Status
Changes
Console Output
Edit Build Information
Delete build '#62'
Timings
Git Build Data
Pipeline Overview
Pipeline Console
Restart from Stage
Replay
Pipeline Steps
Workspaces
Previous Build

Console Output

Download Copy View as plain text

Skipping 17 KB.. Full Log

```
INFO: Hit the cache for 0 out of 0
INFO: Miss the cache for 0 out of 0
INFO: Sensor JavaScript inside YAML analysis [javascript] (done) |
time=21ms
INFO: Sensor JavaScript inside HTML analysis [javascript]
INFO: Detected os: Linux arch: amd64 alpine: false. Platform: LINUX_X64
INFO: Deploy location /var/lib/jenkins/.sonar/js/node-runtime,
tagetRuntime: /var/lib/jenkins/.sonar/js/node-runtime/node,  version:
/var/lib/jenkins/.sonar/js/node-runtime/version.txt
INFO: Using embedded Node.js runtime.
INFO: Using Node.js executable: '/var/lib/jenkins/.sonar/js/node-
runtime/node'.
INFO: Memory configuration: OS (7821 MB), Node.js (2096 MB).
INFO: 1 source file to be analyzed
INFO: 1/1 source file has been analyzed
INFO: Hit the cache for 0 out of 1
INFO: Miss the cache for 1 out of 1: ANALYSIS_MODE_INELIGIBLE [1/1]
INFO: Sensor JavaScript inside HTML analysis [javascript] (done) |
time=4457ms
INFO: Sensor CSS Rules [javascript]
INFO: 1 source file to be analyzed
```

```
INFO: 1/1 source file has been analyzed
INFO: Hit the cache for 0 out of 0
INFO: Miss the cache for 0 out of 0
INFO: Sensor CSS Rules [javascript] (done) | time=83ms
INFO: Sensor IaC Docker Sensor [iac]
INFO: 1 source file to be analyzed
INFO: 1/1 source file has been analyzed
INFO: Sensor IaC Docker Sensor [iac] (done) | time=199ms
INFO: Sensor TextAndSecretsSensor [text]
INFO: Available processors: 5
INFO: Using 5 threads for analysis.
INFO: The property "sonar.tests" is not set. To improve the analysis
accuracy, we categorize a file as a test file if any of the following is
true:
  * The filename starts with "test"
  * The filename contains "test." or "tests."
  * Any directory in the file path is named: "doc", "docs", "test" or
"tests"
  * Any directory in the file path has a name ending in "test" or "tests"

INFO: Using git CLI to retrieve untracked files
INFO: Analyzing language associated files and files included via
"sonar.text.inclusions" that are tracked by git
INFO: 4 source files to be analyzed
INFO: 4/4 source files have been analyzed
INFO: Sensor TextAndSecretsSensor [text] (done) | time=681ms
INFO: ------------- Run sensors on project
INFO: Sensor Zero Coverage Sensor
INFO: Sensor Zero Coverage Sensor (done) | time=0ms
INFO: CPD Executor Calculating CPD for 1 file
```

```
INFO: CPD Executor CPD calculation finished (done) | time=26ms
INFO: SCM revision ID '39aaf427391c717b15d50abb27923c2ed1a8e0d8'
INFO: Analysis report generated in 188ms, dir size=282.6 kB
INFO: Analysis report compressed in 30ms, zip size=41.0 kB
INFO: Analysis report uploaded in 113ms
INFO: ANALYSIS SUCCESSFUL, you can find the results at:
http://localhost:9000/dashboard?id=sample_project
INFO: Note that you will be able to access the updated dashboard once the
server has processed the submitted analysis report
INFO: More about the report processing at
http://localhost:9000/api/ce/task?id=ed2ebcd8-3243-4e9d-9b4a-9b8a4cee1d03
INFO: Analysis total time: 13.740 s
INFO: ------------------------------------------------------------------------
----
INFO: EXECUTION SUCCESS
INFO: ------------------------------------------------------------------------
----
INFO: Total time: 19.062s
INFO: Final Memory: 15M/54M
INFO: ------------------------------------------------------------------------
----
[Pipeline] }
[Pipeline] // script
[Pipeline] }
[Pipeline] // withCredentials
[Pipeline] }
[Pipeline] // stage
[Pipeline] stage
[Pipeline] { (Build Docker Image)
[Pipeline] script
```

Dashboard > CDAC-PROJECT > #62

```
[Pipeline] {
[Pipeline] sh
+ docker build -t srush634/docker-webapp:latest .
#0 building with "default" instance using docker driver

#1 [internal] load build definition from Dockerfile
#1 transferring dockerfile: 101B done
#1 DONE 0.1s

#2 [internal] load metadata for docker.io/library/httpd:latest
#2 ...

