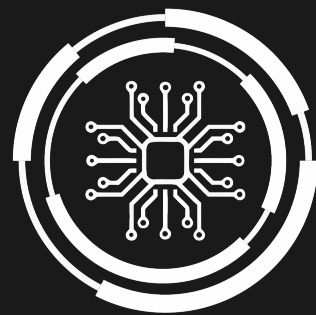


**PADME**

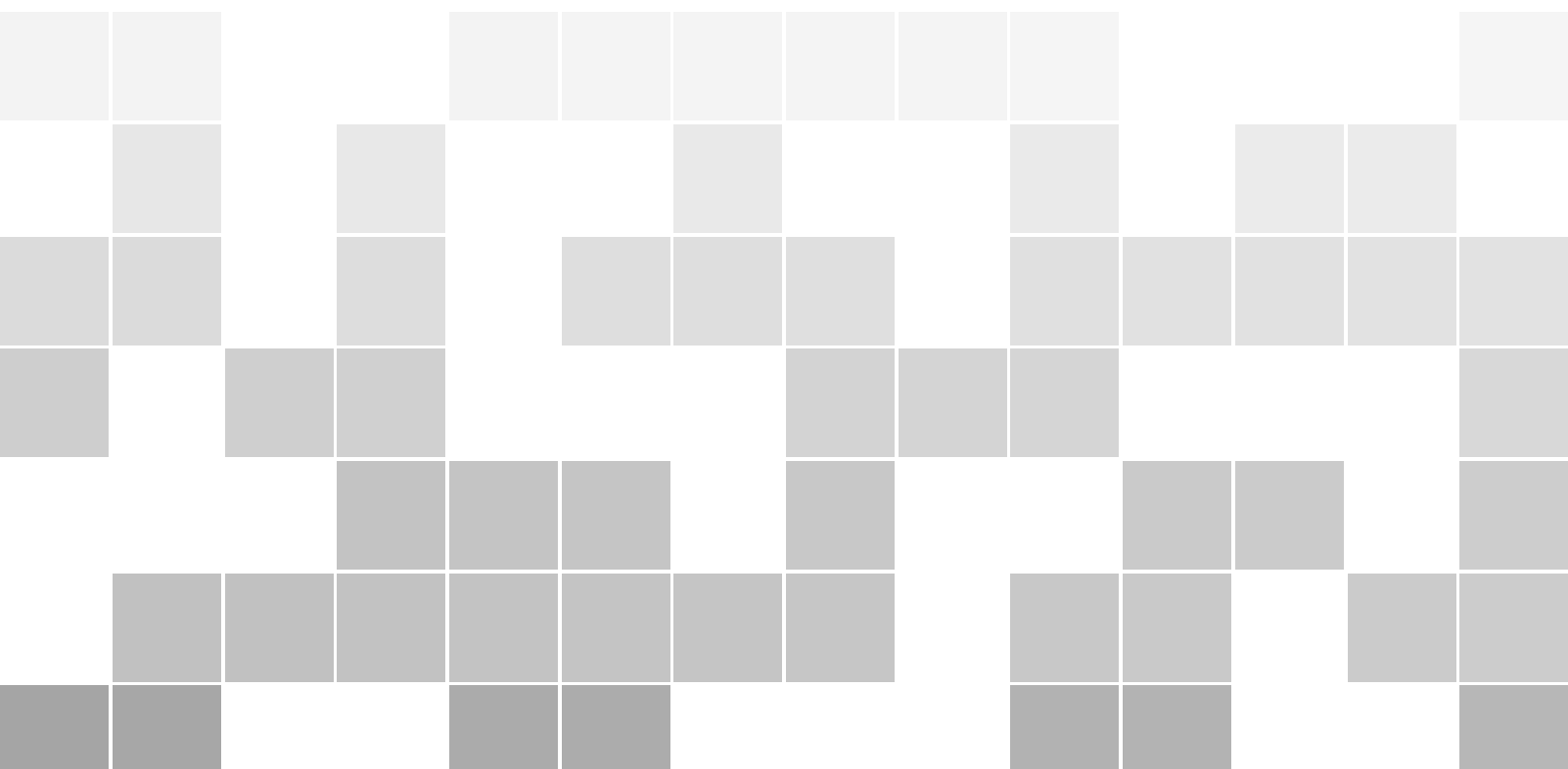
# Manual & Security Audit for Train

**SecretDetection**

Karl Kindermann



**PADME**

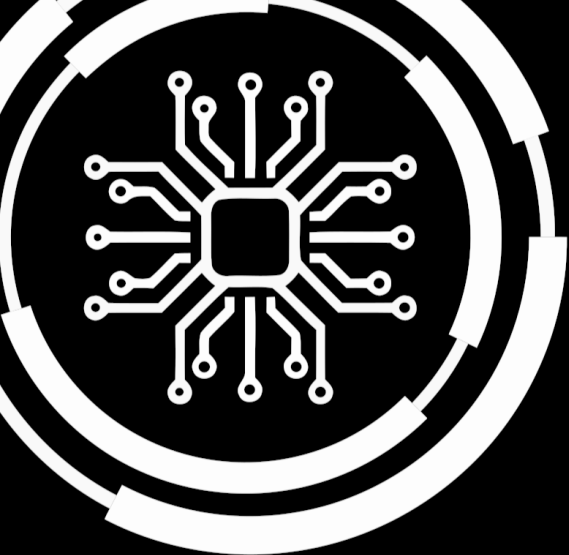


Copyright © 2023 PADME

PADME-ANALYTICS.DE

Licensed under the Creative Commons Attribution-NonCommercial 3.0 Unported License (the “License”). You may not use this file except in compliance with the License. You may obtain a copy of the License at <http://creativecommons.org/licenses/by-nc/3.0>. Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

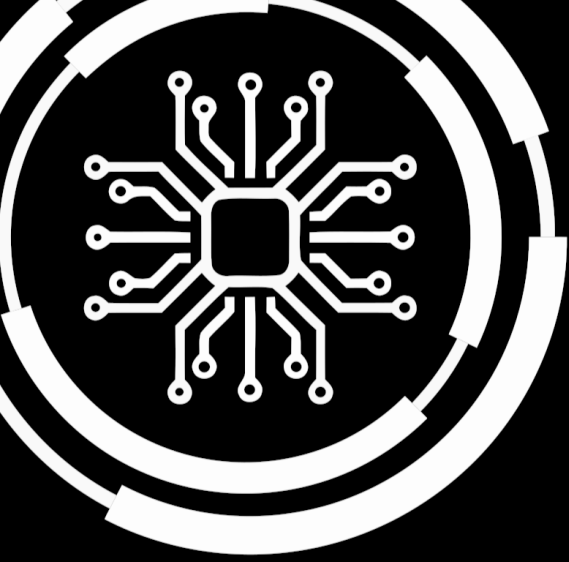
*First printing, February 1, 2024*



## Contents

<b>1</b>	<b>Train Summary .....</b>	<b>5</b>
1.1	Overview	5
1.2	Image Building File	5
1.3	Requirements & Dependencies	6
1.4	Code Base	6
1.5	Connection Parameters	6
<b>2</b>	<b>Static Train Analysis .....</b>	<b>7</b>
2.1	SAST	7
2.2	Secret Detection	8
2.3	Dependency Analysis	8
2.4	Blacklist Detection	8
<b>3</b>	<b>Train Image Analysis .....</b>	<b>9</b>
3.1	Vulnerabilities	9
<b>4</b>	<b>Dynamic Train Analysis .....</b>	<b>17</b>
<b>5</b>	<b>Conclusion .....</b>	<b>19</b>





## 1. Train Summary

### 1.1 Overview

- **Train name:** SecretDetection
- **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=SecretDetection>

### 1.2 Image Building File

Listing 1.1: Image building file

```
FROM python:3.11.7-slim

WORKDIR /usr/src/app

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

COPY . .

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

### 1.3 Requirements & Dependencies

No requirements.txt found

### 1.4 Code Base

Legend: **env** **query** **retrieve\_previous\_results** **execute\_analysis** **save** **log**

