
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.52

Test-specific ID: SNYK-DEBIAN11-EXPAT-2331819 **Severity:** high
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.53

Test-specific ID: SNYK-DEBIAN11-EXPAT-2384928 **Severity:** high
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.54

Test-specific ID: SNYK-DEBIAN11-EXPAT-2405943 **Severity:** high
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.55

Test-specific ID: SNYK-DEBIAN11-EXPAT-3023031 **Severity:** high
Identifiers: **Message**:Use After Free

Vulnerability 3.56

Test-specific ID: SNYK-DEBIAN11-EXPAT-3061093 **Severity:** high
Identifiers: **Message**:Use After Free

Vulnerability 3.57

Test-specific ID: SNYK-DEBIAN11-FREETYPE-2774654 **Severity:** high
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.58

Test-specific ID: SNYK-DEBIAN11-FREETYPE-2774664 **Severity:** high
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.59

Test-specific ID: SNYK-DEBIAN11-FRIBIDI-2433109 **Severity:** high
Identifiers: **Message**:Stack-based Buffer Overflow

Vulnerability 3.60

Test-specific ID: SNYK-DEBIAN11-GDKPIXBUF-2338604 **Severity:** high
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.61

Test-specific ID: SNYK-DEBIAN11-GDKPIXBUF-2960116 **Severity:** high
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.62

Test-specific ID: SNYK-DEBIAN11-GIT-2635965 **Severity:** high
Identifiers: **Message**:Uncontrolled Search Path Element

Vulnerability 3.63

Test-specific ID: SNYK-DEBIAN11-GIT-2949145 **Severity:** high
Identifiers: **Message**:Improper Ownership Management

Vulnerability 3.64

Test-specific ID: SNYK-DEBIAN11-GIT-3051727 **Severity:** high
Identifiers: **Message**:Heap-based Buffer Overflow

Vulnerability 3.65

Test-specific ID: SNYK-DEBIAN11-GIT-3319756 **Severity:** high
Identifiers: **Message**:Directory Traversal

Vulnerability 3.66

Test-specific ID: SNYK-DEBIAN11-GLIBC-1911968 **Severity:** high
Identifiers: **Message**:CVE-2021-43396

Vulnerability 3.67

Test-specific ID: SNYK-DEBIAN11-GLIBC-2340919 **Severity:** high
Identifiers: **Message**:Off-by-one Error

Vulnerability 3.68

Test-specific ID: SNYK-DEBIAN11-GLIBC-5927133 **Severity:** high
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.69

Test-specific ID: SNYK-DEBIAN11-GNUTLS28-2964220 **Severity:** high
Identifiers: **Message**:Double Free

Vulnerability 3.70

Test-specific ID: SNYK-DEBIAN11-GNUTLS28-3318299 **Severity:** high
Identifiers: **Message**:Information Exposure

Vulnerability 3.71

Test-specific ID: SNYK-DEBIAN11-GZIP-2444256 **Severity:** high
Identifiers: **Message**:Improper Input Validation

Vulnerability 3.72

Test-specific ID: SNYK-DEBIAN11-KRB5-3120880 **Severity:** high
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.73

Test-specific ID: SNYK-DEBIAN11-LIBDE265-1585966 **Severity:** high
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.74

Test-specific ID: SNYK-DEBIAN11-LIBDE265-2359240 **Severity:** high
Identifiers: **Message**:Reachable Assertion

Vulnerability 3.75

Test-specific ID: SNYK-DEBIAN11-LIBDE265-3227414 **Severity:** high
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.76

Test-specific ID: SNYK-DEBIAN11-LIBDE265-3336916 **Severity:** high
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.77

Test-specific ID: SNYK-DEBIAN11-LIBDE265-3342948 **Severity:** high
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.78

Test-specific ID: SNYK-DEBIAN11-LIBDE265-3342951 **Severity:** high
Identifiers: **Message**:Buffer Overflow

Vulnerability 3.79

Test-specific ID: SNYK-DEBIAN11-LIBTIRPC-2959390 **Severity:** high
Identifiers: **Message**:Improper Handling of Exceptional Conditions

Vulnerability 3.80

Test-specific ID: SNYK-DEBIAN11-LIBWEBP-5489177 **Severity:** high
Identifiers: **Message**:Double Free

Vulnerability 3.81

Test-specific ID: SNYK-DEBIAN11-LIBWEBP-5893094 **Severity:** high
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.82

Test-specific ID: SNYK-DEBIAN11-LIBX11-5710893 **Severity:** high
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.83

Test-specific ID: SNYK-DEBIAN11-LIBX11-5927150 **Severity:** high
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.84

Test-specific ID: SNYK-DEBIAN11-LIBXML2-2413974 **Severity:** high
Identifiers: **Message**:Use After Free

Vulnerability 3.85

Test-specific ID: SNYK-DEBIAN11-LIBXML2-3059797 **Severity:** high
Identifiers: **Message**:Double Free

Vulnerability 3.86

Test-specific ID: SNYK-DEBIAN11-LIBXML2-3059801 **Severity:** high
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.87

Test-specific ID: SNYK-DEBIAN11-LIBXSLT-2964230 **Severity:** high
Identifiers: **Message**:Use After Free

Vulnerability 3.88

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2389248 **Severity:** high
Identifiers: **Message**:Use After Free

Vulnerability 3.89

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2396504 **Severity:** high
Identifiers: **Message**:Heap-based Buffer Overflow

Vulnerability 3.90

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2396508 **Severity:** high
Identifiers: **Message**:Use After Free

Vulnerability 3.91

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2396510 **Severity:** high
Identifiers: **Message**:Use of Externally-Controlled Format String

Vulnerability 3.92

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2396518 **Severity:** high
Identifiers: **Message**:Stack-based Buffer Overflow

Vulnerability 3.93

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2766283 **Severity:** high
Identifiers: **Message**:CVE-2022-27446

Vulnerability 3.94

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2766285 **Severity:** high
Identifiers: **Message**:Reachable Assertion

Vulnerability 3.95

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2766288 **Severity:** high
Identifiers: **Message**:CVE-2022-27449

Vulnerability 3.96

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2766292 **Severity:** high
Identifiers: **Message**:Use After Free

Vulnerability 3.97

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2766308 **Severity:** high
Identifiers: **Message**:CVE-2022-27445

Vulnerability 3.98

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2766310 **Severity:** high
Identifiers: **Message**:CVE-2022-27444

Vulnerability 3.99

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2766315 **Severity:** high
Identifiers: **Message**:CVE-2022-27451

Vulnerability 3.100

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2766316 **Severity:** high
Identifiers: **Message**:CVE-2022-27452

Vulnerability 3.101

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2766356 **Severity:** high
Identifiers: **Message**:SQL Injection

Vulnerability 3.102

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2766359 **Severity:** high
Identifiers: **Message**:Use After Free

Vulnerability 3.103

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2766368 **Severity:** high
Identifiers: **Message**:SQL Injection

Vulnerability 3.104

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2766381 **Severity:** high
Identifiers: **Message**:SQL Injection

Vulnerability 3.105

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2766382 **Severity:** high
Identifiers: **Message**:Use After Free

Vulnerability 3.106

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2766385 **Severity:** high
Identifiers: **Message**:SQL Injection

Vulnerability 3.107

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2766386 **Severity:** high
Identifiers: **Message**:Reachable Assertion

Vulnerability 3.108

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2766389 **Severity:** high
Identifiers: **Message**:Use After Free

Vulnerability 3.109

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2766399 **Severity:** high
Identifiers: **Message**:Use After Free

Vulnerability 3.110

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2766407 **Severity:** high
Identifiers: **Message**:SQL Injection

Vulnerability 3.111

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2766416 **Severity:** high
Identifiers: **Message**:Use After Free

Vulnerability 3.112

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2766420 **Severity:** high
Identifiers: **Message**:Use After Free

Vulnerability 3.113

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2766425 **Severity:** high
Identifiers: **Message**:Use After Free

Vulnerability 3.114

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2766429 **Severity:** high
Identifiers: **Message**:SQL Injection

Vulnerability 3.115

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2766432 **Severity:** high
Identifiers: **Message**:Buffer Overflow

Vulnerability 3.116

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2766434 **Severity:** high
Identifiers: **Message**:SQL Injection

Vulnerability 3.117

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2940556 **Severity:** high
Identifiers: **Message**:Use After Free

Vulnerability 3.118

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2940559 **Severity:** high
Identifiers: **Message**:CVE-2022-32086

Vulnerability 3.119

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2940561 **Severity:** high
Identifiers: **Message**:CVE-2022-32087

Vulnerability 3.120

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2940567 **Severity:** high
Identifiers: **Message**:CVE-2022-32088

Vulnerability 3.121

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2940570 **Severity:** high
Identifiers: **Message**:CVE-2022-32089

Vulnerability 3.122

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2940577 **Severity:** high
Identifiers: **Message**:Reachable Assertion

Vulnerability 3.123

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2940579 **Severity:** high
Identifiers: **Message**:CVE-2022-32083

Vulnerability 3.124

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2940587 **Severity:** high
Identifiers: **Message**:CVE-2022-32084

Vulnerability 3.125

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2940588 **Severity:** high
Identifiers: **Message**:Use After Free

Vulnerability 3.126

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2940589 **Severity:** high
Identifiers: **Message**:CVE-2022-32085

Vulnerability 3.127

Test-specific ID: SNYK-DEBIAN11-NCURSES-2767191 **Severity:** high
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.128

Test-specific ID: SNYK-DEBIAN11-NCURSES-5421197 **Severity:** high
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.129

Test-specific ID: SNYK-DEBIAN11-NGHTTP2-5953384 **Severity:** high
Identifiers: **Message**:Resource Exhaustion

Vulnerability 3.130

Test-specific ID: SNYK-DEBIAN11-OPENSSH-1660415 **Severity:** high
Identifiers: **Message**:Improper Privilege Management

Vulnerability 3.131

Test-specific ID: SNYK-DEBIAN11-OPENSSH-6139206 **Severity:** high
Identifiers: **Message**:CVE-2023-51767

Vulnerability 3.132

Test-specific ID: SNYK-DEBIAN11-OPENSSL-2426309 **Severity:** high
Identifiers: **Message**:Loop with Unreachable Exit Condition ('Infinite Loop')

Vulnerability 3.133

Test-specific ID: SNYK-DEBIAN11-OPENSSL-3314584 **Severity:** high
Identifiers: **Message**:Access of Resource Using Incompatible Type ('Type Confusion')

Vulnerability 3.134

Test-specific ID: SNYK-DEBIAN11-OPENSSL-3314604 **Severity:** high
Identifiers: **Message**:Use After Free

Vulnerability 3.135

Test-specific ID: SNYK-DEBIAN11-OPENSSL-3314615 **Severity:** high
Identifiers: **Message**:Double Free

Vulnerability 3.136

Test-specific ID: SNYK-DEBIAN11-OPENSSL-3368735 **Severity:** high
Identifiers: **Message**:Improper Certificate Validation

Vulnerability 3.137

Test-specific ID: SNYK-DEBIAN11-PIXMAN-3099045 **Severity:** high
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.138

Test-specific ID: SNYK-DEBIAN11-POSTGRESQL13-2824086 **Severity:** high
Identifiers: **Message**:Incomplete Cleanup

Vulnerability 3.139

Test-specific ID: SNYK-DEBIAN11-POSTGRESQL13-2980116 **Severity:** high
Identifiers: **Message**:Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')

Vulnerability 3.140

Test-specific ID: SNYK-DEBIAN11-POSTGRESQL13-5519349 **Severity:** high
Identifiers: **Message**:CVE-2023-2454

Vulnerability 3.141

Test-specific ID: SNYK-DEBIAN11-POSTGRESQL13-5838224 **Severity:** high
Identifiers: **Message**:SQL Injection

Vulnerability 3.142

Test-specific ID: SNYK-DEBIAN11-POSTGRESQL13-6055641 **Severity:** high
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.143

Test-specific ID: SNYK-DEBIAN11-SUBVERSION-2635643 **Severity:** high
Identifiers: **Message**:Use After Free

Vulnerability 3.144

Test-specific ID: SNYK-DEBIAN11-TIFF-2420602 **Severity:** high
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.145

Test-specific ID: SNYK-DEBIAN11-TIFF-3113871 **Severity:** high
Identifiers: **Message**:Numeric Errors

Vulnerability 3.146

Test-specific ID: SNYK-DEBIAN11-TIFF-5747600 **Severity:** high
Identifiers: **Message**:Buffer Overflow

Vulnerability 3.147

Test-specific ID: SNYK-DEBIAN11-XZUTILS-2444276 **Severity:** high
Identifiers: **Message**:Improper Input Validation

Vulnerability 3.148

Test-specific ID: SNYK-DEBIAN11-ZLIB-2433933 **Severity:** high
Identifiers: **Message**:Out-of-bounds Write

Medium:

Vulnerability 3.149

Test-specific ID: SNYK-DEBIAN11-AOM-2309717 **Severity:** medium
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.150

Test-specific ID: SNYK-DEBIAN11-AOM-2309727 **Severity:** medium
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.151

Test-specific ID: SNYK-DEBIAN11-APRUTIL-3261250 **Severity:** medium
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.152

Test-specific ID: SNYK-DEBIAN11-BLUEZ-6112466 **Severity:** medium
Identifiers: **Message**:Improper Authentication

Vulnerability 3.153

Test-specific ID: SNYK-DEBIAN11-CURL-1585148 **Severity:** medium
Identifiers: **Message**:Insufficient Verification of Data Authenticity

Vulnerability 3.154

Test-specific ID: SNYK-DEBIAN11-CURL-2804158 **Severity:** medium
Identifiers: **Message**:Insufficiently Protected Credentials

Vulnerability 3.155

Test-specific ID: SNYK-DEBIAN11-CURL-2804167 **Severity:** medium
Identifiers: **Message**:Insufficiently Protected Credentials

Vulnerability 3.156

Test-specific ID: SNYK-DEBIAN11-CURL-2936232 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.157

Test-specific ID: SNYK-DEBIAN11-CURL-2936233 **Severity:** medium
Identifiers: **Message**:Allocation of Resources Without Limits or Throttling

Vulnerability 3.158

Test-specific ID: SNYK-DEBIAN11-CURL-2936235 **Severity:** medium
Identifiers: **Message**:Allocation of Resources Without Limits or Throttling

Vulnerability 3.159

Test-specific ID: SNYK-DEBIAN11-CURL-3179186 **Severity:** medium
Identifiers: **Message**:Use After Free