#3 [auth] library/httpd:pull token for registry-1.docker.io
#3 DONE 0.0s

#2 [internal] load metadata for docker.io/library/httpd:latest
#2 DONE 2.0s

#4 [internal] load .dockerignore
#4 transferring context: 2B done
#4 DONE 0.0s

#5 [1/2] FROM
docker.io/library/httpd:latest@sha256:3195404327ecd95b2fa0a5d4eac1f2206bb1
2996fb2561393f91254759e422b9
#5 DONE 0.0s

#6 [internal] load build context
#6 transferring context: 33B 0.0s done
#6 DONE 0.0s
```

```
#7 [2/2] COPY index.html /usr/local/apache2/htdocs/
#7 CACHED

#8 exporting to image
#8 exporting layers done
#8 writing image
sha256:7a0c7cd2f4dc394cf6494839da7a78b5499746a823a2ad291bc39364d423fe9a
0.0s done
#8 naming to docker.io/srush634/docker-webapp:latest 0.0s done
#8 DONE 0.0s
[Pipeline] }
[Pipeline] // script
[Pipeline] }
[Pipeline] // stage
[Pipeline] stage
[Pipeline] { (Security Scan - Trivy)
[Pipeline] script
[Pipeline] {
[Pipeline] sh
+ trivy image srush634/docker-webapp:latest
2025-02-11T16:18:01+05:30       INFO    [vuln] Vulnerability scanning is
enabled
2025-02-11T16:18:01+05:30       INFO    [secret] Secret scanning is
enabled
2025-02-11T16:18:01+05:30       INFO    [secret] If your scanning is slow,
please try '--scanners vuln' to disable secret scanning
2025-02-11T16:18:01+05:30       INFO    [secret] Please see also
https://aquasecurity.github.io/trivy/v0.59/docs/scanner/secret#recommendat
ion for faster secret detection
```

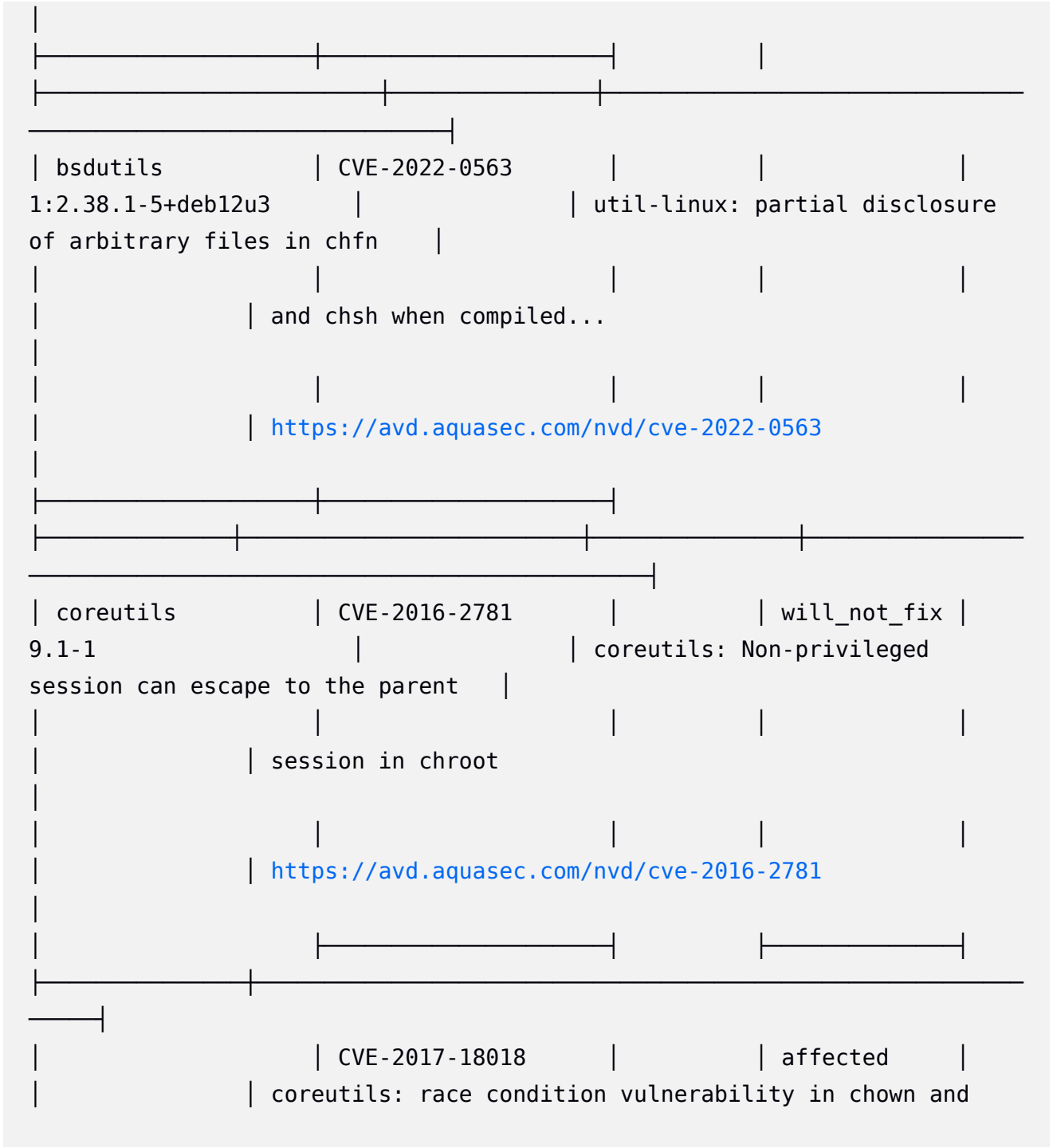
```
2025-02-11T16:18:01+05:30       INFO    Detected OS     family="debian"
version="12.9"
2025-02-11T16:18:01+05:30       INFO    [debian] Detecting
vulnerabilities...      os_version="12" pkg_num=116
2025-02-11T16:18:02+05:30       INFO    Number of language-specific files
num=0
2025-02-11T16:18:02+05:30       WARN    Using severities from other
vendors for some vulnerabilities. Read
https://aquasecurity.github.io/trivy/v0.59/docs/scanner/vulnerability#severity-selection for details.

For OSS Maintainers: VEX Notice
--------------------------------
If you're an OSS maintainer and Trivy has detected vulnerabilities in your
project that you believe are not actually exploitable, consider issuing a
VEX (Vulnerability Exploitability eXchange) statement.