```

1  ssh_key = ""-----BEGIN OPENSSH PRIVATE KEY-----
2  b3BlbnNzaC1rZXktZjEAAAAABG5vbmUAAAAAEbm9uZQAAAAAAAAABAAABFwAAAAAdzc2gtcn
3  NhAAAAAwEAAQAAAEAyKAYR9Ri1choGsn4poF+P11zpiVgrH3a40T/ZwljddM/6taoxavE
4  mhrde6oL7nUiTOgoeJi3DQijRvd/bfy9YvUAKItE4GBvPYEhzTB00/ZCAIw8G92UORG0dr
5  etr9CQH4hZg3GQYb2bH/y/4fExGJeYQtvpdhhb28hEmUZAu4yhzj/TuZFkHAgfhwjULIHY
6  bR8q4diTQlqcfh20dBPnz0ENZpG5iX0izD/Y//HlkeHaLdQ5Unh3lWsV6S7yqtMbf3N5ee
7  Hf1mQinZi6wMWXga+dnvQ4ql2D2SpuodrWZs8cQbEbWKSxzsasqU2TdbnrcMS2rNCOT3hE
8  2MEXloBQAAAA+hddieAXXYngAAAAAdzc2gtcnNhAAABAQDKQBhH1GLVyGgayfimgX4/XX
9  0mJWCsfdrjRP9nCWN10z/q1qjFq8SaGt17qgvudSJM6Ch4mLcNCKNG939t/L1i9QCQi0Tg
10 YG89gSHNME479kIAjDwb3ZTREbR2t62v0JAeniFmDcZBhvZsf/L/h8TEYl5hC2+12FvbyE
11 SZRkC7jKHOP905kWQcCCF/CNQsgdhtHyrh2JNCWpx+HY50E83M4Q1mkbmJc6LMP9j/8eWR
12 4dot1DlSeHeVaxXpLvKq0xt/c3l54d/WZCKdmlrAxZeBr52e9DiqXYPZKm6h2tZmzxxBsR
13 tYpLHOxqypTZN1uetwxLas0I5PeETy4ReWgFBAAAAAwEAAQAAAEAjkt9m7MTLBI5oEt
14 NT7x+fT2nFUD08qlivkMmTUusAF/33CSFeUPEMEhVq6NYkLV/rK7NV0bW+30NouihfjdkU
15 cyFXYSH2Mq3TItN9y7S/5k6L8e7DkfwqNLJ0xK9Bnu4sYmyBU50vb7urAp3mXv93Xvh3Av
16 pP8nuSCik/qsCuzAK/UPntr/KcpInTmEKh4HcG+shs01yygLSb/2vfL4Xfg2DrwKzpIkIH
17 MB0jq4amkNwWySoGkfSQZkFDWFdhNloE2hpjx9S19skwNNHeCruHnK1w4RFYB08yKtyaa+
18 BK1BhQyhdpdKukWgkC4PN69ePY5nrFXWptNA5enGYGODOQAAAIb5H8vShdt6aLroM2IOBc
19 /MsbPa0eZvbxeds1PcRFZN81JdG52xqbcZBB0jocW478jCQXKbswULuSBQeJuQY+MHRUkq
20 EgHKcKzFAP9rIkpqSK81YLZAAeTTPNA6JNwJ5Jq0Y5aht2j6bjwBmnIG2pxro3sC4Pzeds
21 UCZ//WWWHCAAAAAIEA6b4xuLsor52YkF29JpzFA2pbt8n5WCZpXQu001Fi3NTKgtU/Au5S
22 kKG0gvs3Ruoa85bVZ06L7ywCD54o468qEE6QIEVPYU7PgEvT3JkQk3Uk5c9rd685qK4f69
23 MUPuB0/wpdaxYcOK2W774FnFR79fGnmTCB+Ipe2/Cuy4xtLUAAACBAN2C0cyKaHkYa/ap
24 YwaTS+WcJck20egQUS2K2k5w0Q5x905tnSGb5lyyARgXPpxGHIwfa3ptk2WR87cGQgcwFS
25 CwqDrgTqlmfZ1DYKDLpi1MdQTu2lujYXzR5V8miQFCh8uuxhn4RlXIiBV0wT3W5aZiFwK
26 kFNTUujmSmVr5p3dAAAAALWthcmxraW5kZXJtYW5uQDA2NS0xODguZWR1cm9hbS5yd3RoLW
27 FhY2hlbi5kZQECAwQF
28 -----END OPENSSH PRIVATE KEY-----""
29 aws_secret_key = "AKIA1B2C3D4E5F6G7H8I9J0K1L2M3N4O5P6Q7R8S9T0"
30
31 print(ssh_key)
32 print(aws_secret_key)