Vulnerability 3.160

Test-specific ID: SNYK-DEBIAN11-CURL-3320492 **Severity:** medium
Identifiers: **Message**:Cleartext Transmission of Sensitive Information

Vulnerability 3.161

Test-specific ID: SNYK-DEBIAN11-CURL-3320498 **Severity:** medium
Identifiers: **Message**:Allocation of Resources Without Limits or Throttling

Vulnerability 3.162

Test-specific ID: SNYK-DEBIAN11-CURL-3366760 **Severity:** medium
Identifiers: **Message**:Improper Authentication

Vulnerability 3.163

Test-specific ID: SNYK-DEBIAN11-CURL-3366763 **Severity:** medium
Identifiers: **Message**:Improper Authentication

Vulnerability 3.164

Test-specific ID: SNYK-DEBIAN11-CURL-3366765 **Severity:** medium
Identifiers: **Message**:Improper Authentication

Vulnerability 3.165

Test-specific ID: SNYK-DEBIAN11-CURL-5561876 **Severity:** medium
Identifiers: **Message**:Improper Certificate Validation

Vulnerability 3.166

Test-specific ID: SNYK-DEBIAN11-CURL-6100976 **Severity:** medium
Identifiers: **Message**:CVE-2023-46218

Vulnerability 3.167

Test-specific ID: SNYK-DEBIAN11-CURL-6100978 **Severity:** medium
Identifiers: **Message**:Missing Encryption of Sensitive Data

Vulnerability 3.168

Test-specific ID: SNYK-DEBIAN11-EXPAT-2405941 **Severity:** medium
Identifiers: **Message**:Uncontrolled Recursion

Vulnerability 3.169

Test-specific ID: SNYK-DEBIAN11-FILE-5849472 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.170

Test-specific ID: SNYK-DEBIAN11-FRIBIDI-2433110 **Severity:** medium
Identifiers: **Message**:Heap-based Buffer Overflow

Vulnerability 3.171

Test-specific ID: SNYK-DEBIAN11-FRIBIDI-2433114 **Severity:** medium
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.172

Test-specific ID: SNYK-DEBIAN11-GIT-3051720 **Severity:** medium
Identifiers: **Message**:Link Following

Vulnerability 3.173

Test-specific ID: SNYK-DEBIAN11-GIT-3319754 **Severity:** medium
Identifiers: **Message**:Link Following

Vulnerability 3.174

Test-specific ID: SNYK-DEBIAN11-GNUPG2-2939851 **Severity:** medium
Identifiers: **Message**:Arbitrary Code Injection

Vulnerability 3.175

Test-specific ID: SNYK-DEBIAN11-GNUTLS28-2419151 **Severity:** medium
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.176

Test-specific ID: SNYK-DEBIAN11-IMAGEMAGICK-3314439 **Severity:** medium
Identifiers: **Message**:Improper Resource Shutdown or Release

Vulnerability 3.177

Test-specific ID: SNYK-DEBIAN11-IMAGEMAGICK-3314444 **Severity:** medium
Identifiers: **Message**:CVE-2022-44268

Vulnerability 3.178

Test-specific ID: SNYK-DEBIAN11-IMAGEMAGICK-5746983 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.179

Test-specific ID: SNYK-DEBIAN11-IMAGEMAGICK-5933305 **Severity:** medium
Identifiers: **Message**:Use After Free

Vulnerability 3.180

Test-specific ID: SNYK-DEBIAN11-KRB5-5825661 **Severity:** medium
Identifiers: **Message**:Access of Uninitialized Pointer

Vulnerability 3.181

Test-specific ID: SNYK-DEBIAN11-LIBDE265-1585960 **Severity:** medium
Identifiers: **Message**:CVE-2020-21605

Vulnerability 3.182

Test-specific ID: SNYK-DEBIAN11-LIBDE265-1585961 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.183

Test-specific ID: SNYK-DEBIAN11-LIBDE265-1585963 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.184

Test-specific ID: SNYK-DEBIAN11-LIBDE265-1585964 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.185

Test-specific ID: SNYK-DEBIAN11-LIBDE265-1585967 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.186

Test-specific ID: SNYK-DEBIAN11-LIBDE265-1585984 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.187

Test-specific ID: SNYK-DEBIAN11-LIBDE265-1585991 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.188

Test-specific ID: SNYK-DEBIAN11-LIBDE265-1585995 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.189

Test-specific ID: SNYK-DEBIAN11-LIBDE265-1585997 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.190

Test-specific ID: SNYK-DEBIAN11-LIBDE265-1586004 **Severity:** medium
Identifiers: **Message**:Buffer Overflow

Vulnerability 3.191

Test-specific ID: SNYK-DEBIAN11-LIBDE265-1586007 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.192

Test-specific ID: SNYK-DEBIAN11-LIBDE265-1586008 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.193

Test-specific ID: SNYK-DEBIAN11-LIBDE265-2359235 **Severity:** medium
Identifiers: **Message**:Use After Free

Vulnerability 3.194

Test-specific ID: SNYK-DEBIAN11-LIBDE265-2359244 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.195

Test-specific ID: SNYK-DEBIAN11-LIBDE265-2359245 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.196

Test-specific ID: SNYK-DEBIAN11-LIBDE265-2359246 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.197

Test-specific ID: SNYK-DEBIAN11-LIBDE265-3098976 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.198

Test-specific ID: SNYK-DEBIAN11-LIBDE265-3098978 **Severity:** medium
Identifiers: **Message**:CVE-2022-43245

Vulnerability 3.199

Test-specific ID: SNYK-DEBIAN11-LIBDE265-3098979 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.200

Test-specific ID: SNYK-DEBIAN11-LIBDE265-3098986 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.201

Test-specific ID: SNYK-DEBIAN11-LIBDE265-3098990 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.202

Test-specific ID: SNYK-DEBIAN11-LIBDE265-3098995 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.203

Test-specific ID: SNYK-DEBIAN11-LIBDE265-3098997 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.204

Test-specific ID: SNYK-DEBIAN11-LIBDE265-3098999 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.205

Test-specific ID: SNYK-DEBIAN11-LIBDE265-3099002 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.206

Test-specific ID: SNYK-DEBIAN11-LIBDE265-3099003 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.207

Test-specific ID: SNYK-DEBIAN11-LIBDE265-3099006 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.208

Test-specific ID: SNYK-DEBIAN11-LIBDE265-3099011 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.209

Test-specific ID: SNYK-DEBIAN11-LIBDE265-3099012 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.210

Test-specific ID: SNYK-DEBIAN11-LIBDE265-3099021 **Severity:** medium
Identifiers: **Message**:CVE-2022-43238

Vulnerability 3.211

Test-specific ID: SNYK-DEBIAN11-LIBDE265-3099026 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.212

Test-specific ID: SNYK-DEBIAN11-LIBDE265-3099031 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.213

Test-specific ID: SNYK-DEBIAN11-LIBDE265-3336900 **Severity:** medium
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.214

Test-specific ID: SNYK-DEBIAN11-LIBDE265-3336902 **Severity:** medium
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.215

Test-specific ID: SNYK-DEBIAN11-LIBDE265-3336903 **Severity:** medium
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.216

Test-specific ID: SNYK-DEBIAN11-LIBDE265-3336908 **Severity:** medium
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.217

Test-specific ID: SNYK-DEBIAN11-LIBDE265-3336909 **Severity:** medium
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.218

Test-specific ID: SNYK-DEBIAN11-LIBDE265-3336912 **Severity:** medium
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.219

Test-specific ID: SNYK-DEBIAN11-LIBDE265-3336917 **Severity:** medium
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.220

Test-specific ID: SNYK-DEBIAN11-LIBRSVG-5802977 **Severity:** medium
Identifiers: **Message**:Directory Traversal

Vulnerability 3.221

Test-specific ID: SNYK-DEBIAN11-LIBX11-5927151 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.222

Test-specific ID: SNYK-DEBIAN11-LIBX11-5927154 **Severity:** medium
Identifiers: **Message**:Loop with Unreachable Exit Condition ('Infinite Loop')

Vulnerability 3.223

Test-specific ID: SNYK-DEBIAN11-LIBXML2-2806812 **Severity:** medium
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.224

Test-specific ID: SNYK-DEBIAN11-LIBXML2-5423817 **Severity:** medium
Identifiers: **Message**:Double Free

Vulnerability 3.225

Test-specific ID: SNYK-DEBIAN11-LIBXML2-5423819 **Severity:** medium
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.226

Test-specific ID: SNYK-DEBIAN11-MARIADB105-1924613 **Severity:** medium
Identifiers: **Message**:CVE-2021-35604

Vulnerability 3.227

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2388609 **Severity:** medium
Identifiers: **Message**:CVE-2021-46659

Vulnerability 3.228

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2389246 **Severity:** medium
Identifiers: **Message**:CVE-2021-46663

Vulnerability 3.229

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2389259 **Severity:** medium
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.230

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2389263 **Severity:** medium
Identifiers: **Message**:CVE-2021-46662

Vulnerability 3.231

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2389276 **Severity:** medium
Identifiers: **Message**:Resource Exhaustion

Vulnerability 3.232

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2389278 **Severity:** medium
Identifiers: **Message**:CVE-2021-46661

Vulnerability 3.233

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2389279 **Severity:** medium
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.234

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2389297 **Severity:** medium
Identifiers: **Message**:CVE-2021-46665

Vulnerability 3.235

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2848384 **Severity:** medium
Identifiers: **Message**:Improper Locking

Vulnerability 3.236

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2848388 **Severity:** medium
Identifiers: **Message**:Improper Locking

Vulnerability 3.237

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2848393 **Severity:** medium
Identifiers: **Message**:Improper Locking

Vulnerability 3.238

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2848395 **Severity:** medium
Identifiers: **Message**:Improper Locking

Vulnerability 3.239

Test-specific ID: SNYK-DEBIAN11-MARIADB105-2994376 **Severity:** medium
Identifiers: **Message**:Improper Locking

Vulnerability 3.240

Test-specific ID: SNYK-DEBIAN11-MARIADB105-3325557 **Severity:** medium
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.241

Test-specific ID: SNYK-DEBIAN11-OPENEXR-1300562 **Severity:** medium
Identifiers: **Message**:Integer Underflow

Vulnerability 3.242

Test-specific ID: SNYK-DEBIAN11-OPENEXR-1300568 **Severity:** medium
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.243

Test-specific ID: SNYK-DEBIAN11-OPENEXR-1304909 **Severity:** medium
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.244

Test-specific ID: SNYK-DEBIAN11-OPENEXR-1310951 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.245

Test-specific ID: SNYK-DEBIAN11-OPENEXR-1913908 **Severity:** medium
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.246

Test-specific ID: SNYK-DEBIAN11-OPENEXR-1913915 **Severity:** medium
Identifiers: **Message**:Divide By Zero

Vulnerability 3.247

Test-specific ID: SNYK-DEBIAN11-OPENEXR-2329539 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.248

Test-specific ID: SNYK-DEBIAN11-OPENSSH-6130525 **Severity:** medium
Identifiers: **Message**:OS Command Injection

Vulnerability 3.249

Test-specific ID: SNYK-DEBIAN11-OPENSSH-6130527 **Severity:** medium
Identifiers: **Message**:Improper Validation of Integrity Check Value

Vulnerability 3.250

Test-specific ID: SNYK-DEBIAN11-OPENSSL-2388380 **Severity:** medium
Identifiers: **Message**:CVE-2021-4160

Vulnerability 3.251

Test-specific ID: SNYK-DEBIAN11-OPENSSL-2941242 **Severity:** medium
Identifiers: **Message**:Use of a Broken or Risky Cryptographic Algorithm

Vulnerability 3.252

Test-specific ID: SNYK-DEBIAN11-OPENSSL-3314592 **Severity:** medium
Identifiers: **Message**:Information Exposure

Vulnerability 3.253

Test-specific ID: SNYK-DEBIAN11-OPENSSL-5291773 **Severity:** medium
Identifiers: **Message**:Improper Certificate Validation

Vulnerability 3.254

Test-specific ID: SNYK-DEBIAN11-OPENSSL-5291777 **Severity:** medium
Identifiers: **Message**:Improper Certificate Validation

Vulnerability 3.255

Test-specific ID: SNYK-DEBIAN11-OPENSSL-5661566 **Severity:** medium
Identifiers: **Message**:Allocation of Resources Without Limits or Throttling

Vulnerability 3.256

Test-specific ID: SNYK-DEBIAN11-OPENSSL-5788324 **Severity:** medium
Identifiers: **Message**:Inefficient Regular Expression Complexity

Vulnerability 3.257

Test-specific ID: SNYK-DEBIAN11-OPENSSL-5812634 **Severity:** medium
Identifiers: **Message**:Excessive Iteration

Vulnerability 3.258

Test-specific ID: SNYK-DEBIAN11-POSTGRESQL13-5519351 **Severity:** medium
Identifiers: **Message**:CVE-2023-2455

Vulnerability 3.259

Test-specific ID: SNYK-DEBIAN11-POSTGRESQL13-6055638 **Severity:** medium
Identifiers: **Message**:CVE-2023-5868

Vulnerability 3.260

Test-specific ID: SNYK-DEBIAN11-POSTGRESQL13-6055648 **Severity:** medium
Identifiers: **Message**:CVE-2023-5870

Vulnerability 3.261

Test-specific ID: SNYK-DEBIAN11-PYTHON39-5861805 **Severity:** medium
Identifiers: **Message**:CVE-2023-40217

Vulnerability 3.262

Test-specific ID: SNYK-DEBIAN11-SUBVERSION-2635645 **Severity:** medium
Identifiers: **Message**:Information Exposure

Vulnerability 3.263

Test-specific ID: SNYK-DEBIAN11-SYSTEMD-2332025 **Severity:** medium
Identifiers: **Message**:Uncontrolled Recursion

Vulnerability 3.264

Test-specific ID: SNYK-DEBIAN11-SYSTEMD-3111119 **Severity:** medium
Identifiers: **Message**:Off-by-one Error

Vulnerability 3.265

Test-specific ID: SNYK-DEBIAN11-SYSTEMD-3177742 **Severity:** medium
Identifiers: **Message**:CVE-2022-4415

Vulnerability 3.266

Test-specific ID: SNYK-DEBIAN11-TIFF-2331931 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.267

Test-specific ID: SNYK-DEBIAN11-TIFF-2399969 **Severity:** medium
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.268

Test-specific ID: SNYK-DEBIAN11-TIFF-2399973 **Severity:** medium
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.269