VEX allows you to communicate the actual status of vulnerabilities in your
project, improving security transparency and reducing false positives for
your users.
Learn more and start using VEX:
https://aquasecurity.github.io/trivy/v0.59/docs/supply-chain/vex/repo#publishing-vex-documents

To disable this notice, set the TRIVY_DISABLE_VEX_NOTICE environment
variable.


srush634/docker-webapp:latest (debian 12.9)
==========================================
Total: 129 (UNKNOWN: 0, LOW: 89, MEDIUM: 29, HIGH: 10, CRITICAL: 1)
```

```
┌──────────────────────┬──────────────────────┬──────────┬──────────────┬──────
──────────────────────┬──────────────────┬──────────────────────────────────────
──────────────────────┐
│      Library         │    Vulnerability     │ Severity │    Status    │
Installed Version    │ Fixed Version │                                Title
│
├──────────────────────┼──────────────────────┼──────────┼──────────────┼──────
──────────────────────┼──────────────────┼──────────────────────────────────────
──────────────────────┤
│ apt                  │ CVE-2011-3374        │ LOW      │ affected     │
2.6.1                   │                  │ It was found that apt-key in
apt, all versions, do not       │
│                      │                      │          │              │
│                 │ correctly...
│
│                      │                      │          │              │
│                 │ https://avd.aquasec.com/nvd/cve-2011-3374
│
├──────────────────────┼──────────────────────┤          │
├──────────────────────┼──────────────────┼──────────────────────────────────────
──────────────────────┤
│ bash                 │ TEMP-0841856-B18BAF  │          │              │
5.2.15-2+b7             │                  │ [Privilege escalation possible
to other user than root]      │
│                      │                      │          │              │
│                 │ https://security-tracker.debian.org/tracker/TEMP-
0841856-B1- │
│                      │                      │          │              │
│                 │ 8BAF
```


bsdutils | CVE-2022-0563 | | | 1:2.38.1-5+deb12u3 | | util-linux: partial disclosure of arbitrary files in chfn
and chsh when compiled...
https://avd.aquasec.com/nvd/cve-2022-0563
coreutils | CVE-2016-2781 | | will_not_fix | 9.1-1 | | coreutils: Non-privileged session can escape to the parent
session in chroot
https://avd.aquasec.com/nvd/cve-2016-2781
CVE-2017-18018 | | affected |
coreutils: race condition vulnerability in chown and

```
chgrp   │
│                    │                       │          │              │
│               │ https://avd.aquasec.com/nvd/cve-2017-18018
│
├────────────────────┼───────────────────────┤          │
├──────────────────────────┼──────────────────┼──────────────────────────────
──────────────────────────┤
│ gcc-12-base        │ CVE-2022-27943      │          │              │
12.2.0-14               │               │ binutils: libiberty/rust-
demangle.c in GNU GCC 11.2 allows   │
│                    │                       │          │              │
│               │ stack exhaustion in demangle_const
│
│                    │                       │          │              │
│               │ https://avd.aquasec.com/nvd/cve-2022-27943
│
│                    ├───────────────────────┤          │              │
├────────────────┼──────────────────────────────────────────────────────────
────┤
│                    │ CVE-2023-4039       │          │              │
│               │ gcc: -fstack-protector fails to guard dynamic stack
│
│                    │                       │          │              │
│               │ allocations on ARM64
│
│                    │                       │          │              │
│               │ https://avd.aquasec.com/nvd/cve-2023-4039
│
├────────────────────┼───────────────────────┤          │
├──────────────────────────┼──────────────────┼──────────────────────────────
──────────────────────────┤
```

```
──────────────────────────────────┤
│ gpgv                │ CVE-2022-3219       │          │              │
2.2.40-1.1               │               │ gnupg: denial of service issue
(resource consumption) using  │
│                     │                     │          │              │
│                │ compressed packets
│
│                     │                     │          │              │
│                │ https://avd.aquasec.com/nvd/cve-2022-3219
│
├─────────────────────┼─────────────────────┤          │
├──────────────────────────┼─────────────────┼──────────────────────────────
──────────────────────────────────┤
│ libapt-pkg6.0       │ CVE-2011-3374       │          │              │
2.6.1                    │               │ It was found that apt-key in
apt, all versions, do not       │
│                     │                     │          │              │
│                │ correctly...
│
│                     │                     │          │              │
│                │ https://avd.aquasec.com/nvd/cve-2011-3374
│
├─────────────────────┼─────────────────────┤          │
├──────────────────────────┼─────────────────┼──────────────────────────────
──────────────────────────────────┤
│ libblkid1           │ CVE-2022-0563       │          │              │
2.38.1-5+deb12u3         │               │ util-linux: partial disclosure
of arbitrary files in chfn    │
│                     │                     │          │              │
│                │ and chsh when compiled...