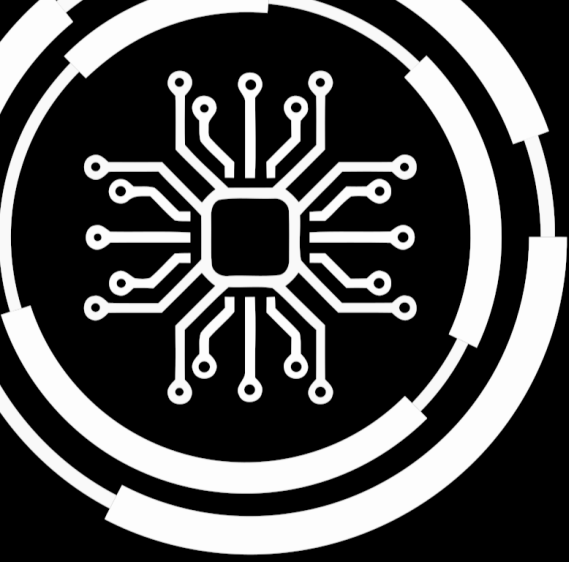
```

Listing 1.2: main.py

### 1.5 Connection Parameters

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

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



## 2. Static Train Analysis

### Summary 2.1

- **Number of Lines:** 223847
- **Vulnerabilities per Line:** 3.5e-05
- **Analysis Score:** 1.0

#### Total

Summary: Low: 0 Medium: 0 High: 0

### 2.1 SAST

Summary: Low: 0 Medium: 0 High: 0

#### Detailed Vulnerabilities:

### Vulnerability 2.1

**Test-specific ID:** 4099944ca7baf64e63e878f6de549c10abe426a2cbe5688e7f33170908e1f6fb

**Severity:** Info

#### Identifiers:

- **semgrep\_id:** bandit.B105
- **cwe:** 259
- **owasp:** A3
- **bandit\_test\_id:** B105

**Message:** Use of Hard-coded Password

**File:** SecretDetection/main.py

**Start line:** 29

## 2.2 Secret Detection

Summary: Low: 0 Medium: 0 High: 0

Detailed Secret Detection:

### Secret Detection 2.1

Test-specific ID: 2a1df70f7f1b525e915e2a4966d33cf9e6ccd7e5b4f11b17bbc760d1c20679c6

Severity: Critical

Identifiers:

- gitleaks\_rule\_id: SSH private key

File:SecretDetection/main.py

Start line: 1

## 2.3 Dependency Analysis

Summary: Low: 0 Medium: 0 High: 0

Detailed Dependency Analysis:

## 2.4 Blacklist Detection

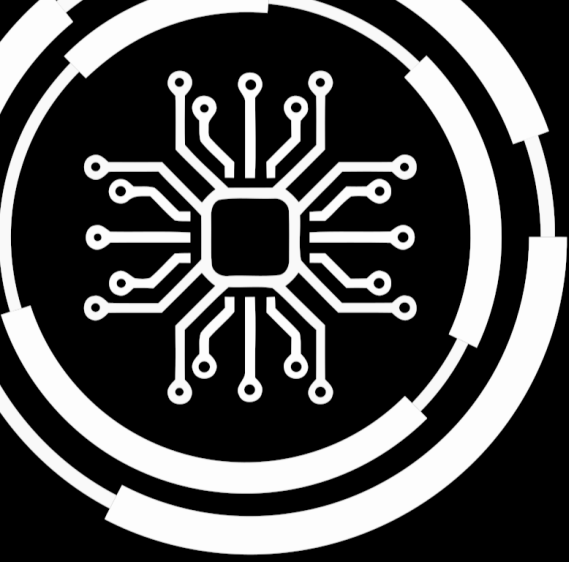
The following patterns have been configured:

\bPOST\b

The following matches have been found:

None





## 3. Train Image Analysis

### 3.1 Vulnerabilities

Summary: Low: 45 Medium: 0 High: 0 Critical: 1

#### Detailed Vulnerabilities:

##### Critical:

#### Vulnerability 3.1

**Test-specific ID:** SNYK-DEBIAN12-ZLIB-6008963 **Severity:** critical

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

##### High:

##### Medium:

##### Low:

#### Vulnerability 3.2

**Test-specific ID:** SNYK-DEBIAN12-APT-1541449 **Severity:** low

**Identifiers:** Message:Improper Verification of Cryptographic Signature

#### Vulnerability 3.3

**Test-specific ID:** SNYK-DEBIAN12-COREUTILS-1543939 **Severity:** low

**Identifiers:** Message:Improper Input Validation

### Vulnerability 3.4

**Test-specific ID:** SNYK-DEBIAN12-COREUTILS-1543947 **Severity:** low

**Identifiers:** **Message:**Race Condition

### Vulnerability 3.5

**Test-specific ID:** SNYK-DEBIAN12-GCC12-2606941 **Severity:** low

**Identifiers:** **Message:**Uncontrolled Recursion

### Vulnerability 3.6

**Test-specific ID:** SNYK-DEBIAN12-GCC12-5901316 **Severity:** low

**Identifiers:** **Message:**CVE-2023-4039

### Vulnerability 3.7

**Test-specific ID:** SNYK-DEBIAN12-GLIBC-1546991 **Severity:** low

**Identifiers:** **Message:**Information Exposure

### Vulnerability 3.8

**Test-specific ID:** SNYK-DEBIAN12-GLIBC-1547039 **Severity:** low

**Identifiers:** **Message:**Uncontrolled Recursion

### Vulnerability 3.9

**Test-specific ID:** SNYK-DEBIAN12-GLIBC-1547069 **Severity:** low

**Identifiers:** **Message:**Uncontrolled Recursion

### Vulnerability 3.10

**Test-specific ID:** SNYK-DEBIAN12-GLIBC-1547135 **Severity:** low

**Identifiers:** **Message:**Use of Insufficiently Random Values

### Vulnerability 3.11

**Test-specific ID:** SNYK-DEBIAN12-GLIBC-1547196 **Severity:** low

**Identifiers:** **Message:** Out-of-Bounds

### Vulnerability 3.12

**Test-specific ID:** SNYK-DEBIAN12-GLIBC-1547293 **Severity:** low

**Identifiers:** **Message:** Resource Management Errors

### Vulnerability 3.13

**Test-specific ID:** SNYK-DEBIAN12-GLIBC-1547373 **Severity:** low

**Identifiers:** **Message:** CVE-2019-1010023

### Vulnerability 3.14

**Test-specific ID:** SNYK-DEBIAN12-GNUPG2-3330747 **Severity:** low

**Identifiers:** **Message:** Out-of-bounds Write

### Vulnerability 3.15

**Test-specific ID:** SNYK-DEBIAN12-GNUTLS28-1547121 **Severity:** low

**Identifiers:** **Message:** Improper Input Validation

### Vulnerability 3.16

**Test-specific ID:** SNYK-DEBIAN12-GNUTLS28-6159410 **Severity:** low

**Identifiers:** **Message:** Improper Verification of Cryptographic Signature

### Vulnerability 3.17

**Test-specific ID:** SNYK-DEBIAN12-GNUTLS28-6159418 **Severity:** low

**Identifiers:** **Message:** Information Exposure

### Vulnerability 3.18

**Test-specific ID:** SNYK-DEBIAN12-KRB5-1549480 **Severity:** low

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