Test-specific ID: SNYK-DEBIAN11-TIFF-2419111 **Severity:** medium
Identifiers: **Message**:Reachable Assertion

Vulnerability 3.270

Test-specific ID: SNYK-DEBIAN11-TIFF-2421376 **Severity:** medium
Identifiers: **Message**:Unchecked Return Value

Vulnerability 3.271

Test-specific ID: SNYK-DEBIAN11-TIFF-2421380 **Severity:** medium
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.272

Test-specific ID: SNYK-DEBIAN11-TIFF-2421384 **Severity:** medium
Identifiers: **Message**:Divide By Zero

Vulnerability 3.273

Test-specific ID: SNYK-DEBIAN11-TIFF-2421389 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.274

Test-specific ID: SNYK-DEBIAN11-TIFF-2774162 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.275

Test-specific ID: SNYK-DEBIAN11-TIFF-2774167 **Severity:** medium
Identifiers: **Message**:Stack-based Buffer Overflow

Vulnerability 3.276

Test-specific ID: SNYK-DEBIAN11-TIFF-2823289 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.277

Test-specific ID: SNYK-DEBIAN11-TIFF-2823291 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.278

Test-specific ID: SNYK-DEBIAN11-TIFF-2938519 **Severity:** medium
Identifiers: **Message**:Divide By Zero

Vulnerability 3.279

Test-specific ID: SNYK-DEBIAN11-TIFF-2938520 **Severity:** medium
Identifiers: **Message**:Divide By Zero

Vulnerability 3.280

Test-specific ID: SNYK-DEBIAN11-TIFF-2938525 **Severity:** medium
Identifiers: **Message**:Divide By Zero

Vulnerability 3.281

Test-specific ID: SNYK-DEBIAN11-TIFF-2964237 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.282

Test-specific ID: SNYK-DEBIAN11-TIFF-2987009 **Severity:** medium
Identifiers: **Message**:Integer Underflow

Vulnerability 3.283

Test-specific ID: SNYK-DEBIAN11-TIFF-2987011 **Severity:** medium
Identifiers: **Message**:Integer Underflow

Vulnerability 3.284

Test-specific ID: SNYK-DEBIAN11-TIFF-2987014 **Severity:** medium
Identifiers: **Message**:Improper Validation of Specified Quantity in Input

Vulnerability 3.285

Test-specific ID: SNYK-DEBIAN11-TIFF-3008946 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.286

Test-specific ID: SNYK-DEBIAN11-TIFF-3012393 **Severity:** medium
Identifiers: **Message**:Double Free

Vulnerability 3.287

Test-specific ID: SNYK-DEBIAN11-TIFF-3012398 **Severity:** medium
Identifiers: **Message**:Incorrect Calculation of Buffer Size

Vulnerability 3.288

Test-specific ID: SNYK-DEBIAN11-TIFF-3012399 **Severity:** medium
Identifiers: **Message**:Release of Invalid Pointer or Reference

Vulnerability 3.289

Test-specific ID: SNYK-DEBIAN11-TIFF-3058771 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.290

Test-specific ID: SNYK-DEBIAN11-TIFF-3058775 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.291

Test-specific ID: SNYK-DEBIAN11-TIFF-3058778 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.292

Test-specific ID: SNYK-DEBIAN11-TIFF-3058779 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.293

Test-specific ID: SNYK-DEBIAN11-TIFF-3058787 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.294

Test-specific ID: SNYK-DEBIAN11-TIFF-3058792 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.295

Test-specific ID: SNYK-DEBIAN11-TIFF-3244453 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.296

Test-specific ID: SNYK-DEBIAN11-TIFF-3319790 **Severity:** medium
Identifiers: **Message**:Use After Free

Vulnerability 3.297

Test-specific ID: SNYK-DEBIAN11-TIFF-3319791 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.298

Test-specific ID: SNYK-DEBIAN11-TIFF-3319804 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.299

Test-specific ID: SNYK-DEBIAN11-TIFF-3319810 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.300

Test-specific ID: SNYK-DEBIAN11-TIFF-3319811 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.301

Test-specific ID: SNYK-DEBIAN11-TIFF-3319813 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.302

Test-specific ID: SNYK-DEBIAN11-TIFF-3319814 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.303

Test-specific ID: SNYK-DEBIAN11-TIFF-3319820 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.304

Test-specific ID: SNYK-DEBIAN11-TIFF-3319824 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.305

Test-specific ID: SNYK-DEBIAN11-TIFF-3319826 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.306

Test-specific ID: SNYK-DEBIAN11-TIFF-3339158 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.307

Test-specific ID: SNYK-DEBIAN11-TIFF-5425902 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.308

Test-specific ID: SNYK-DEBIAN11-TIFF-5518072 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.309

Test-specific ID: SNYK-DEBIAN11-TIFF-5747608 **Severity:** medium
Identifiers: **Message**:Buffer Overflow

Vulnerability 3.310

Test-specific ID: SNYK-DEBIAN11-TIFF-5862860 **Severity:** medium
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.311

Test-specific ID: SNYK-DEBIAN11-TIFF-5862861 **Severity:** medium
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.312

Test-specific ID: SNYK-DEBIAN11-TIFF-5934951 **Severity:** medium
Identifiers: **Message**:Memory Leak

Vulnerability 3.313

Test-specific ID: SNYK-DEBIAN11-UNZIP-2396444 **Severity:** medium
Identifiers: **Message**:CVE-2022-0530

Vulnerability 3.314

Test-specific ID: SNYK-DEBIAN11-UNZIP-2396445 **Severity:** medium
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.315

Test-specific ID: SNYK-DEBIAN11-UTILLINUX-2359396 **Severity:** medium
Identifiers: **Message**:Files or Directories Accessible to External Parties

Vulnerability 3.316

Test-specific ID: SNYK-DEBIAN11-UTILLINUX-2359400 **Severity:** medium
Identifiers: **Message**:Files or Directories Accessible to External Parties

Low:

Vulnerability 3.317

Test-specific ID: SNYK-DEBIAN11-AOM-1085722 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.318

Test-specific ID: SNYK-DEBIAN11-AOM-6140325 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.319

Test-specific ID: SNYK-DEBIAN11-APT-522585 **Severity:** low
Identifiers: **Message**:Improper Verification of Cryptographic Signature

Vulnerability 3.320

Test-specific ID: SNYK-DEBIAN11-BASH-3112361 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.321

Test-specific ID: SNYK-DEBIAN11-BINUTILS-1054596 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.322

Test-specific ID: SNYK-DEBIAN11-BINUTILS-1065551 **Severity:** low
Identifiers: **Message**:Link Following

Vulnerability 3.323

Test-specific ID: SNYK-DEBIAN11-BINUTILS-1086496 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.324

Test-specific ID: SNYK-DEBIAN11-BINUTILS-1292158 **Severity:** low
Identifiers: **Message**:Uncontrolled Recursion

Vulnerability 3.325

Test-specific ID: SNYK-DEBIAN11-BINUTILS-1296883 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.326

Test-specific ID: SNYK-DEBIAN11-BINUTILS-2321369 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.327

Test-specific ID: SNYK-DEBIAN11-BINUTILS-2341553 **Severity:** low
Identifiers: **Message**:Uncontrolled Recursion

Vulnerability 3.328

Test-specific ID: SNYK-DEBIAN11-BINUTILS-2993560 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.329

Test-specific ID: SNYK-DEBIAN11-BINUTILS-3041902 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.330

Test-specific ID: SNYK-DEBIAN11-BINUTILS-3172914 **Severity:** low
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.331

Test-specific ID: SNYK-DEBIAN11-BINUTILS-522743 **Severity:** low
Identifiers: **Message**:Uncontrolled Recursion

Vulnerability 3.332

Test-specific ID: SNYK-DEBIAN11-BINUTILS-523191 **Severity:** low
Identifiers: **Message**:Allocation of Resources Without Limits or Throttling

Vulnerability 3.333

Test-specific ID: SNYK-DEBIAN11-BINUTILS-525795 **Severity:** low
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.334

Test-specific ID: SNYK-DEBIAN11-BINUTILS-527784 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.335

Test-specific ID: SNYK-DEBIAN11-BINUTILS-528223 **Severity:** low
Identifiers: **Message**:Improper Input Validation

Vulnerability 3.336

Test-specific ID: SNYK-DEBIAN11-BINUTILS-529902 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.337

Test-specific ID: SNYK-DEBIAN11-BINUTILS-5416281 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.338

Test-specific ID: SNYK-DEBIAN11-BINUTILS-5422223 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.339

Test-specific ID: SNYK-DEBIAN11-BINUTILS-5803140 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.340

Test-specific ID: SNYK-DEBIAN11-BINUTILS-5853670 **Severity:** low
Identifiers: **Message**:Memory Leak

Vulnerability 3.341

Test-specific ID: SNYK-DEBIAN11-BINUTILS-5853671 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.342

Test-specific ID: SNYK-DEBIAN11-BINUTILS-5853674 **Severity:** low
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.343

Test-specific ID: SNYK-DEBIAN11-BINUTILS-5853682 **Severity:** low
Identifiers: **Message**:Resource Exhaustion

Vulnerability 3.344

Test-specific ID: SNYK-DEBIAN11-BINUTILS-5853683 **Severity:** low
Identifiers: **Message**:Reachable Assertion

Vulnerability 3.345

Test-specific ID: SNYK-DEBIAN11-BINUTILS-5853688 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.346

Test-specific ID: SNYK-DEBIAN11-BINUTILS-5853695 **Severity:** low
Identifiers: **Message**:Memory Leak

Vulnerability 3.347

Test-specific ID: SNYK-DEBIAN11-BINUTILS-5853709 **Severity:** low
Identifiers: **Message**:CVE-2022-47695

Vulnerability 3.348

Test-specific ID: SNYK-DEBIAN11-BINUTILS-5853710 **Severity:** low
Identifiers: **Message**:Memory Leak

Vulnerability 3.349

Test-specific ID: SNYK-DEBIAN11-BINUTILS-5853712 **Severity:** low
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.350

Test-specific ID: SNYK-DEBIAN11-BINUTILS-5853726 **Severity:** low
Identifiers: **Message**:Memory Leak

Vulnerability 3.351

Test-specific ID: SNYK-DEBIAN11-BINUTILS-5853727 **Severity:** low
Identifiers: **Message**:CVE-2022-47696

Vulnerability 3.352

Test-specific ID: SNYK-DEBIAN11-BINUTILS-5853734 **Severity:** low
Identifiers: **Message**:Allocation of Resources Without Limits or Throttling

Vulnerability 3.353

Test-specific ID: SNYK-DEBIAN11-BINUTILS-5853737 **Severity:** low
Identifiers: **Message**:Memory Leak

Vulnerability 3.354

Test-specific ID: SNYK-DEBIAN11-BINUTILS-5858434 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.355

Test-specific ID: SNYK-DEBIAN11-BINUTILS-5862063 **Severity:** low
Identifiers: **Message**:CVE-2020-19726

Vulnerability 3.356

Test-specific ID: SNYK-DEBIAN11-BINUTILS-5903050 **Severity:** low
Identifiers: **Message**:Use of Uninitialized Resource

Vulnerability 3.357

Test-specific ID: SNYK-DEBIAN11-BINUTILS-5903055 **Severity:** low
Identifiers: **Message**:Use of Uninitialized Resource

Vulnerability 3.358

Test-specific ID: SNYK-DEBIAN11-BINUTILS-5903056 **Severity:** low
Identifiers: **Message**:Use of Uninitialized Resource

Vulnerability 3.359

Test-specific ID: SNYK-DEBIAN11-BINUTILS-5903065 **Severity:** low
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.360

Test-specific ID: SNYK-DEBIAN11-BLUEZ-1534589 **Severity:** low
Identifiers: **Message**:Incorrect Authorization

Vulnerability 3.361

Test-specific ID: SNYK-DEBIAN11-BLUEZ-1911958 **Severity:** low
Identifiers: **Message**:Use After Free

Vulnerability 3.362

Test-specific ID: SNYK-DEBIAN11-BLUEZ-1920810 **Severity:** low
Identifiers: **Message**:Resource Exhaustion

Vulnerability 3.363

Test-specific ID: SNYK-DEBIAN11-BLUEZ-2340902 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.364

Test-specific ID: SNYK-DEBIAN11-BLUEZ-3014388 **Severity:** low
Identifiers: **Message**:CVE-2022-39176

Vulnerability 3.365

Test-specific ID: SNYK-DEBIAN11-BLUEZ-3014391 **Severity:** low
Identifiers: **Message**:CVE-2022-39177

Vulnerability 3.366

Test-specific ID: SNYK-DEBIAN11-BLUEZ-518769 **Severity:** low
Identifiers: **Message**:Use After Free

Vulnerability 3.367

Test-specific ID: SNYK-DEBIAN11-BLUEZ-520206 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.368

Test-specific ID: SNYK-DEBIAN11-BLUEZ-522081 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.369

Test-specific ID: SNYK-DEBIAN11-BLUEZ-522178 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.370

Test-specific ID: SNYK-DEBIAN11-BLUEZ-522296 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.371

Test-specific ID: SNYK-DEBIAN11-BLUEZ-526253 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.372

Test-specific ID: SNYK-DEBIAN11-BLUEZ-529128 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.373

Test-specific ID: SNYK-DEBIAN11-BLUEZ-530051 **Severity:** low
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.374

Test-specific ID: SNYK-DEBIAN11-BLUEZ-531504 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.375

Test-specific ID: SNYK-DEBIAN11-BLUEZ-533160 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.376

Test-specific ID: SNYK-DEBIAN11-CAIRO-515907 **Severity:** low
Identifiers: **Message**:Loop with Unreachable Exit Condition ('Infinite Loop')

Vulnerability 3.377

Test-specific ID: SNYK-DEBIAN11-CAIRO-517926 **Severity:** low
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.378

Test-specific ID: SNYK-DEBIAN11-CAIRO-525337 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.379

Test-specific ID: SNYK-DEBIAN11-CAIRO-530691 **Severity:** low
Identifiers: **Message**:Reachable Assertion

Vulnerability 3.380

Test-specific ID: SNYK-DEBIAN11-COREUTILS-514776 **Severity:** low
Identifiers: **Message**:Improper Input Validation

Vulnerability 3.381

Test-specific ID: SNYK-DEBIAN11-COREUTILS-527269 **Severity:** low
Identifiers: **Message**:Race Condition

Vulnerability 3.382

Test-specific ID: SNYK-DEBIAN11-CURL-1296884 **Severity:** low
Identifiers: **Message**:Missing Initialization of Resource