```

```
|
|                  |                     |          |              |
|              | https://avd.aquasec.com/nvd/cve-2022-0563
|
├──────────────────┼─────────────────────┼──────────┤
├──────────────────────────┼──────────────────┼──────────────────────────────
──────────────────────────────┤
| libc-bin           | CVE-2025-0395       | MEDIUM   |              |
2.36-9+deb12u9          |               | glibc: buffer overflow in the
GNU C Library's assert()       |
|                  |                     |          |              |
|              | https://avd.aquasec.com/nvd/cve-2025-0395
|
|                  ├─────────────────────┼──────────┤              |
├──────────────┼──────────────────────────────────────────────────────────────
────┤
|                  | CVE-2010-4756       | LOW      |              |
|              | glibc: glob implementation can cause excessive CPU and
|
|                  |                     |          |              |
|              | memory consumption due to...
|
|                  |                     |          |              |
|              | https://avd.aquasec.com/nvd/cve-2010-4756
|
|                  ├─────────────────────┤          |              |
├──────────────┼──────────────────────────────────────────────────────────────
────┤
|                  | CVE-2018-20796      |          |              |
|              | glibc: uncontrolled recursion in function
```


check_dst_limits_calc_pos_1 in posix/regexec.c
https://avd.aquasec.com/nvd/cve-2018-20796
CVE-2019-1010022
glibc: stack guard protection bypass
https://avd.aquasec.com/nvd/cve-2019-1010022
CVE-2019-1010023
glibc: running ldd on malicious ELF leads to code execution
because of...
https://avd.aquasec.com/nvd/cve-2019-1010023

```
─────┤
|                    | CVE-2019-1010024    |          |              |
|                | glibc: ASLR bypass using cache of thread stack and heap
|
|                    |                     |          |              |
|                | https://avd.aquasec.com/nvd/cve-2019-1010024
|
|                    |─────────────────────|          |              |
|──────────────|──────────────────────────────────────────────────────────
─────┤
|                    | CVE-2019-1010025    |          |              |
|                | glibc: information disclosure of heap addresses of
|
|                    |                     |          |              |
|                | pthread_created thread
|
|                    |                     |          |              |
|                | https://avd.aquasec.com/nvd/cve-2019-1010025
|
|                    |─────────────────────|          |              |
|──────────────|──────────────────────────────────────────────────────────
─────┤
|                    | CVE-2019-9192       |          |              |
|                | glibc: uncontrolled recursion in function
|
|                    |                     |          |              |
|                | check_dst_limits_calc_pos_1 in posix/regexec.c
|
|                    |                     |          |              |
|                | https://avd.aquasec.com/nvd/cve-2019-9192
```

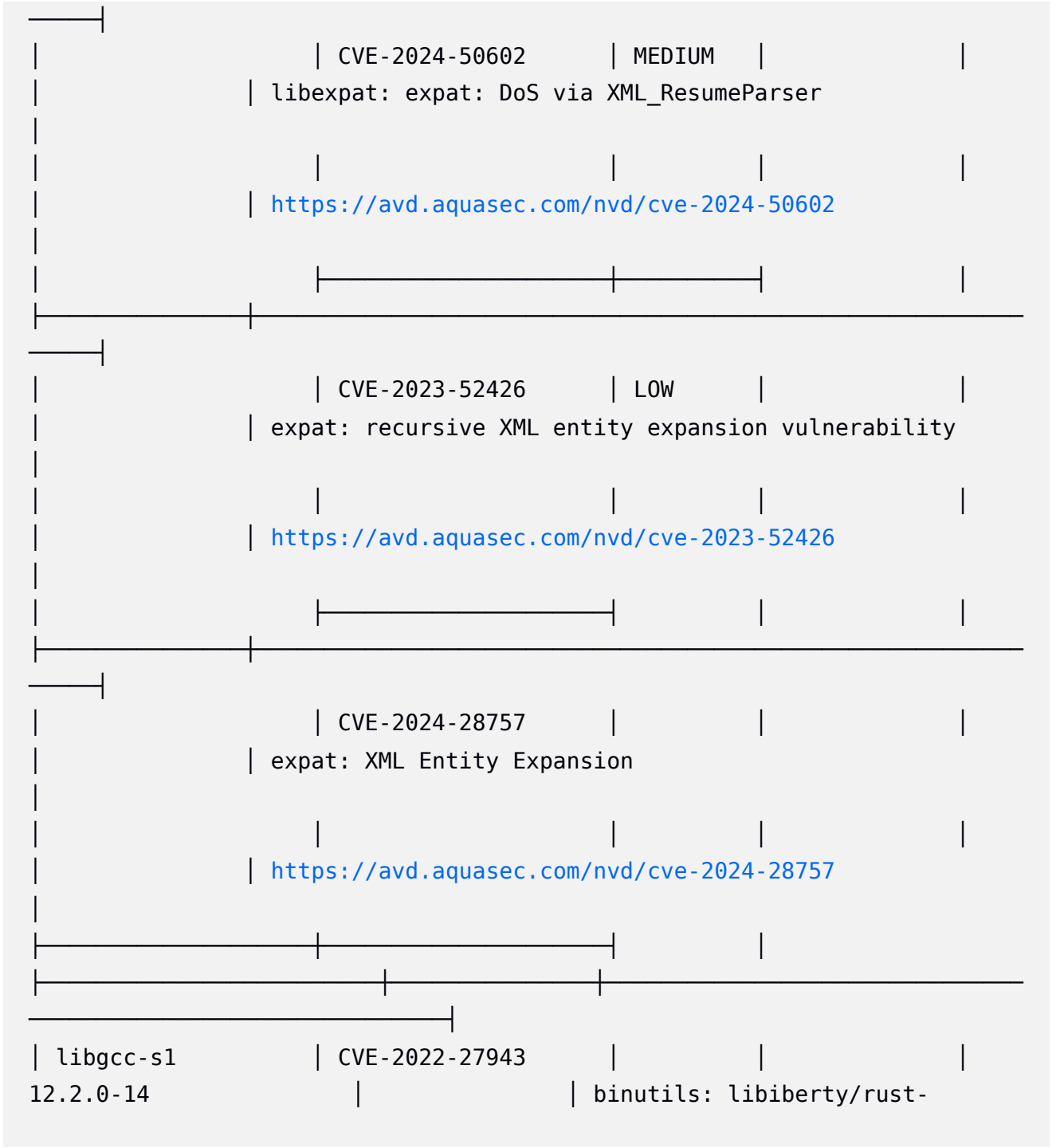
```
│
├────────────────────┼──────────────────────┼──────────┤              │
├───────────────┼──────────────────────────────────────────────────────
─────┤
│ libc6               │ CVE-2025-0395        │ MEDIUM   │              │
│               │ glibc: buffer overflow in the GNU C Library's assert()
│
│                     │                      │          │              │
│               │ https://avd.aquasec.com/nvd/cve-2025-0395
│
│                     ├──────────────────────┼──────────┤              │
├───────────────┼──────────────────────────────────────────────────────
─────┤
│                     │ CVE-2010-4756        │ LOW      │              │
│               │ glibc: glob implementation can cause excessive CPU and
│
│                     │                      │          │              │
│               │ memory consumption due to...