### Vulnerability 3.19

**Test-specific ID:** SNYK-DEBIAN12-LIBGCRYPT20-1550206 **Severity:** low

**Identifiers:** **Message:**Use of a Broken or Risky Cryptographic Algorithm

### Vulnerability 3.20

**Test-specific ID:** SNYK-DEBIAN12-NCURSES-6123823 **Severity:** low

**Identifiers:** **Message:**CVE-2023-50495

### Vulnerability 3.21

**Test-specific ID:** SNYK-DEBIAN12-OPENSSL-1555825 **Severity:** low

**Identifiers:** **Message:**Cryptographic Issues

### Vulnerability 3.22

**Test-specific ID:** SNYK-DEBIAN12-OPENSSL-1555907 **Severity:** low

**Identifiers:** **Message:**Cryptographic Issues

### Vulnerability 3.23

**Test-specific ID:** SNYK-DEBIAN12-OPENSSL-6048820 **Severity:** low

**Identifiers:** **Message:**Improper Check for Unusual or Exceptional Conditions

### Vulnerability 3.24

**Test-specific ID:** SNYK-DEBIAN12-OPENSSL-6148845 **Severity:** low

**Identifiers:** **Message:**Out-of-bounds Write

### Vulnerability 3.25

**Test-specific ID:** SNYK-DEBIAN12-OPENSSL-6157243 **Severity:** low

**Identifiers:** **Message:**CVE-2023-6237

### Vulnerability 3.26

**Test-specific ID:** SNYK-DEBIAN12-OPENSSL-6190223 **Severity:** low

**Identifiers:** **Message:**CVE-2024-0727

### Vulnerability 3.27

**Test-specific ID:** SNYK-DEBIAN12-PAM-6178914 **Severity:** low

**Identifiers:** **Message:**CVE-2024-22365

### Vulnerability 3.28

**Test-specific ID:** SNYK-DEBIAN12-PERL-1556505 **Severity:** low

**Identifiers:** **Message:**Link Following

### Vulnerability 3.29

**Test-specific ID:** SNYK-DEBIAN12-PERL-5489184 **Severity:** low

**Identifiers:** **Message:**Improper Certificate Validation

### Vulnerability 3.30

**Test-specific ID:** SNYK-DEBIAN12-PERL-5489190 **Severity:** low

**Identifiers:** **Message:**Improper Certificate Validation

### Vulnerability 3.31

**Test-specific ID:** SNYK-DEBIAN12-SHADOW-1559391 **Severity:** low

**Identifiers:** **Message:**Access Restriction Bypass

### Vulnerability 3.32

**Test-specific ID:** SNYK-DEBIAN12-SHADOW-1559403 **Severity:** low

**Identifiers:** **Message:**Incorrect Permission Assignment for Critical Resource

### Vulnerability 3.33

**Test-specific ID:** SNYK-DEBIAN12-SHADOW-5423923 **Severity:** low

**Identifiers:** **Message:**Arbitrary Code Injection

### Vulnerability 3.34

**Test-specific ID:** SNYK-DEBIAN12-SHADOW-5879156 **Severity:** low

**Identifiers:** **Message:**Improper Authentication

### Vulnerability 3.35

**Test-specific ID:** SNYK-DEBIAN12-SQLITE3-2407042 **Severity:** low