Vulnerability 3.383

Test-specific ID: SNYK-DEBIAN11-CURL-1322658 **Severity:** low
Identifiers: **Message**:Use of Incorrectly-Resolved Name or Reference

Vulnerability 3.384

Test-specific ID: SNYK-DEBIAN11-CURL-1322659 **Severity:** low
Identifiers: **Message**:Insufficiently Protected Credentials

Vulnerability 3.385

Test-specific ID: SNYK-DEBIAN11-CURL-1322667 **Severity:** low
Identifiers: **Message**:Improper Validation of Integrity Check Value

Vulnerability 3.386

Test-specific ID: SNYK-DEBIAN11-CURL-3012384 **Severity:** low
Identifiers: **Message**:CVE-2022-35252

Vulnerability 3.387

Test-specific ID: SNYK-DEBIAN11-CURL-5561869 **Severity:** low
Identifiers: **Message**:Race Condition

Vulnerability 3.388

Test-specific ID: SNYK-DEBIAN11-CURL-5561885 **Severity:** low
Identifiers: **Message**:CVE-2023-28322

Vulnerability 3.389

Test-specific ID: SNYK-DEBIAN11-CURL-5955029 **Severity:** low
Identifiers: **Message**:CVE-2023-38546

Vulnerability 3.390

Test-specific ID: SNYK-DEBIAN11-DAV1D-5518049 **Severity:** low
Identifiers: **Message**:Race Condition

Vulnerability 3.391

Test-specific ID: SNYK-DEBIAN11-DB53-2825168 **Severity:** low
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.392

Test-specific ID: SNYK-DEBIAN11-DJVULIBRE-5858452 **Severity:** low
Identifiers: **Message**:Divide By Zero

Vulnerability 3.393

Test-specific ID: SNYK-DEBIAN11-DJVULIBRE-5858455 **Severity:** low
Identifiers: **Message**:Divide By Zero

Vulnerability 3.394

Test-specific ID: SNYK-DEBIAN11-E2FSPROGS-2628459 **Severity:** low
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.395

Test-specific ID: SNYK-DEBIAN11-ELFUTILS-5803145 **Severity:** low
Identifiers: **Message**:Loop with Unreachable Exit Condition ('Infinite Loop')

Vulnerability 3.396

Test-specific ID: SNYK-DEBIAN11-EXPAT-524217 **Severity:** low
Identifiers: **Message**:XML External Entity (XXE) Injection

Vulnerability 3.397

Test-specific ID: SNYK-DEBIAN11-FREETYPE-2848681 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.398

Test-specific ID: SNYK-DEBIAN11-GCC10-5901313 **Severity:** low
Identifiers: **Message**:CVE-2023-4039

Vulnerability 3.399

Test-specific ID: SNYK-DEBIAN11-GCC9-5901306 **Severity:** low
Identifiers: **Message**:CVE-2023-4039

Vulnerability 3.400

Test-specific ID: SNYK-DEBIAN11-GDKPIXBUF-6207389 **Severity:** low
Identifiers: **Message**:CVE-2022-48622

Vulnerability 3.401

Test-specific ID: SNYK-DEBIAN11-GIT-2399903 **Severity:** low
Identifiers: **Message**:Exposure of Resource to Wrong Sphere

Vulnerability 3.402

Test-specific ID: SNYK-DEBIAN11-GIT-514769 **Severity:** low
Identifiers: **Message**:Improper Input Validation

Vulnerability 3.403

Test-specific ID: SNYK-DEBIAN11-GIT-5461943 **Severity:** low
Identifiers: **Message**:Arbitrary Code Injection

Vulnerability 3.404

Test-specific ID: SNYK-DEBIAN11-GIT-5461949 **Severity:** low
Identifiers: **Message**:Directory Traversal

Vulnerability 3.405

Test-specific ID: SNYK-DEBIAN11-GIT-5461951 **Severity:** low
Identifiers: **Message**:Use of Externally-Controlled Format String

Vulnerability 3.406

Test-specific ID: SNYK-DEBIAN11-GLIB20-518210 **Severity:** low
Identifiers: **Message**:Cryptographic Issues

Vulnerability 3.407

Test-specific ID: SNYK-DEBIAN11-GLIB20-5670987 **Severity:** low
Identifiers: **Message**:Resource Exhaustion

Vulnerability 3.408

Test-specific ID: SNYK-DEBIAN11-GLIB20-5670989 **Severity:** low
Identifiers: **Message**:Deserialization of Untrusted Data

Vulnerability 3.409

Test-specific ID: SNYK-DEBIAN11-GLIB20-5670995 **Severity:** low
Identifiers: **Message**:Resource Exhaustion

Vulnerability 3.410

Test-specific ID: SNYK-DEBIAN11-GLIBC-521063 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.411

Test-specific ID: SNYK-DEBIAN11-GLIBC-521199 **Severity:** low
Identifiers: **Message**:Uncontrolled Recursion

Vulnerability 3.412

Test-specific ID: SNYK-DEBIAN11-GLIBC-522385 **Severity:** low
Identifiers: **Message**:Use of Insufficiently Random Values

Vulnerability 3.413

Test-specific ID: SNYK-DEBIAN11-GLIBC-529848 **Severity:** low
Identifiers: **Message**:Information Exposure

Vulnerability 3.414

Test-specific ID: SNYK-DEBIAN11-GLIBC-531451 **Severity:** low
Identifiers: **Message**:CVE-2019-1010023

Vulnerability 3.415

Test-specific ID: SNYK-DEBIAN11-GLIBC-531492 **Severity:** low
Identifiers: **Message**:Uncontrolled Recursion

Vulnerability 3.416

Test-specific ID: SNYK-DEBIAN11-GLIBC-532215 **Severity:** low
Identifiers: **Message**:Resource Management Errors

Vulnerability 3.417

Test-specific ID: SNYK-DEBIAN11-GLIBC-5894105 **Severity:** low
Identifiers: **Message**:Use After Free

Vulnerability 3.418

Test-specific ID: SNYK-DEBIAN11-GLIBC-5894112 **Severity:** low
Identifiers: **Message**:Use After Free

Vulnerability 3.419

Test-specific ID: SNYK-DEBIAN11-GNUPG2-3330745 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.420

Test-specific ID: SNYK-DEBIAN11-GNUTLS28-515971 **Severity:** low
Identifiers: **Message**:Improper Input Validation

Vulnerability 3.421

Test-specific ID: SNYK-DEBIAN11-GNUTLS28-6062102 **Severity:** low
Identifiers: **Message**:Information Exposure

Vulnerability 3.422

Test-specific ID: SNYK-DEBIAN11-GNUTLS28-6159417 **Severity:** low
Identifiers: **Message**:Improper Verification of Cryptographic Signature

Vulnerability 3.423

Test-specific ID: SNYK-DEBIAN11-HARFBUZZ-2934730 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.424

Test-specific ID: SNYK-DEBIAN11-HARFBUZZ-3311295 **Severity:** low
Identifiers: **Message**:Allocation of Resources Without Limits or Throttling

Vulnerability 3.425

Test-specific ID: SNYK-DEBIAN11-IMAGEMAGICK-1075500 **Severity:** low
Identifiers: **Message**:Divide By Zero

Vulnerability 3.426

Test-specific ID: SNYK-DEBIAN11-IMAGEMAGICK-1075505 **Severity:** low
Identifiers: **Message**:Divide By Zero

Vulnerability 3.427

Test-specific ID: SNYK-DEBIAN11-IMAGEMAGICK-1075508 **Severity:** low
Identifiers: **Message**:Divide By Zero

Vulnerability 3.428

Test-specific ID: SNYK-DEBIAN11-IMAGEMAGICK-1078460 **Severity:** low
Identifiers: **Message**:Divide By Zero

Vulnerability 3.429

Test-specific ID: SNYK-DEBIAN11-IMAGEMAGICK-1085782 **Severity:** low
Identifiers: **Message**:Divide By Zero

Vulnerability 3.430

Test-specific ID: SNYK-DEBIAN11-IMAGEMAGICK-1244104 **Severity:** low
Identifiers: **Message**:Divide By Zero

Vulnerability 3.431

Test-specific ID: SNYK-DEBIAN11-IMAGEMAGICK-1246262 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.432

Test-specific ID: SNYK-DEBIAN11-IMAGEMAGICK-1246513 **Severity:** low
Identifiers: **Message**:Information Exposure

Vulnerability 3.433

Test-specific ID: SNYK-DEBIAN11-IMAGEMAGICK-1247328 **Severity:** low
Identifiers: **Message**:Divide By Zero

Vulnerability 3.434

Test-specific ID: SNYK-DEBIAN11-IMAGEMAGICK-1312915 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.435

Test-specific ID: SNYK-DEBIAN11-IMAGEMAGICK-1584525 **Severity:** low
Identifiers: **Message**:Exposure of Resource to Wrong Sphere

Vulnerability 3.436

Test-specific ID: SNYK-DEBIAN11-IMAGEMAGICK-2431244 **Severity:** low
Identifiers: **Message**:Improper Input Validation

Vulnerability 3.437

Test-specific ID: SNYK-DEBIAN11-IMAGEMAGICK-2441371 **Severity:** low
Identifiers: **Message**:Use After Free

Vulnerability 3.438

Test-specific ID: SNYK-DEBIAN11-IMAGEMAGICK-2441374 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.439

Test-specific ID: SNYK-DEBIAN11-IMAGEMAGICK-2812515 **Severity:** low
Identifiers: **Message**:Buffer Overflow

Vulnerability 3.440

Test-specific ID: SNYK-DEBIAN11-IMAGEMAGICK-2928981 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.441

Test-specific ID: SNYK-DEBIAN11-IMAGEMAGICK-2928984 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.442

Test-specific ID: SNYK-DEBIAN11-IMAGEMAGICK-2928988 **Severity:** low
Identifiers: **Message**:Incorrect Type Conversion or Cast

Vulnerability 3.443

Test-specific ID: SNYK-DEBIAN11-IMAGEMAGICK-3008094 **Severity:** low
Identifiers: **Message**:Memory Leak

Vulnerability 3.444

Test-specific ID: SNYK-DEBIAN11-IMAGEMAGICK-3027309 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.445

Test-specific ID: SNYK-DEBIAN11-IMAGEMAGICK-3358956 **Severity:** low
Identifiers: **Message**:Improper Input Validation

Vulnerability 3.446

Test-specific ID: SNYK-DEBIAN11-IMAGEMAGICK-517389 **Severity:** low
Identifiers: **Message**:CVE-2005-0406

Vulnerability 3.447

Test-specific ID: SNYK-DEBIAN11-IMAGEMAGICK-517989 **Severity:** low
Identifiers: **Message**:Resource Management Errors

Vulnerability 3.448

Test-specific ID: SNYK-DEBIAN11-IMAGEMAGICK-524566 **Severity:** low
Identifiers: **Message**:Missing Release of Resource after Effective Lifetime

Vulnerability 3.449

Test-specific ID: SNYK-DEBIAN11-IMAGEMAGICK-524567 **Severity:** low
Identifiers: **Message**:Resource Exhaustion

Vulnerability 3.450

Test-specific ID: SNYK-DEBIAN11-IMAGEMAGICK-527684 **Severity:** low
Identifiers: **Message**:Missing Release of Resource after Effective Lifetime

Vulnerability 3.451

Test-specific ID: SNYK-DEBIAN11-IMAGEMAGICK-527794 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.452

Test-specific ID: SNYK-DEBIAN11-IMAGEMAGICK-530647 **Severity:** low
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.453

Test-specific ID: SNYK-DEBIAN11-IMAGEMAGICK-5421093 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.454

Test-specific ID: SNYK-DEBIAN11-IMAGEMAGICK-5591138 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.455

Test-specific ID: SNYK-DEBIAN11-IMAGEMAGICK-5660572 **Severity:** low
Identifiers: **Message**:OS Command Injection

Vulnerability 3.456

Test-specific ID: SNYK-DEBIAN11-IMAGEMAGICK-5660609 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.457

Test-specific ID: SNYK-DEBIAN11-IMAGEMAGICK-5707517 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.458

Test-specific ID: SNYK-DEBIAN11-IMAGEMAGICK-5858556 **Severity:** low
Identifiers: **Message**:Divide By Zero

Vulnerability 3.459

Test-specific ID: SNYK-DEBIAN11-JBIGKIT-514977 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.460

Test-specific ID: SNYK-DEBIAN11-KRB5-524883 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.461

Test-specific ID: SNYK-DEBIAN11-LIBDE265-3361564 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.462

Test-specific ID: SNYK-DEBIAN11-LIBDE265-3361568 **Severity:** low
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.463

Test-specific ID: SNYK-DEBIAN11-LIBDE265-6062369 **Severity:** low
Identifiers: **Message**:Buffer Overflow

Vulnerability 3.464

Test-specific ID: SNYK-DEBIAN11-LIBDE265-6070698 **Severity:** low
Identifiers: **Message**:Buffer Overflow

Vulnerability 3.465

Test-specific ID: SNYK-DEBIAN11-LIBDE265-6105344 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.466

Test-specific ID: SNYK-DEBIAN11-LIBDE265-6105346 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.467

Test-specific ID: SNYK-DEBIAN11-LIBDE265-6105352 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.468

Test-specific ID: SNYK-DEBIAN11-LIBGCRYPT20-1297892 **Severity:** low
Identifiers: **Message**:Information Exposure

Vulnerability 3.469

Test-specific ID: SNYK-DEBIAN11-LIBGCRYPT20-523947 **Severity:** low
Identifiers: **Message**:Use of a Broken or Risky Cryptographic Algorithm

Vulnerability 3.470

Test-specific ID: SNYK-DEBIAN11-LIBHEIF-3331227 **Severity:** low
Identifiers: **Message**:Buffer Overflow

Vulnerability 3.471

Test-specific ID: SNYK-DEBIAN11-LIBHEIF-5498470 **Severity:** low
Identifiers: **Message**:Divide By Zero

Vulnerability 3.472

Test-specific ID: SNYK-DEBIAN11-LIBHEIF-6105357 **Severity:** low
Identifiers: **Message**:CVE-2023-49462

Vulnerability 3.473

Test-specific ID: SNYK-DEBIAN11-LIBHEIF-6105365 **Severity:** low
Identifiers: **Message**:CVE-2023-49460

Vulnerability 3.474

Test-specific ID: SNYK-DEBIAN11-LIBHEIF-6105371 **Severity:** low
Identifiers: **Message**:CVE-2023-49464