│
│                     │                      │          │              │
│               │ https://avd.aquasec.com/nvd/cve-2010-4756
│
│                     ├──────────────────────┤          │              │
├───────────────┼──────────────────────────────────────────────────────
─────┤
│                     │ CVE-2018-20796       │          │              │
│               │ glibc: uncontrolled recursion in function
│
│                     │                      │          │              │
│               │ check_dst_limits_calc_pos_1 in posix/regexec.c
```

```
|
|                    |                    |          |              |
|               | https://avd.aquasec.com/nvd/cve-2018-20796
|
|                    |--------------------|          |              |
|--------------|-----------------------------------------------------------
-----|
|                    | CVE-2019-1010022   |          |              |
|               | glibc: stack guard protection bypass
|
|                    |                    |          |              |
|               | https://avd.aquasec.com/nvd/cve-2019-1010022
|
|                    |--------------------|          |              |
|--------------|-----------------------------------------------------------
-----|
|                    | CVE-2019-1010023   |          |              |
|               | glibc: running ldd on malicious ELF leads to code
execution  |
|                    |                    |          |              |
|               | because of...
|
|                    |                    |          |              |
|               | https://avd.aquasec.com/nvd/cve-2019-1010023
|
|                    |--------------------|          |              |
|--------------|-----------------------------------------------------------
-----|
|                    | CVE-2019-1010024   |          |              |
|               | glibc: ASLR bypass using cache of thread stack and heap
```


https://avd.aquasec.com/nvd/cve-2019-1010024
CVE-2019-1010025
glibc: information disclosure of heap addresses of
pthread_created thread
https://avd.aquasec.com/nvd/cve-2019-1010025
CVE-2019-9192
glibc: uncontrolled recursion in function
check_dst_limits_calc_pos_1 in posix/regexec.c
https://avd.aquasec.com/nvd/cve-2019-9192

```
──────────────────────────────────┤
│ libcurl4           │ CVE-2024-11053      │ MEDIUM   │              │
7.88.1-10+deb12u8       │               │ curl: curl netrc password leak
│
│                    │                     │          │              │
│                │ https://avd.aquasec.com/nvd/cve-2024-11053
│
│                    ├─────────────────────┤          │              │
├────────────────┼──────────────────────────────────────────────────────────
────┤
│                    │ CVE-2024-9681       │          │              │
│                │ curl: HSTS subdomain overwrites parent cache entry
│
│                    │                     │          │              │
│                │ https://avd.aquasec.com/nvd/cve-2024-9681
│
│                    ├─────────────────────┼──────────┤              │
├────────────────┼──────────────────────────────────────────────────────────
────┤
│                    │ CVE-2024-2379       │ LOW      │              │
│                │ curl: QUIC certificate check bypass with wolfSSL
│
│                    │                     │          │              │
│                │ https://avd.aquasec.com/nvd/cve-2024-2379
│
│                    ├─────────────────────┤          │              │
├────────────────┼──────────────────────────────────────────────────────────
────┤
│                    │ CVE-2025-0167       │          │              │
│                │ When asked to use a `.netrc` file for credentials
```

```
**and** to │
│                    │                      │          │              │
│               │ follow...