**Identifiers:** **Message:**Memory Leak

### Vulnerability 3.36

**Test-specific ID:** SNYK-DEBIAN12-SQLITE3-6139924 **Severity:** low

**Identifiers:** **Message:**Out-of-Bounds

### Vulnerability 3.37

**Test-specific ID:** SNYK-DEBIAN12-SQLITE3-6155400 **Severity:** low

**Identifiers:** **Message:**Use After Free

### Vulnerability 3.38

**Test-specific ID:** SNYK-DEBIAN12-SYSTEMD-1560739 **Severity:** low

**Identifiers:** **Message:**Link Following

### Vulnerability 3.39

**Test-specific ID:** SNYK-DEBIAN12-SYSTEMD-5733385 **Severity:** low

**Identifiers:** **Message:**Improper Validation of Integrity Check Value

### Vulnerability 3.40

**Test-specific ID:** SNYK-DEBIAN12-SYSTEMD-5733390 **Severity:** low

**Identifiers:** **Message:**Improper Validation of Integrity Check Value

### Vulnerability 3.41

**Test-specific ID:** SNYK-DEBIAN12-SYSTEMD-5733398 **Severity:** low

**Identifiers:** **Message:**Improper Validation of Integrity Check Value

### Vulnerability 3.42

**Test-specific ID:** SNYK-DEBIAN12-SYSTEMD-6137714 **Severity:** low

**Identifiers:** **Message:**CVE-2023-7008

### Vulnerability 3.43

**Test-specific ID:** SNYK-DEBIAN12-TAR-1560620 **Severity:** low

**Identifiers:** **Message:**CVE-2005-2541

### Vulnerability 3.44

**Test-specific ID:** SNYK-DEBIAN12-TAR-3253526 **Severity:** low

**Identifiers:** **Message:**Out-of-bounds Read

### Vulnerability 3.45

**Test-specific ID:** SNYK-DEBIAN12-TAR-6120422 **Severity:** low

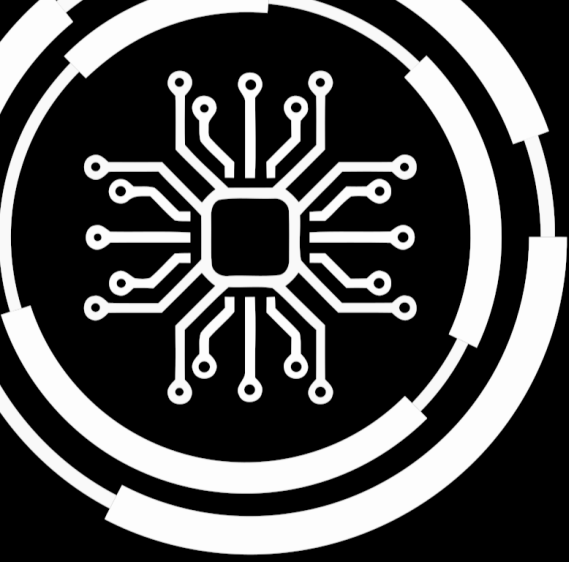
**Identifiers:** **Message:**CVE-2023-39804

## Vulnerability 3.46

**Test-specific ID:** SNYK-DEBIAN12-UTILLINUX-2401083 **Severity:** low

**Identifiers:** **Message:**Information Exposure

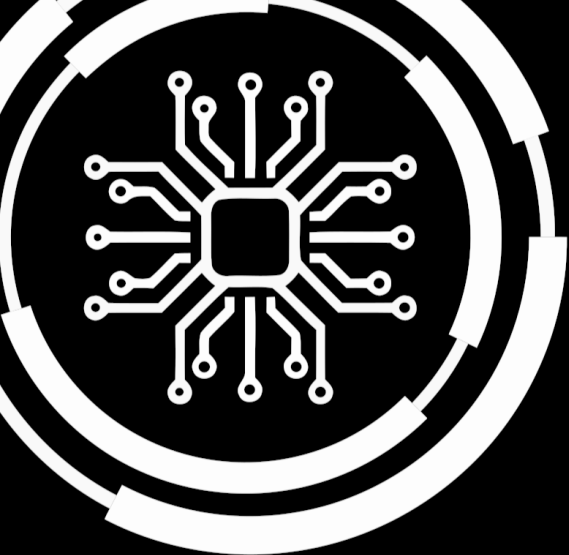




## 4. Dynamic Train Analysis

No Dynamic Report Available





## 5. Conclusion

The PADME Security Audit has come to the following conclusion:

Static Complete	SAST	Dependencies	Secret Detection

Standard Compliant	Blacklist	Train Image Analysis	DAST

### Warnings

- Found 1 critical vulnerability in the static 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>]).
- The reports dynamic\_report.json are missing. Acceptance threshold increased from 0.5 to 0.75.

### Audit Result

**Train Rejected**

February 1, 2024