Vulnerability 3.475

Test-specific ID: SNYK-DEBIAN11-LIBHEIF-6105375 **Severity:** low
Identifiers: **Message**:CVE-2023-49463

Vulnerability 3.476

Test-specific ID: SNYK-DEBIAN11-LIBJPEGTURBO-2932112 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.477

Test-specific ID: SNYK-DEBIAN11-LIBPNG16-2363923 **Severity:** low
Identifiers: **Message**:Buffer Overflow

Vulnerability 3.478

Test-specific ID: SNYK-DEBIAN11-LIBPNG16-529373 **Severity:** low
Identifiers: **Message**:Memory Leak

Vulnerability 3.479

Test-specific ID: SNYK-DEBIAN11-LIBSEPOL-1315627 **Severity:** low
Identifiers: **Message**:Use After Free

Vulnerability 3.480

Test-specific ID: SNYK-DEBIAN11-LIBSEPOL-1315629 **Severity:** low
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.481

Test-specific ID: SNYK-DEBIAN11-LIBSEPOL-1315635 **Severity:** low
Identifiers: **Message**:Use After Free

Vulnerability 3.482

Test-specific ID: SNYK-DEBIAN11-LIBSEPOL-1315641 **Severity:** low
Identifiers: **Message**:Use After Free

Vulnerability 3.483

Test-specific ID: SNYK-DEBIAN11-LIBSSH2-5861756 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.484

Test-specific ID: SNYK-DEBIAN11-LIBWMF-514692 **Severity:** low
Identifiers: **Message**:Numeric Errors

Vulnerability 3.485

Test-specific ID: SNYK-DEBIAN11-LIBWMF-517351 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.486

Test-specific ID: SNYK-DEBIAN11-LIBWMF-519792 **Severity:** low
Identifiers: **Message**:Resource Management Errors

Vulnerability 3.487

Test-specific ID: SNYK-DEBIAN11-LIBWMF-527814 **Severity:** low
Identifiers: **Message**:Numeric Errors

Vulnerability 3.488

Test-specific ID: SNYK-DEBIAN11-LIBXML2-2964223 **Severity:** low
Identifiers: **Message**:Cross-site Scripting (XSS)

Vulnerability 3.489

Test-specific ID: SNYK-DEBIAN11-LIBXML2-5747746 **Severity:** low
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.490

Test-specific ID: SNYK-DEBIAN11-LIBXML2-5871334 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.491

Test-specific ID: SNYK-DEBIAN11-LIBXML2-5947664 **Severity:** low
Identifiers: **Message**:Use After Free

Vulnerability 3.492

Test-specific ID: SNYK-DEBIAN11-LIBXSLT-514942 **Severity:** low
Identifiers: **Message**:Use of Insufficiently Random Values

Vulnerability 3.493

Test-specific ID: SNYK-DEBIAN11-LIBZSTD-5406388 **Severity:** low
Identifiers: **Message**:Resource Exhaustion

Vulnerability 3.494

Test-specific ID: SNYK-DEBIAN11-M4-517010 **Severity:** low
Identifiers: **Message**:CVE-2008-1688

Vulnerability 3.495

Test-specific ID: SNYK-DEBIAN11-M4-525846 **Severity:** low
Identifiers: **Message**:CVE-2008-1687

Vulnerability 3.496

Test-specific ID: SNYK-DEBIAN11-MARIADB105-6091684 **Severity:** low
Identifiers: **Message**:CVE-2023-22084

Vulnerability 3.497

Test-specific ID: SNYK-DEBIAN11-NCURSES-6123820 **Severity:** low
Identifiers: **Message**:CVE-2023-50495

Vulnerability 3.498

Test-specific ID: SNYK-DEBIAN11-OPENEXR-1300565 **Severity:** low
Identifiers: **Message**:Integer Underflow

Vulnerability 3.499

Test-specific ID: SNYK-DEBIAN11-OPENEXR-522136 **Severity:** low
Identifiers: **Message**:Resource Exhaustion

Vulnerability 3.500

Test-specific ID: SNYK-DEBIAN11-OPENJPEG2-1247329 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.501

Test-specific ID: SNYK-DEBIAN11-OPENJPEG2-1301277 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.502

Test-specific ID: SNYK-DEBIAN11-OPENJPEG2-2434865 **Severity:** low
Identifiers: **Message**:Improper Initialization

Vulnerability 3.503

Test-specific ID: SNYK-DEBIAN11-OPENJPEG2-515201 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.504

Test-specific ID: SNYK-DEBIAN11-OPENJPEG2-515749 **Severity:** low
Identifiers: **Message**:Allocation of Resources Without Limits or Throttling

Vulnerability 3.505

Test-specific ID: SNYK-DEBIAN11-OPENJPEG2-516225 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.506

Test-specific ID: SNYK-DEBIAN11-OPENJPEG2-517708 **Severity:** low
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.507

Test-specific ID: SNYK-DEBIAN11-OPENJPEG2-518208 **Severity:** low
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.508

Test-specific ID: SNYK-DEBIAN11-OPENJPEG2-522491 **Severity:** low
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.509

Test-specific ID: SNYK-DEBIAN11-OPENJPEG2-524264 **Severity:** low
Identifiers: **Message**:Improper Input Validation

Vulnerability 3.510

Test-specific ID: SNYK-DEBIAN11-OPENJPEG2-524898 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.511

Test-specific ID: SNYK-DEBIAN11-OPENJPEG2-525517 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.512

Test-specific ID: SNYK-DEBIAN11-OPENJPEG2-526311 **Severity:** low
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.513

Test-specific ID: SNYK-DEBIAN11-OPENJPEG2-527081 **Severity:** low
Identifiers: **Message**:Divide By Zero

Vulnerability 3.514

Test-specific ID: SNYK-DEBIAN11-OPENJPEG2-528361 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.515

Test-specific ID: SNYK-DEBIAN11-OPENJPEG2-529941 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.516

Test-specific ID: SNYK-DEBIAN11-OPENJPEG2-532154 **Severity:** low
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.517

Test-specific ID: SNYK-DEBIAN11-OPENLDAP-521320 **Severity:** low
Identifiers: **Message**:Improper Initialization

Vulnerability 3.518

Test-specific ID: SNYK-DEBIAN11-OPENLDAP-531344 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.519

Test-specific ID: SNYK-DEBIAN11-OPENLDAP-531747 **Severity:** low
Identifiers: **Message**:Cryptographic Issues

Vulnerability 3.520

Test-specific ID: SNYK-DEBIAN11-OPENLDAP-5660622 **Severity:** low
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.521

Test-specific ID: SNYK-DEBIAN11-OPENLDAP-584937 **Severity:** low
Identifiers: **Message**:Improper Certificate Validation

Vulnerability 3.522

Test-specific ID: SNYK-DEBIAN11-OPENSSH-1585650 **Severity:** low
Identifiers: **Message**:CVE-2016-20012

Vulnerability 3.523

Test-specific ID: SNYK-DEBIAN11-OPENSSH-2422621 **Severity:** low
Identifiers: **Message**:Improper Authentication

Vulnerability 3.524

Test-specific ID: SNYK-DEBIAN11-OPENSSH-517822 **Severity:** low
Identifiers: **Message**:Information Exposure

Vulnerability 3.525

Test-specific ID: SNYK-DEBIAN11-OPENSSH-520976 **Severity:** low
Identifiers: **Message**:Information Exposure

Vulnerability 3.526

Test-specific ID: SNYK-DEBIAN11-OPENSSH-529002 **Severity:** low
Identifiers: **Message**:Improper Authentication

Vulnerability 3.527

Test-specific ID: SNYK-DEBIAN11-OPENSSH-529482 **Severity:** low
Identifiers: **Message**:Access Restriction Bypass

Vulnerability 3.528

Test-specific ID: SNYK-DEBIAN11-OPENSSH-530703 **Severity:** low
Identifiers: **Message**:Inappropriate Encoding for Output Context

Vulnerability 3.529

Test-specific ID: SNYK-DEBIAN11-OPENSSH-574760 **Severity:** low
Identifiers: **Message**:Information Exposure

Vulnerability 3.530

Test-specific ID: SNYK-DEBIAN11-OPENSSH-590139 **Severity:** low
Identifiers: **Message**:OS Command Injection

Vulnerability 3.531

Test-specific ID: SNYK-DEBIAN11-OPENSSL-518334 **Severity:** low
Identifiers: **Message**:Cryptographic Issues

Vulnerability 3.532

Test-specific ID: SNYK-DEBIAN11-OPENSSL-525332 **Severity:** low
Identifiers: **Message**:Cryptographic Issues

Vulnerability 3.533

Test-specific ID: SNYK-DEBIAN11-OPENSSL-6048819 **Severity:** low
Identifiers: **Message**:Improper Check for Unusual or Exceptional Conditions

Vulnerability 3.534

Test-specific ID: SNYK-DEBIAN11-OPENSSL-6190224 **Severity:** low
Identifiers: **Message**:CVE-2024-0727

Vulnerability 3.535

Test-specific ID: SNYK-DEBIAN11-PAM-6178915 **Severity:** low
Identifiers: **Message**:CVE-2024-22365

Vulnerability 3.536

Test-specific ID: SNYK-DEBIAN11-PATCH-2324789 **Severity:** low
Identifiers: **Message**:Release of Invalid Pointer or Reference

Vulnerability 3.537

Test-specific ID: SNYK-DEBIAN11-PATCH-525129 **Severity:** low
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.538

Test-specific ID: SNYK-DEBIAN11-PATCH-525153 **Severity:** low
Identifiers: **Message**:Directory Traversal

Vulnerability 3.539

Test-specific ID: SNYK-DEBIAN11-PATCH-526305 **Severity:** low
Identifiers: **Message**:Double Free

Vulnerability 3.540

Test-specific ID: SNYK-DEBIAN11-PCRE2-5788325 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.541

Test-specific ID: SNYK-DEBIAN11-PCRE3-523392 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.542

Test-specific ID: SNYK-DEBIAN11-PCRE3-525075 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.543

Test-specific ID: SNYK-DEBIAN11-PCRE3-529298 **Severity:** low
Identifiers: **Message**:Uncontrolled Recursion

Vulnerability 3.544

Test-specific ID: SNYK-DEBIAN11-PCRE3-529490 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.545

Test-specific ID: SNYK-DEBIAN11-PCRE3-572353 **Severity:** low
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.546

Test-specific ID: SNYK-DEBIAN11-PERL-1925976 **Severity:** low
Identifiers: **Message**:Improper Verification of Cryptographic Signature

Vulnerability 3.547

Test-specific ID: SNYK-DEBIAN11-PERL-532614 **Severity:** low
Identifiers: **Message**:Link Following

Vulnerability 3.548

Test-specific ID: SNYK-DEBIAN11-PERL-5489185 **Severity:** low
Identifiers: **Message**:Improper Certificate Validation

Vulnerability 3.549

Test-specific ID: SNYK-DEBIAN11-PERL-5489191 **Severity:** low
Identifiers: **Message**:Improper Certificate Validation

Vulnerability 3.550

Test-specific ID: SNYK-DEBIAN11-PERL-6085272 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.551

Test-specific ID: SNYK-DEBIAN11-PIXMAN-5803158 **Severity:** low
Identifiers: **Message**:Divide By Zero

Vulnerability 3.552

Test-specific ID: SNYK-DEBIAN11-POSTGRESQL13-3318091 **Severity:** low
Identifiers: **Message**:CVE-2022-41862

Vulnerability 3.553

Test-specific ID: SNYK-DEBIAN11-PROCPS-5816467 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.554

Test-specific ID: SNYK-DEBIAN11-PYTHON39-1021152 **Severity:** low
Identifiers: **Message**:CVE-2020-27619

Vulnerability 3.555

Test-specific ID: SNYK-DEBIAN11-PYTHON39-1085113 **Severity:** low
Identifiers: **Message**:Information Exposure

Vulnerability 3.556

Test-specific ID: SNYK-DEBIAN11-PYTHON39-1290158 **Severity:** low
Identifiers: **Message**:Improper Input Validation

Vulnerability 3.557

Test-specific ID: SNYK-DEBIAN11-PYTHON39-1570176 **Severity:** low
Identifiers: **Message**:Resource Exhaustion

Vulnerability 3.558

Test-specific ID: SNYK-DEBIAN11-PYTHON39-1579738 **Severity:** low
Identifiers: **Message**:Resource Exhaustion

Vulnerability 3.559

Test-specific ID: SNYK-DEBIAN11-PYTHON39-2329042 **Severity:** low
Identifiers: **Message**:Unchecked Return Value

Vulnerability 3.560

Test-specific ID: SNYK-DEBIAN11-PYTHON39-2388383 **Severity:** low
Identifiers: **Message**:Arbitrary Code Injection

Vulnerability 3.561

Test-specific ID: SNYK-DEBIAN11-PYTHON39-2764968 **Severity:** low
Identifiers: **Message**:Arbitrary Command Injection

Vulnerability 3.562

Test-specific ID: SNYK-DEBIAN11-PYTHON39-3017608 **Severity:** low
Identifiers: **Message**:Incorrect Type Conversion or Cast

Vulnerability 3.563

Test-specific ID: SNYK-DEBIAN11-PYTHON39-3032984 **Severity:** low
Identifiers: **Message**:Open Redirect

Vulnerability 3.564

Test-specific ID: SNYK-DEBIAN11-PYTHON39-3090932 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.565

Test-specific ID: SNYK-DEBIAN11-PYTHON39-3092471 **Severity:** low
Identifiers: **Message**:CVE-2022-42919

Vulnerability 3.566

Test-specific ID: SNYK-DEBIAN11-PYTHON39-3111117 **Severity:** low
Identifiers: **Message**:Algorithmic Complexity

Vulnerability 3.567

Test-specific ID: SNYK-DEBIAN11-PYTHON39-3325303 **Severity:** low
Identifiers: **Message**:Improper Input Validation

Vulnerability 3.568

Test-specific ID: SNYK-DEBIAN11-PYTHON39-5430933 **Severity:** low
Identifiers: **Message**:Improper Input Validation

Vulnerability 3.569

Test-specific ID: SNYK-DEBIAN11-PYTHON39-5754616 **Severity:** low
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.570

Test-specific ID: SNYK-DEBIAN11-SHADOW-526940 **Severity:** low
Identifiers: **Message**:Access Restriction Bypass

Vulnerability 3.571

Test-specific ID: SNYK-DEBIAN11-SHADOW-528840 **Severity:** low
Identifiers: **Message**:Time-of-check Time-of-use (TOCTOU)