│
│                    │                      │          │              │
│               │ https://avd.aquasec.com/nvd/cve-2025-0167
│
│                    ├──────────────────────┤          │              │
├──────────────┼──────────────────────────────────────────────────────────
────┤
│                    │ CVE-2025-0725        │          │              │
│               │ libcurl: Buffer Overflow in libcurl via zlib Integer
│
│                    │                      │          │              │
│               │ Overflow
│
│                    │                      │          │              │
│               │ https://avd.aquasec.com/nvd/cve-2025-0725
│
├──────────────────┼──────────────────────┼──────────┤
├──────────────────────────┼──────────────┼──────────────────────────────
──────────────────┤
│ libexpat1          │ CVE-2023-52425       │ HIGH     │              │
2.5.0-1+deb12u1         │               │ expat: parsing large tokens can
trigger a denial of service  │
│                    │                      │          │              │
│               │ https://avd.aquasec.com/nvd/cve-2023-52425
│
│                    ├──────────────────────┼──────────┤              │
├──────────────┼──────────────────────────────────────────────────────────
```


CVE-2024-50602
MEDIUM
libexpat: expat: DoS via XML_ResumeParser
https://avd.aquasec.com/nvd/cve-2024-50602
CVE-2023-52426
LOW
expat: recursive XML entity expansion vulnerability
https://avd.aquasec.com/nvd/cve-2023-52426
CVE-2024-28757
expat: XML Entity Expansion
https://avd.aquasec.com/nvd/cve-2024-28757
libgcc-s1
CVE-2022-27943
12.2.0-14
binutils: libiberty/rust-

```
demangle.c in GNU GCC 11.2 allows   |
|                    |                       |          |              |
|               | stack exhaustion in demangle_const
|
|                    |                       |          |              |
|               | https://avd.aquasec.com/nvd/cve-2022-27943
|
|                    ├───────────────────────┤          |              |
├──────────────┼──────────────────────────────────────────────────────────
──────┤
|                    | CVE-2023-4039         |          |              |
|               | gcc: -fstack-protector fails to guard dynamic stack
|
|                    |                       |          |              |
|               | allocations on ARM64
|
|                    |                       |          |              |
|               | https://avd.aquasec.com/nvd/cve-2023-4039
|
├──────────────┼──────────────────────┼──────────┼──────────────┼──
──────────────────┼──────────────┼──────────────────────────────────────
──────────────────────┤
| libgcrypt20        | CVE-2024-2236        | MEDIUM   | fix_deferred |
1.10.1-3               |               | libgcrypt: vulnerable to Marvin
Attack                      |
|                    |                       |          |              |
|               | https://avd.aquasec.com/nvd/cve-2024-2236
|
|                    ├───────────────────────┼──────────┼──────────────┤
├──────────────┼──────────────────────────────────────────────────────────
──────┤
```

```
─────┤
│                    | CVE-2018-6829       | LOW      | affected     |
│                | libgcrypt: ElGamal implementation doesn't have semantic
│
│                    |                     |          |              |
│                | security due to incorrectly encoded plaintexts...
│
│                    |                     |          |              |
│                | https://avd.aquasec.com/nvd/cve-2018-6829
│
├──────────────────┼─────────────────────┼──────────┤
├──────────────────────────┼────────────────┼──────────────────────────────
──────────────────────────────┤
| libgnutls30        | CVE-2024-12243      | MEDIUM   |              |
3.7.9-2+deb12u3         |                | gnutls: GnuTLS Impacted by
Inefficient DER Decoding in       |
│                    |                     |          |              |
│                | libtasn1 Leading to Remote...
│
│                    |                     |          |              |
│                | https://avd.aquasec.com/nvd/cve-2024-12243
│
│                    ├─────────────────────┼──────────┤              |
├──────────────┼──────────────────────────────────────────────────────────
─────┤
│                    | CVE-2011-3389       | LOW      |              |
│                | HTTPS: block-wise chosen-plaintext attack against
SSL/TLS    |
│                    |                     |          |              |
│                | (BEAST)
```

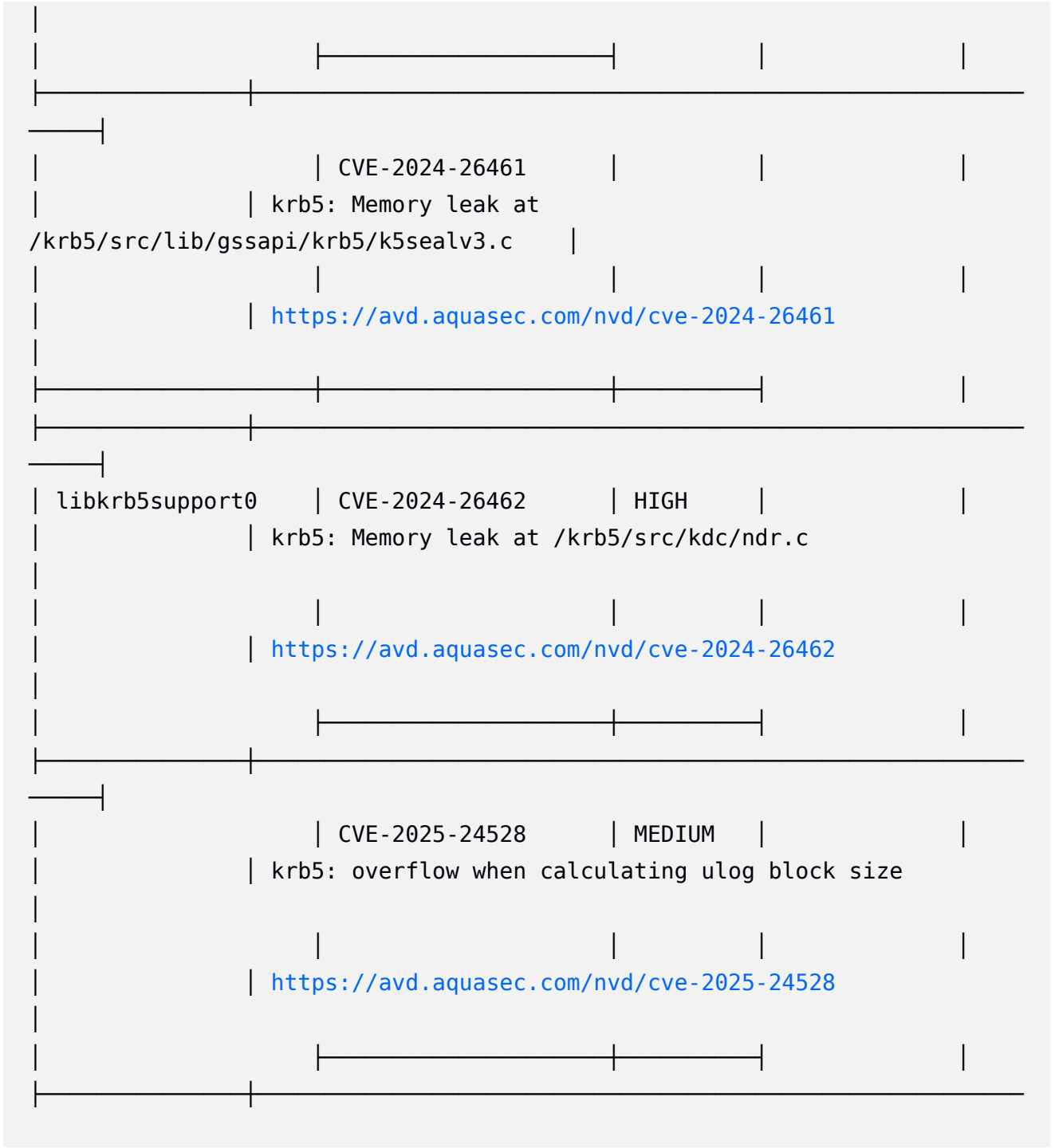

https://avd.aquasec.com/nvd/cve-2011-3389
libgssapi-krb5-2 CVE-2024-26462 HIGH
1.20.1-2+deb12u2 krb5: Memory leak at
/krb5/src/kdc/ndr.c
https://avd.aquasec.com/nvd/cve-2024-26462
CVE-2025-24528 MEDIUM
krb5: overflow when calculating ulog block size
https://avd.aquasec.com/nvd/cve-2025-24528
CVE-2018-5709 LOW
krb5: integer overflow in dbentry->n_key_data in
kadmin/dbutil/dump.c

```
│
│                    │                     │          │              │
│              │ https://avd.aquasec.com/nvd/cve-2018-5709
│
│                    ├─────────────────────┤          │              │
├──────────────┼──────────────────────────────────────────────────────
─────┤
│                    │ CVE-2024-26458      │          │              │
│              │ krb5: Memory leak at /krb5/src/lib/rpc/pmap_rmt.c
│
│                    │                     │          │              │
│              │ https://avd.aquasec.com/nvd/cve-2024-26458
│
│                    ├─────────────────────┤          │              │
├──────────────┼──────────────────────────────────────────────────────
─────┤
│                    │ CVE-2024-26461      │          │              │
│              │ krb5: Memory leak at
/krb5/src/lib/gssapi/krb5/k5sealv3.c    │
│                    │                     │          │              │
│              │ https://avd.aquasec.com/nvd/cve-2024-26461
│
├────────────────────┼─────────────────────┤          │
├─────────────────────────┼───────────────┼───────────────────────────
──────────────────────────────┤
│ libjansson4        │ CVE-2020-36325      │          │              │
2.14-2                  │               │ jansson: out-of-bounds read in
json_loads() due to a parsing │
│                    │                     │          │              │
│              │ error
```

```
│
│                     │                      │          │               │
│                │ https://avd.aquasec.com/nvd/cve-2020-36325
│
├─────────────────────┼──────────────────────┼──────────┤
├──────────────────────────┼───────────────┼──────────────────────────────
────────────────────────────────┤
│ libk5crypto3        │ CVE-2024-26462       │ HIGH     │               │
1.20.1-2+deb12u2        │               │ krb5: Memory leak at
/krb5/src/kdc/ndr.c                         │
│                     │                      │          │               │
│                │ https://avd.aquasec.com/nvd/cve-2024-26462
│
│                     ├──────────────────────┼──────────┤               │
├────────────────┼──────────────────────────────────────────────────────
─────┤
│                     │ CVE-2025-24528       │ MEDIUM   │               │
│                │ krb5: overflow when calculating ulog block size
│
│                     │                      │          │               │
│                │ https://avd.aquasec.com/nvd/cve-2025-24528
│
│                     ├──────────────────────┼──────────┤               │
├────────────────┼──────────────────────────────────────────────────────
─────┤
│                     │ CVE-2018-5709        │ LOW      │               │
│                │ krb5: integer overflow in dbentry->n_key_data in
│
│                     │                      │          │               │
│                │ kadmin/dbutil/dump.c
```

```
|
|                    |                     |          |              |
|               | https://avd.aquasec.com/nvd/cve-2018-5709
|
|                    |---------------------|          |              |
|---------------|-----------------------------------------------------------------
----|
|                    | CVE-2024-26458      |          |              |
|               | krb5: Memory leak at /krb5/src/lib/rpc/pmap_rmt.c
|
|                    |                     |          |              |
|               | https://avd.aquasec.com/nvd/cve-2024-26458
|
|                    |---------------------|          |              |
|---------------|-----------------------------------------------------------------
----|
|                    | CVE-2024-26461      |          |              |
|               | krb5: Memory leak at
/krb5/src/lib/gssapi/krb5/k5sealv3.c    |
|                    |                     |          |              |
|               | https://avd.aquasec.com/nvd/cve-2024-26461
|
|-------------------|---------------------|----------|              |
|---------------|-----------------------------------------------------------------
----|
| libkrb5-3          | CVE-2024-26462      | HIGH     |              |
|               | krb5: Memory leak at /krb5/src/kdc/ndr.c
|
|                    |                     |          |              |
|               | https://avd.aquasec.com/nvd/cve-2024-26462
```


| CVE-2025-24528 | MEDIUM |
| krb5: overflow when calculating ulog block size
| https://avd.aquasec.com/nvd/cve-2025-24528
| CVE-2018-5709 | LOW |
| krb5: integer overflow in dbentry->n_key_data in
| kadmin/dbutil/dump.c
| https://avd.aquasec.com/nvd/cve-2018-5709
| CVE-2024-26458 | | |
| krb5: Memory leak at /krb5/src/lib/rpc/pmap_rmt.c
| https://avd.aquasec.com/nvd/cve-2024-26458


	CVE-2024-26461			
krb5: Memory leak at /krb5/src/lib/gssapi/krb5/k5sealv3.c				
https://avd.aquasec.com/nvd/cve-2024-26461				
libkrb5support0	CVE-2024-26462	HIGH		
krb5: Memory leak at /krb5/src/kdc/ndr.c				
https://avd.aquasec.com/nvd/cve-2024-26462				
	CVE-2025-24528	MEDIUM		
krb5: overflow when calculating ulog block size				
https://avd.aquasec.com/nvd/cve-2025-24528				

```
──────┤
│                    │ CVE-2018-5709       │ LOW      │              │
│                │ krb5: integer overflow in dbentry->n_key_data in
│
│                    │                     │          │              │
│                │ kadmin/dbutil/dump.c
│
│                    │                     │          │              │
│                │ https://avd.aquasec.com/nvd/cve-2018-5709
│
│                    ├─────────────────────┤          │              │
├────────────────┼──────────────────────────────────────────────────────────────
──────┤
│                    │ CVE-2024-26458      │          │              │
│                │ krb5: Memory leak at /krb5/src/lib/rpc/pmap_rmt.c
│
│                    │                     │          │              │
│                │ https://avd.aquasec.com/nvd/cve-2024-26458
│
│                    ├─────────────────────┤          │              │