Vulnerability 3.572

Test-specific ID: SNYK-DEBIAN11-SHADOW-539870 **Severity:** low
Identifiers: **Message**:Incorrect Permission Assignment for Critical Resource

Vulnerability 3.573

Test-specific ID: SNYK-DEBIAN11-SHADOW-5423922 **Severity:** low
Identifiers: **Message**:Arbitrary Code Injection

Vulnerability 3.574

Test-specific ID: SNYK-DEBIAN11-SHADOW-5879152 **Severity:** low
Identifiers: **Message**:Improper Authentication

Vulnerability 3.575

Test-specific ID: SNYK-DEBIAN11-SQLITE3-1569419 **Severity:** low
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.576

Test-specific ID: SNYK-DEBIAN11-SQLITE3-2407045 **Severity:** low
Identifiers: **Message**:Memory Leak

Vulnerability 3.577

Test-specific ID: SNYK-DEBIAN11-SQLITE3-2959400 **Severity:** low
Identifiers: **Message**:Improper Validation of Array Index

Vulnerability 3.578

Test-specific ID: SNYK-DEBIAN11-SQLITE3-5562381 **Severity:** low
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.579

Test-specific ID: SNYK-DEBIAN11-SQLITE3-6139925 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.580

Test-specific ID: SNYK-DEBIAN11-SYSTEMD-1291054 **Severity:** low
Identifiers: **Message**:Authentication Bypass

Vulnerability 3.581

Test-specific ID: SNYK-DEBIAN11-SYSTEMD-524969 **Severity:** low
Identifiers: **Message**:Link Following

Vulnerability 3.582

Test-specific ID: SNYK-DEBIAN11-SYSTEMD-5733387 **Severity:** low
Identifiers: **Message**:Improper Validation of Integrity Check Value

Vulnerability 3.583

Test-specific ID: SNYK-DEBIAN11-SYSTEMD-5733391 **Severity:** low
Identifiers: **Message**:Improper Validation of Integrity Check Value

Vulnerability 3.584

Test-specific ID: SNYK-DEBIAN11-SYSTEMD-5733392 **Severity:** low
Identifiers: **Message**:Improper Validation of Integrity Check Value

Vulnerability 3.585

Test-specific ID: SNYK-DEBIAN11-SYSTEMD-6137713 **Severity:** low
Identifiers: **Message**:CVE-2023-7008

Vulnerability 3.586

Test-specific ID: SNYK-DEBIAN11-TAR-3253527 **Severity:** low
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.587

Test-specific ID: SNYK-DEBIAN11-TAR-523480 **Severity:** low
Identifiers: **Message**:CVE-2005-2541

Vulnerability 3.588

Test-specific ID: SNYK-DEBIAN11-TAR-6120424 **Severity:** low
Identifiers: **Message**:CVE-2023-39804

Vulnerability 3.589

Test-specific ID: SNYK-DEBIAN11-TCL86-1316209 **Severity:** low
Identifiers: **Message**:Use of Externally-Controlled Format String

Vulnerability 3.590

Test-specific ID: SNYK-DEBIAN11-TIFF-2434417 **Severity:** low
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.591

Test-specific ID: SNYK-DEBIAN11-TIFF-2440571 **Severity:** low
Identifiers: **Message**:Improper Resource Shutdown or Release

Vulnerability 3.592

Test-specific ID: SNYK-DEBIAN11-TIFF-514595 **Severity:** low
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.593

Test-specific ID: SNYK-DEBIAN11-TIFF-516778 **Severity:** low
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.594

Test-specific ID: SNYK-DEBIAN11-TIFF-518574 **Severity:** low
Identifiers: **Message**:Missing Release of Resource after Effective Lifetime

Vulnerability 3.595

Test-specific ID: SNYK-DEBIAN11-TIFF-520936 **Severity:** low
Identifiers: **Message**:Use After Free

Vulnerability 3.596

Test-specific ID: SNYK-DEBIAN11-TIFF-531474 **Severity:** low
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.597

Test-specific ID: SNYK-DEBIAN11-TIFF-5416363 **Severity:** low
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.598

Test-specific ID: SNYK-DEBIAN11-TIFF-5425904 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.599

Test-specific ID: SNYK-DEBIAN11-TIFF-5673712 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.600

Test-specific ID: SNYK-DEBIAN11-TIFF-5724641 **Severity:** low
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.601

Test-specific ID: SNYK-DEBIAN11-TIFF-5747597 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.602

Test-specific ID: SNYK-DEBIAN11-TIFF-5749339 **Severity:** low
Identifiers: **Message**:Buffer Overflow

Vulnerability 3.603

Test-specific ID: SNYK-DEBIAN11-TIFF-5750143 **Severity:** low
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.604

Test-specific ID: SNYK-DEBIAN11-TIFF-5767900 **Severity:** low
Identifiers: **Message**:Buffer Overflow

Vulnerability 3.605

Test-specific ID: SNYK-DEBIAN11-TIFF-5773188 **Severity:** low
Identifiers: **Message**:Buffer Overflow

Vulnerability 3.606

Test-specific ID: SNYK-DEBIAN11-TIFF-5853001 **Severity:** low
Identifiers: **Message**:Loop with Unreachable Exit Condition ('Infinite Loop')

Vulnerability 3.607

Test-specific ID: SNYK-DEBIAN11-TIFF-6079927 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.608

Test-specific ID: SNYK-DEBIAN11-TIFF-6084515 **Severity:** low
Identifiers: **Message**:Resource Exhaustion

Vulnerability 3.609

Test-specific ID: SNYK-DEBIAN11-TIFF-6190609 **Severity:** low
Identifiers: **Message**:CVE-2023-52356

Vulnerability 3.610

Test-specific ID: SNYK-DEBIAN11-TIFF-6190787 **Severity:** low
Identifiers: **Message**:CVE-2023-52355

Vulnerability 3.611

Test-specific ID: SNYK-DEBIAN11-UNZIP-2387325 **Severity:** low
Identifiers: **Message**:NULL Pointer Dereference

Vulnerability 3.612

Test-specific ID: SNYK-DEBIAN11-UTILLINUX-2401081 **Severity:** low
Identifiers: **Message**:Information Exposure

Vulnerability 3.613

Test-specific ID: SNYK-DEBIAN11-WGET-1277610 **Severity:** low
Identifiers: **Message**:Open Redirect

4. Dynamic Train Analysis

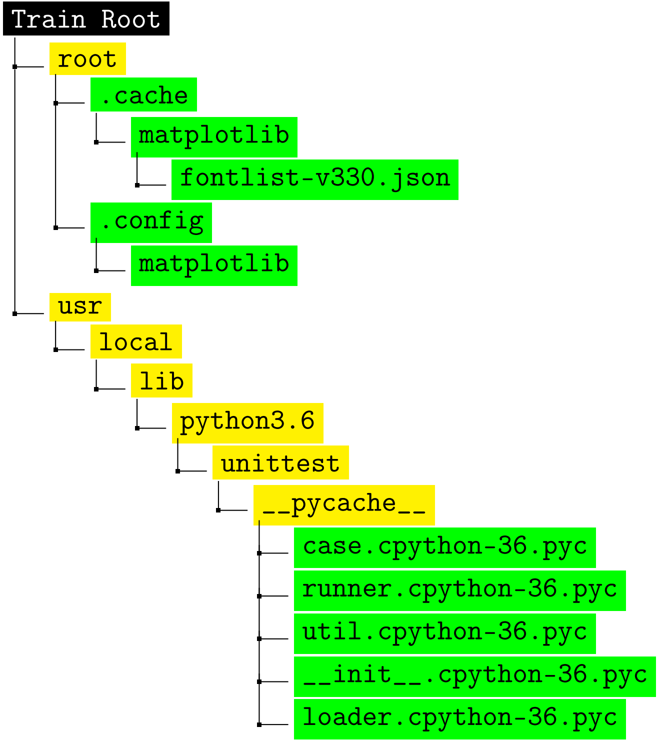
4.1 Image size differences after simulation:

4.1.1 Simulated route:

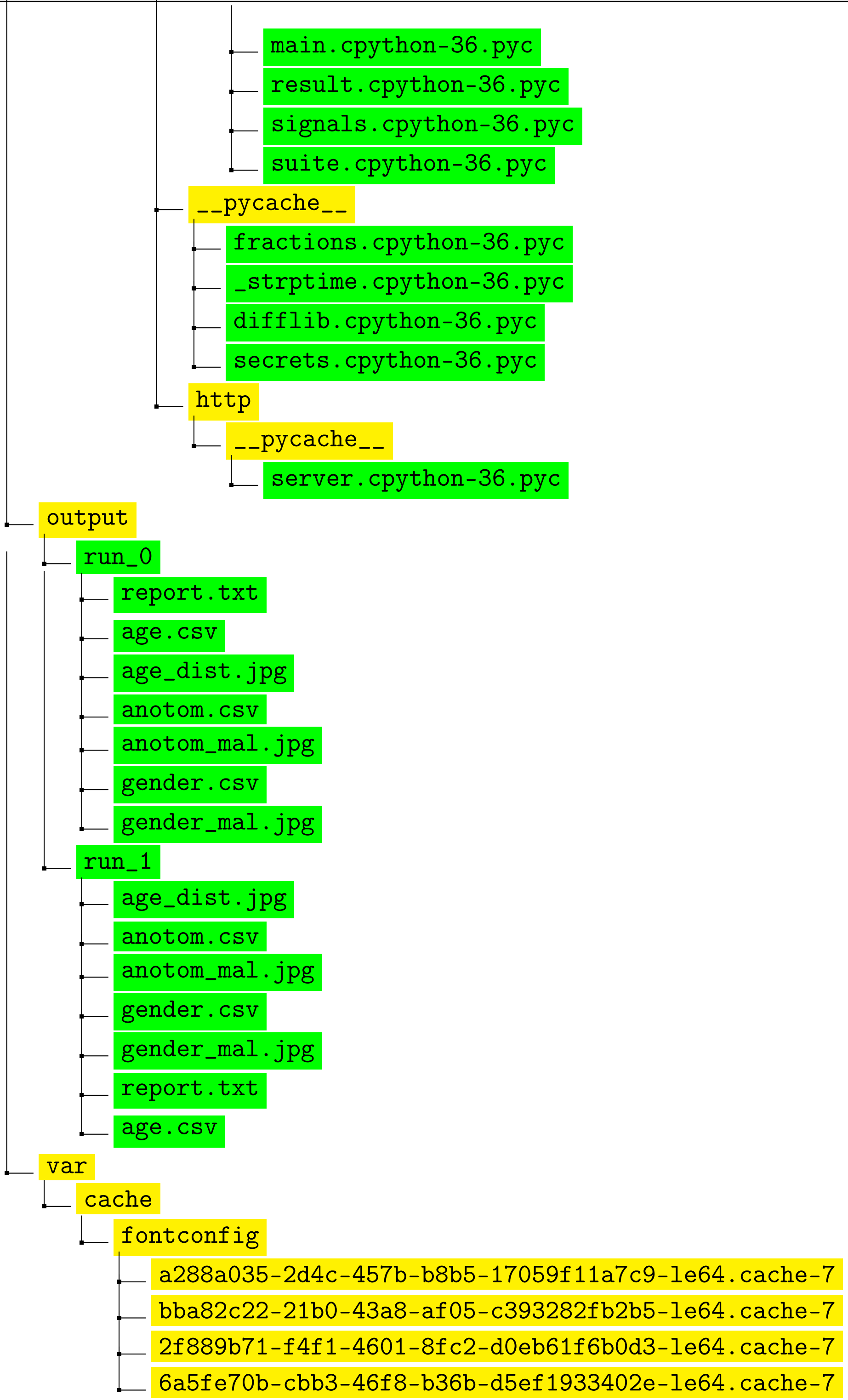
- Station 5bce186a-5005-4ca8-878e-9d8d4e0747c0: 404200
- Station d7b0a9a7-07fd-4a31-b93a-3c946dc82667: 132017

4.1.2 Directory Overview of changed files:

Legend: Modified Added Deleted



```
Train Root
├── root
│   ├── .cache
│   │   └── matplotlib
│   │       └── fontlist-v330.json
│   └── .config
│       └── matplotlib
└── usr
    └── local
        └── lib
            └── python3.6
                └── unittest
                    └── __pycache__
                        ├── case.cpython-36.pyc
                        ├── runner.cpython-36.pyc
                        ├── util.cpython-36.pyc
                        ├── __init__.cpython-36.pyc
                        └── loader.cpython-36.pyc
```



4.1.3 ./simulationResults/fontlist-v330.json

Listing 4.1: fontlist-v330.json

```
{
  "_version": 330,
  "_FontManager__default_weight": "normal",
  "default_size": null,
  "defaultFamily": {
    "ttf": "DejaVu Sans",
    "afm": "Helvetica"
  },
  "afmlist": [
    {
      "fname": "fonts/afm/pbkd8a.afm",
      "name": "ITC Bookman",
      "style": "normal",
      "variant": "normal",
      "weight": "demi",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/afm/phvl8a.afm",
      "name": "Helvetica",
      "style": "normal",
      "variant": "normal",
      "weight": "light",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/afm/cmtt10.afm",
      "name": "Computer Modern",
      "style": "normal",
      "variant": "normal",
      "weight": "medium",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/afm/cmr10.afm",
      "name": "Computer Modern",
      "style": "normal",
      "variant": "normal",
      "weight": "medium",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/afm/pbkl8a.afm",
      "name": "ITC Bookman",
      "style": "normal",
      "variant": "normal",
      "weight": "light",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/afm/putb8a.afm",
      "name": "Utopia",
      "style": "normal",
      "variant": "normal",
      "weight": "bold",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/pdfcorefonts/Times-Bold.afm",
      "name": "Times",
      "style": "normal",
      "variant": "normal",
      "weight": "bold",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/pdfcorefonts/Courier-Bold.afm",
      "name": "Courier",
      "style": "normal",
      "variant": "normal",
      "weight": "bold",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/pdfcorefonts/Helvetica.afm",
      "name": "Helvetica",
      "style": "normal",
      "variant": "normal",
      "weight": "medium",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/afm/phvro8a.afm",
      "name": "Helvetica",
      "style": "italic",
      "variant": "normal",
      "weight": "medium",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/afm/pagd8a.afm",
      "name": "ITC Avant Garde Gothic",
      "style": "normal",
      "variant": "normal",
      "weight": "demi",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/pdfcorefonts/Helvetica-Bold.afm",
      "name": "Helvetica",
      "style": "normal",
      "variant": "normal",
      "weight": "bold",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/afm/pzcmi8a.afm",
      "name": "ITC Zapf Chancery",
      "style": "italic",
      "variant": "normal",
      "weight": "medium",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/afm/ptmb8a.afm",
      "name": "Times",
      "style": "normal",
      "variant": "normal",
      "weight": "bold",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/afm/putri8a.afm",
      "name": "Utopia",
      "style": "italic",
      "variant": "normal",
      "weight": "regular",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/afm/pzdr.afm",
      "name": "ITC Zapf Dingbats",
      "style": "normal",
      "variant": "normal",
      "weight": "medium",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/afm/pplri8a.afm",
      "name": "Palatino",
      "style": "italic",
      "variant": "normal",
      "weight": "medium",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/afm/phvlo8a.afm",
      "name": "Helvetica",
      "style": "italic",
      "variant": "normal",
      "weight": "light",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/afm/pcrb8a.afm",
      "name": "Courier",
      "style": "normal",
      "variant": "normal",
      "weight": "bold",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/afm/pncr8a.afm",
      "name": "New Century Schoolbook",
      "style": "normal",
      "variant": "normal",
      "weight": "roman",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/afm/pncb8a.afm",
      "name": "New Century Schoolbook",
      "style": "normal",
      "variant": "normal",
      "weight": "bold",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/afm/pplbi8a.afm",
      "name": "Palatino",
      "style": "italic",
      "variant": "normal",
      "weight": "bold",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/afm/cmsy10.afm",
      "name": "Computer Modern",
      "style": "italic",
      "variant": "normal",
      "weight": "medium",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/afm/ptmbi8a.afm",
      "name": "Times",
      "style": "italic",
      "variant": "normal",
      "weight": "bold",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/afm/pplb8a.afm",
      "name": "Palatino",
      "style": "normal",
      "variant": "normal",
      "weight": "bold",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/afm/pagdo8a.afm",
      "name": "ITC Avant Garde Gothic",
      "style": "italic",
      "variant": "normal",
      "weight": "demi",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/pdfcorefonts/Symbol.afm",
      "name": "Symbol",
      "style": "normal",
      "variant": "normal",
      "weight": "medium",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/afm/pagko8a.afm",
      "name": "ITC Avant Garde Gothic",
      "style": "italic",
      "variant": "normal",
      "weight": "book",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/pdfcorefonts/Courier-BoldOblique.afm",
      "name": "Courier",
      "style": "italic",
      "variant": "normal",
      "weight": "bold",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/afm/ptmri8a.afm",
      "name": "Times",
      "style": "italic",
      "variant": "normal",
      "weight": "medium",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/pdfcorefonts/Times-Roman.afm",
      "name": "Times",
      "style": "normal",
      "variant": "normal",
      "weight": "roman",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/afm/phvbo8an.afm",
      "name": "Helvetica",
      "style": "italic",
      "variant": "normal",
      "weight": "bold",
      "stretch": "condensed",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/afm/ptmr8a.afm",
      "name": "Times",
      "style": "normal",
      "variant": "normal",
      "weight": "roman",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/afm/phvr8an.afm",
      "name": "Helvetica",
      "style": "normal",
      "variant": "normal",
      "weight": "medium",
      "stretch": "condensed",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/afm/phvbo8a.afm",
      "name": "Helvetica",
      "style": "italic",
      "variant": "normal",
      "weight": "bold",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/afm/phvb8an.afm",
      "name": "Helvetica",
      "style": "normal",
      "variant": "normal",
      "weight": "bold",
      "stretch": "condensed",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/afm/pbkdi8a.afm",
      "name": "ITC Bookman",
      "style": "italic",
      "variant": "normal",
      "weight": "demi",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/afm/putbi8a.afm",
      "name": "Utopia",
      "style": "italic",
      "variant": "normal",
      "weight": "bold",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/afm/pcrro8a.afm",
      "name": "Courier",
      "style": "italic",
      "variant": "normal",
      "weight": "medium",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/afm/pncbi8a.afm",
      "name": "New Century Schoolbook",
      "style": "italic",
      "variant": "normal",
      "weight": "bold",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/pdfcorefonts/Helvetica-BoldOblique.afm",
      "name": "Helvetica",
      "style": "italic",
      "variant": "normal",
      "weight": "bold",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/afm/phvro8an.afm",
      "name": "Helvetica",
      "style": "italic",
      "variant": "normal",
      "weight": "medium",
      "stretch": "condensed",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/pdfcorefonts/Courier.afm",
      "name": "Courier",
      "style": "normal",
      "variant": "normal",
      "weight": "medium",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/afm/pbkli8a.afm",
      "name": "ITC Bookman",
      "style": "italic",
      "variant": "normal",
      "weight": "light",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/afm/phvr8a.afm",
      "name": "Helvetica",
      "style": "normal",
      "variant": "normal",
      "weight": "medium",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/afm/phvb8a.afm",
      "name": "Helvetica",
      "style": "normal",
      "variant": "normal",
      "weight": "bold",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/pdfcorefonts/Courier-Oblique.afm",
      "name": "Courier",
      "style": "italic",
      "variant": "normal",
      "weight": "medium",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/afm/pncri8a.afm",
      "name": "New Century Schoolbook",
      "style": "italic",
      "variant": "normal",
      "weight": "medium",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/pdfcorefonts/ZapfDingbats.afm",
      "name": "ZapfDingbats",
      "style": "normal",
      "variant": "normal",
      "weight": "medium",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/afm/pcrr8a.afm",
      "name": "Courier",
      "style": "normal",
      "variant": "normal",
      "weight": "medium",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/afm/pplr8a.afm",
      "name": "Palatino",
      "style": "normal",
      "variant": "normal",
      "weight": "roman",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/afm/pcrbo8a.afm",
      "name": "Courier",
      "style": "italic",
      "variant": "normal",
      "weight": "bold",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/pdfcorefonts/Times-BoldItalic.afm",
      "name": "Times",
      "style": "italic",
      "variant": "normal",
      "weight": "bold",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/pdfcorefonts/Helvetica-Oblique.afm",
      "name": "Helvetica",
      "style": "italic",
      "variant": "normal",
      "weight": "medium",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/pdfcorefonts/Times-Italic.afm",
      "name": "Times",
      "style": "italic",
      "variant": "normal",
      "weight": "medium",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/afm/psyr.afm",
      "name": "Symbol",
      "style": "normal",
      "variant": "normal",
      "weight": "medium",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/afm/putr8a.afm",
      "name": "Utopia",
      "style": "normal",
      "variant": "normal",
      "weight": "regular",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/afm/cmex10.afm",
      "name": "Computer Modern",
      "style": "normal",
      "variant": "normal",
      "weight": "medium",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/afm/pagk8a.afm",
      "name": "ITC Avant Garde Gothic",
      "style": "normal",
      "variant": "normal",
      "weight": "book",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/afm/cmmi10.afm",
      "name": "Computer Modern",
      "style": "italic",
      "variant": "normal",
      "weight": "medium",
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    }
  ],
  "ttflist": [
    {
      "fname": "fonts/ttf/DejaVuSansMono-Bold.ttf",
      "name": "DejaVu Sans Mono",
      "style": "normal",
      "variant": "normal",
      "weight": 700,
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/ttf/STIXSizThreeSymBol.ttf",
      "name": "STIXSizeThreeSym",
      "style": "normal",
      "variant": "normal",
      "weight": 700,
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/ttf/DejaVuSerif-BoldItalic.ttf",
      "name": "DejaVu Serif",
      "style": "italic",
      "variant": "normal",
      "weight": 700,
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/ttf/STIXGeneral.ttf",
      "name": "STIXGeneral",
      "style": "normal",
      "variant": "normal",
      "weight": 400,
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/ttf/STIXSizFourSymBol.ttf",
      "name": "STIXSizeFourSym",
      "style": "normal",
      "variant": "normal",
      "weight": 700,
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/ttf/DejaVuSerif-Bold.ttf",
      "name": "DejaVu Serif",
      "style": "normal",
      "variant": "normal",
      "weight": 700,
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/ttf/cmsy10.ttf",
      "name": "cmsy10",
      "style": "normal",
      "variant": "normal",
      "weight": 400,
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/ttf/DejaVuSansDisplay.ttf",
      "name": "DejaVu Sans Display",
      "style": "normal",
      "variant": "normal",
      "weight": 400,
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/ttf/STIXSizFourSymReg.ttf",
      "name": "STIXSizeFourSym",
      "style": "normal",
      "variant": "normal",
      "weight": 400,
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/ttf/STIXGeneralBol.ttf",
      "name": "STIXGeneral",
      "style": "normal",
      "variant": "normal",
      "weight": 700,
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/ttf/cmb10.ttf",
      "name": "cmb10",
      "style": "normal",
      "variant": "normal",
      "weight": 400,
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/ttf/STIXSizTwoSymBol.ttf",
      "name": "STIXSizeTwoSym",
      "style": "normal",
      "variant": "normal",
      "weight": 700,
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/ttf/cmss10.ttf",
      "name": "cmss10",
      "style": "normal",
      "variant": "normal",
      "weight": 400,
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/ttf/STIXSizOneSymBol.ttf",
      "name": "STIXSizeOneSym",
      "style": "normal",
      "variant": "normal",
      "weight": 700,
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/ttf/STIXNonUniBol.ttf",
      "name": "STIXNonUnicode",
      "style": "normal",
      "variant": "normal",
      "weight": 700,
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/ttf/cmex10.ttf",
      "name": "cmex10",
      "style": "normal",
      "variant": "normal",
      "weight": 400,
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/ttf/STIXGeneralItalic.ttf",
      "name": "STIXGeneral",
      "style": "italic",
      "variant": "normal",
      "weight": 400,
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/ttf/DejaVuSansMono-BoldOblique.ttf",
      "name": "DejaVu Sans Mono",
      "style": "oblique",
      "variant": "normal",
      "weight": 700,
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/ttf/DejaVuSerif-Italic.ttf",
      "name": "DejaVu Serif",
      "style": "italic",
      "variant": "normal",
      "weight": 400,
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/ttf/cmtt10.ttf",
      "name": "cmtt10",
      "style": "normal",
      "variant": "normal",
      "weight": 400,
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/ttf/DejaVuSans-BoldOblique.ttf",
      "name": "DejaVu Sans",
      "style": "oblique",
      "variant": "normal",
      "weight": 700,
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/ttf/DejaVuSerif.ttf",
      "name": "DejaVu Serif",
      "style": "normal",
      "variant": "normal",
      "weight": 400,
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/ttf/STIXSizOneSymReg.ttf",
      "name": "STIXSizeOneSym",
      "style": "normal",
      "variant": "normal",
      "weight": 400,
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/ttf/cmmi10.ttf",
      "name": "cmmi10",
      "style": "normal",
      "variant": "normal",
      "weight": 400,
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/ttf/DejaVuSansMono-Oblique.ttf",
      "name": "DejaVu Sans Mono",
      "style": "oblique",
      "variant": "normal",
      "weight": 400,
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/ttf/STIXGeneralBolIta.ttf",
      "name": "STIXGeneral",
      "style": "italic",
      "variant": "normal",
      "weight": 700,
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/ttf/STIXNonUniBolIta.ttf",
      "name": "STIXNonUnicode",
      "style": "italic",
      "variant": "normal",
      "weight": 700,
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/ttf/STIXNonUni.ttf",
      "name": "STIXNonUnicode",
      "style": "normal",
      "variant": "normal",
      "weight": 400,
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/ttf/DejaVuSans-Bold.ttf",
      "name": "DejaVu Sans",
      "style": "normal",
      "variant": "normal",
      "weight": 700,
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/ttf/STIXNonUniIta.ttf",
      "name": "STIXNonUnicode",
      "style": "italic",
      "variant": "normal",
      "weight": 400,
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/ttf/DejaVuSansMono.ttf",
      "name": "DejaVu Sans Mono",
      "style": "normal",
      "variant": "normal",
      "weight": 400,
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/ttf/DejaVuSans.ttf",
      "name": "DejaVu Sans",
      "style": "normal",
      "variant": "normal",
      "weight": 400,
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/ttf/STIXSizFiveSymReg.ttf",
      "name": "STIXSizeFiveSym",
      "style": "normal",
      "variant": "normal",
      "weight": 400,
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/ttf/STIXSizTwoSymReg.ttf",
      "name": "STIXSizeTwoSym",
      "style": "normal",
      "variant": "normal",
      "weight": 400,
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/ttf/DejaVuSans-Oblique.ttf",
      "name": "DejaVu Sans",
      "style": "oblique",
      "variant": "normal",
      "weight": 400,
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/ttf/STIXSizThreeSymReg.ttf",
      "name": "STIXSizeThreeSym",
      "style": "normal",
      "variant": "normal",
      "weight": 400,
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/ttf/DejaVuSerifDisplay.ttf",
      "name": "DejaVu Serif Display",
      "style": "normal",
      "variant": "normal",
      "weight": 400,
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "fonts/ttf/cmr10.ttf",
      "name": "cmr10",
      "style": "normal",
      "variant": "normal",
      "weight": 400,
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "/usr/share/fonts/truetype/dejavu/DejaVuSans.
         ttf",
      "name": "DejaVu Sans",
      "style": "normal",
      "variant": "normal",
      "weight": 400,
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "/usr/share/fonts/truetype/dejavu/
         DejaVuSansMono-Bold.ttf",
      "name": "DejaVu Sans Mono",
      "style": "normal",
      "variant": "normal",
      "weight": 700,
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "/usr/share/fonts/truetype/dejavu/DejaVuSerif.
         ttf",
      "name": "DejaVu Serif",
      "style": "normal",
      "variant": "normal",
      "weight": 400,
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "/usr/share/fonts/truetype/dejavu/
         DejaVuSansMono.ttf",
      "name": "DejaVu Sans Mono",
      "style": "normal",
      "variant": "normal",
      "weight": 400,
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "/usr/share/fonts/truetype/dejavu/DejaVuSans-Bold.ttf",
      "name": "DejaVu Sans",
      "style": "normal",
      "variant": "normal",
      "weight": 700,
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    },
    {
      "fname": "/usr/share/fonts/truetype/dejavu/DejaVuSerif-Bold.ttf",
      "name": "DejaVu Serif",
      "style": "normal",
      "variant": "normal",
      "weight": 700,
      "stretch": "normal",
      "size": "scalable",
      "__class__": "FontEntry"
    }
  ],
  "__class__": "FontManager"
}
```

4.1.4 ./simulationResults/matplotlib

No Preview Available! https://git.rwth-aachen.de/padme-development/padme-train-depot/-/jobs/4570470/artifacts/file/simulationResults/matplotlib

4.1.5 ./simulationResults/case.cpython-36.pyc

No Preview Available! https://git.rwth-aachen.de/padme-development/padme-train-depot/-/jobs/4570470/artifacts/file/simulationResults/case.cpython-36.pyc

4.1.6 ./simulationResults/runner.cpython-36.pyc

No Preview Available! https://git.rwth-aachen.de/padme-development/padme-train-depot/-/jobs/4570470/artifacts/file/simulationResults/runner.cpython-36.pyc

4.1.7 ./simulationResults/util.cpython-36.pyc

No Preview Available! https://git.rwth-aachen.de/padme-development/padme-train-depot/-/jobs/4570470/artifacts/file/simulationResults/util.cpython-36.pyc

4.1.8 ./simulationResults/__init__.cpython-36.pyc

No Preview Available! https://git.rwth-aachen.de/padme-development/padme-train-depot/-/jobs/4570470/artifacts/file/simulationResults/__init__.cpython-36.pyc

4.1.9 ./simulationResults/loader.cpython-36.pyc

No Preview Available! `https://git.rwth-aachen.de/padme-development/padme-train-depot/-/jobs/4570470/artifacts/file/simulationResults/loader.cpython-36.pyc`

4.1.10 ./simulationResults/main.cpython-36.pyc

No Preview Available! `https://git.rwth-aachen.de/padme-development/padme-train-depot/-/jobs/4570470/artifacts/file/simulationResults/main.cpython-36.pyc`

4.1.11 ./simulationResults/result.cpython-36.pyc

No Preview Available! `https://git.rwth-aachen.de/padme-development/padme-train-depot/-/jobs/4570470/artifacts/file/simulationResults/result.cpython-36.pyc`

4.1.12 ./simulationResults/signals.cpython-36.pyc

No Preview Available! `https://git.rwth-aachen.de/padme-development/padme-train-depot/-/jobs/4570470/artifacts/file/simulationResults/signals.cpython-36.pyc`

4.1.13 ./simulationResults/suite.cpython-36.pyc

No Preview Available! `https://git.rwth-aachen.de/padme-development/padme-train-depot/-/jobs/4570470/artifacts/file/simulationResults/suite.cpython-36.pyc`

4.1.14 ./simulationResults/fractions.cpython-36.pyc

No Preview Available! `https://git.rwth-aachen.de/padme-development/padme-train-depot/-/jobs/4570470/artifacts/file/simulationResults/fractions.cpython-36.pyc`

4.1.15 ./simulationResults/_strptime.cpython-36.pyc

No Preview Available! `https://git.rwth-aachen.de/padme-development/padme-train-depot/-/jobs/4570470/artifacts/file/simulationResults/_strptime.cpython-36.pyc`

4.1.16 ./simulationResults/difflib.cpython-36.pyc

No Preview Available! `https://git.rwth-aachen.de/padme-development/padme-train-depot/-/jobs/4570470/artifacts/file/simulationResults/difflib.cpython-36.pyc`

4.1.17 ./simulationResults/secrets.cpython-36.pyc

No Preview Available! `https://git.rwth-aachen.de/padme-development/padme-train-depot/-/jobs/4570470/artifacts/file/simulationResults/secrets.cpython-36.pyc`

4.1.18 ./simulationResults/server.cpython-36.pyc

No Preview Available! `https://git.rwth-aachen.de/padme-development/padme-train-depot/-/jobs/4570470/artifacts/file/simulationResults/server.cpython-36.pyc`

4.1.19 ./simulationResults/report.txt

Listing 4.2: report.txt

```
Stations have 8301 instances with complete attributes
Station has 142 instances whose attribute "age" is missing
Station has 0 instances whose attribute "gender" is missing
Station has 891 instances whose attribute "bodySite" is
   missing
```

4.1.20 ./simulationResults/age.csv

Listing 4.3: age.csv

```
,MEL,NV,BCC,AK,BKL,DF,VASC,SCC
lower quartile,51.0,36.0,56.0,61.0,56.0,46.0,41.0,66.0
median,61.0,46.0,71.0,71.0,66.0,56.0,56.0,71.0
upper quartile,76.0,56.0,81.0,76.0,76.0,66.0,71.0,81.0
```

4.1.21 ./simulationResults/age_dist.jpg

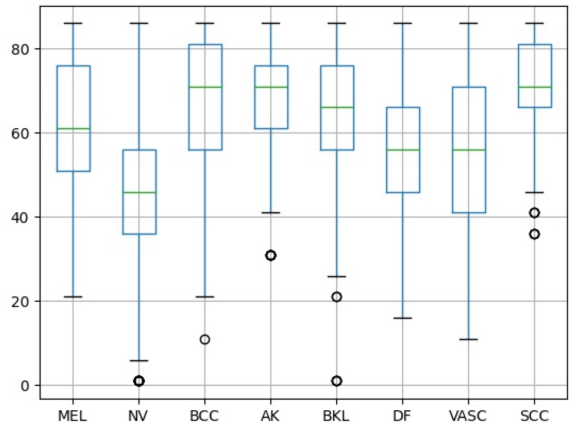


Figure 4.1: age_dist.jpg

4.1.22 ./simulationResults/anotom.csv

Listing 4.4: anotom.csv

```
bodySite,MEL,NV,BCC,AK,BKL,DF,VASC,SCC
anterior torso,439,1232,384,34,144,11,24,35
head/neck,309,261,354,226,340,0,9,63
lateral torso,4,14,0,0,2,0,0,0
lower extremity,258,992,158,22,141,43,31,62
oral/genital,5,15,0,0,6,0,1,0
palms/soles,69,54,0,2,1,0,0,5
posterior torso,140,602,41,2,79,0,4,10
upper extremity,222,419,128,31,73,17,4,30
```

4.1.23 ./simulationResults/anotom_mal.jpg

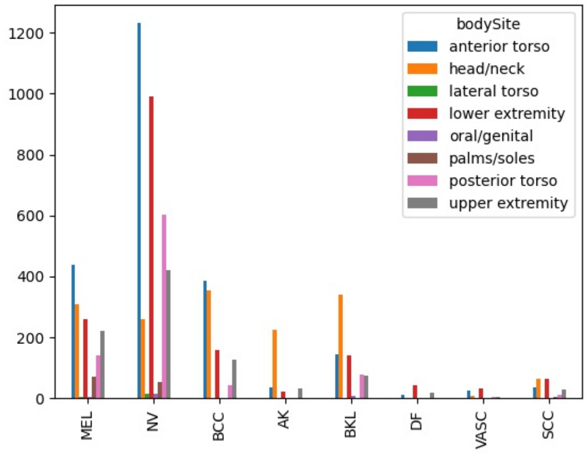


Figure 4.2: anotom_mal.jpg

4.1.24 ./simulationResults/gender.csv

Listing 4.5: gender.csv

```
gender,MEL,NV,BCC,AK,BKL,DF,VASC,SCC
female,650,2139,424,156,367,45,43,63
male,810,2087,654,163,504,27,41,142
unknown,31,85,3,1,8,0,0,0
```

4.1.25 ./simulationResults/gender_mal.jpg

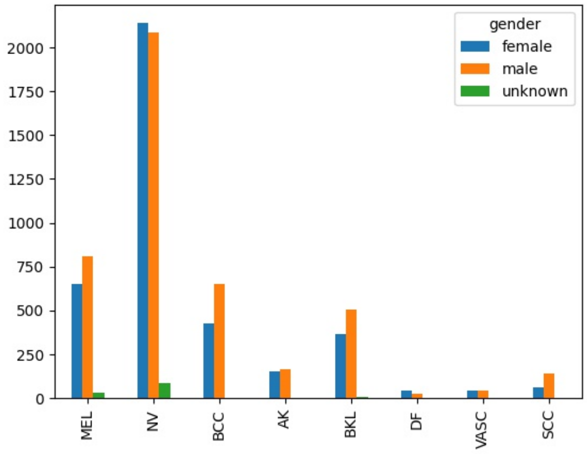


Figure 4.3: gender_mal.jpg

4.1.26 ./simulationResults/age_dist.jpg

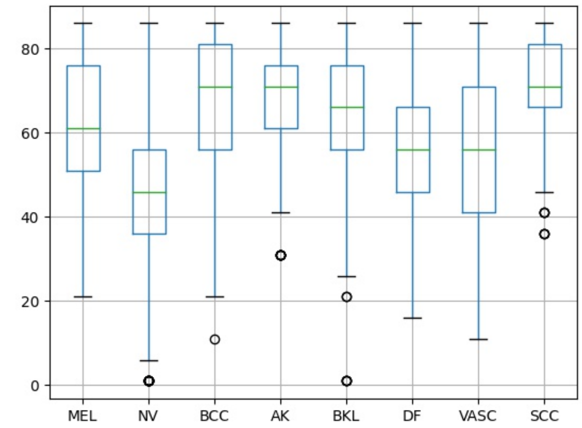


Figure 4.4: age_dist.jpg

4.1.27 ./simulationResults/anotom.csv

Listing 4.6: anotom.csv

```
bodySite,MEL,NV,BCC,AK,BKL,DF,VASC,SCC
anterior torso,439,1232,384,34,144,11,24,35
head/neck,309,261,354,226,340,0,9,63
lateral torso,4,14,0,0,2,0,0,0
lower extremity,258,992,158,22,141,43,31,62
oral/genital,5,15,0,0,6,0,1,0
palms/soles,69,54,0,2,1,0,0,5
posterior torso,140,602,41,2,79,0,4,10
upper extremity,222,419,128,31,73,17,4,30
```

4.1.28 ./simulationResults/anotom_mal.jpg

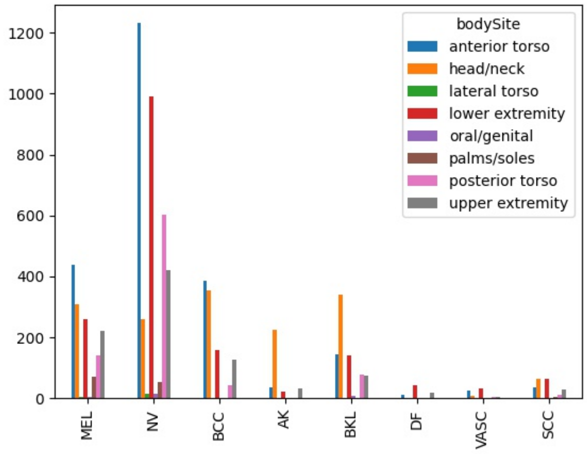


Figure 4.5: anotom_mal.jpg

4.1.29 ./simulationResults/gender.csv

Listing 4.7: gender.csv

```
gender,MEL,NV,BCC,AK,BKL,DF,VASC,SCC
female,650,2139,424,156,367,45,43,63
male,810,2087,654,163,504,27,41,142
unknown,31,85,3,1,8,0,0,0
```

4.1.30 ./simulationResults/gender_mal.jpg

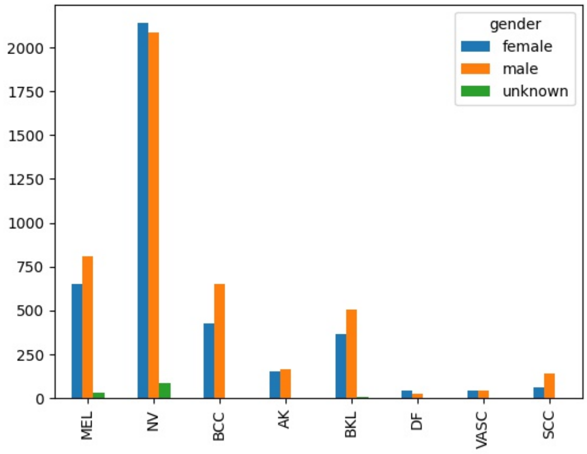


Figure 4.6: gender_mal.jpg

4.1.31 ./simulationResults/report.txt

Listing 4.8: report.txt

```
Stations have 8301 instances with complete attributes
Station has 142 instances whose attribute "age" is missing
Station has 0 instances whose attribute "gender" is missing
Station has 891 instances whose attribute "bodySite" is
   missing
```

4.1.32 ./simulationResults/age.csv

Listing 4.9: age.csv

```
,MEL,NV,BCC,AK,BKL,DF,VASC,SCC
lower quartile,51.0,36.0,56.0,61.0,56.0,46.0,41.0,66.0
median,61.0,46.0,71.0,71.0,66.0,56.0,56.0,71.0
upper quartile,76.0,56.0,81.0,76.0,76.0,66.0,71.0,81.0
```

4.1.33 ./simulationResults/a288a035-2d4c-457b-b8b5-17059f11a7c9-le64.cache-7

No Preview Available! https://git.rwth-aachen.de/padme-development/padme-train-depot/-/jobs/4570470/artifacts/file/simulationResults/a288a035-2d4c-457b-b8b5-17059f11a7c9-le64.cache-7

4.1.34 ./simulationResults/bba82c22-21b0-43a8-af05-c393282fb2b5-le64.cache-7

No Preview Available! `https://git.rwth-aachen.de/padme-development/padme-train-depot/-/jobs/4570470/artifacts/file/simulationResults/bba82c22-21b0-43a8-af05-c393282fb2b5-le64.cache-7`

4.1.35 ./simulationResults/2f889b71-f4f1-4601-8fc2-d0eb61f6b0d3-le64.cache-7

No Preview Available! `https://git.rwth-aachen.de/padme-development/padme-train-depot/-/jobs/4570470/artifacts/file/simulationResults/2f889b71-f4f1-4601-8fc2-d0eb61f6b0d3-le64.cache-7`

4.1.36 ./simulationResults/6a5fe70b-cbb3-46f8-b36b-d5ef1933402e-le64.cache-7

No Preview Available! `https://git.rwth-aachen.de/padme-development/padme-train-depot/-/jobs/4570470/artifacts/file/simulationResults/6a5fe70b-cbb3-46f8-b36b-d5ef1933402e-le64.cache-7`

4.2 Execution metrics:

- Maximum CPU Usage:3.890077356321839
- Maximum Memory Usage:102563840
- Maximum Number of PIDS:2

4.3 Network I/O:

- RX (Reading):7844432
- TX (Transmitting):241115

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

- Identified network traffic in dynamic analysis.
- 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]).

Audit Result

Train Rejected 🟥

January 31, 2024