├────────────────┼──────────────────────────────────────────────────────────────
──────┤
│                    │ CVE-2024-26461      │          │              │
│                │ krb5: Memory leak at
/krb5/src/lib/gssapi/krb5/k5sealv3.c    │
│                    │                     │          │              │
│                │ https://avd.aquasec.com/nvd/cve-2024-26461
│
├────────────────────┼─────────────────────┼──────────┤
├────────────────────────┼─────────────────┼──────────────────────────────────
```

```
──────────────────────────────────┤
│ libldap-2.5-0      │ CVE-2023-2953       │ HIGH     │              │
2.5.13+dfsg-5           │               │ openldap: null pointer
dereference in ber_memalloc_x         │
│                    │                     │          │              │
│               │ function
│
│                    │                     │          │              │
│               │ https://avd.aquasec.com/nvd/cve-2023-2953
│
│                    ├─────────────────────┼──────────┤              │
├──────────────┼──────────────────────────────────────────────────────────────
──────┤
│                    │ CVE-2015-3276       │ LOW      │              │
│               │ openldap: incorrect multi-keyword mode cipherstring
parsing  │
│                    │                     │          │              │
│               │ https://avd.aquasec.com/nvd/cve-2015-3276
│
│                    ├─────────────────────┤          │              │
├──────────────┼──────────────────────────────────────────────────────────────
──────┤
│                    │ CVE-2017-14159      │          │              │
│               │ openldap: Privilege escalation via PID file manipulation
│
│                    │                     │          │              │
│               │ https://avd.aquasec.com/nvd/cve-2017-14159
│
│                    ├─────────────────────┤          │              │
├──────────────┼──────────────────────────────────────────────────────────────
──────┤
```

```
─────┤
│                  | CVE-2017-17740      |          |              |
│               | openldap: contrib/slapd-modules/nops/nops.c attempts to
free |
│                  |                     |          |              |
│               | stack buffer allowing remote attackers to cause...
│
│                  |                     |          |              |
│               | https://avd.aquasec.com/nvd/cve-2017-17740
│
│                  ├─────────────────────┤          |              |
├──────────────┼──────────────────────────────────────────────────────────
─────┤
│                  | CVE-2020-15719      |          |              |
│               | openldap: Certificate validation incorrectly matches
name    |
│                  |                     |          |              |
│               | against CN-ID
│
│                  |                     |          |              |
│               | https://avd.aquasec.com/nvd/cve-2020-15719
│
├──────────────────┼─────────────────────┼──────────┤              |
├──────────────┼──────────────────────────────────────────────────────────
─────┤
| libldap-common     | CVE-2023-2953       | HIGH     |              |
│               | openldap: null pointer dereference in ber_memalloc_x
│
│                  |                     |          |              |
│               | function
```

```
|
|                  |                     |          |              |
|               | https://avd.aquasec.com/nvd/cve-2023-2953
|
|                  |---------------------|----------|              |
|---------------|-------------------------------------------------------------
-----|
|                  | CVE-2015-3276       | LOW      |              |
|               | openldap: incorrect multi-keyword mode cipherstring
parsing  |
|                  |                     |          |              |
|               | https://avd.aquasec.com/nvd/cve-2015-3276
|
|                  |---------------------|          |              |
|---------------|-------------------------------------------------------------
-----|
|                  | CVE-2017-14159      |          |              |
|               | openldap: Privilege escalation via PID file manipulation
|
|                  |                     |          |              |
|               | https://avd.aquasec.com/nvd/cve-2017-14159
|
|                  |---------------------|          |              |
|---------------|-------------------------------------------------------------
-----|
|                  | CVE-2017-17740      |          |              |
|               | openldap: contrib/slapd-modules/nops/nops.c attempts to
free |
|                  |                     |          |              |
|               | stack buffer allowing remote attackers to cause...
```

```
|
|                    |                       |          |              |
|               | https://avd.aquasec.com/nvd/cve-2017-17740
|
|                    |-----------------------|          |              |
|-------------|-------------------------------------------------------------
-----|
|                    | CVE-2020-15719        |          |              |
|               | openldap: Certificate validation incorrectly matches
name    |
|                    |                       |          |              |
|               | against CN-ID
|
|                    |                       |          |              |
|               | https://avd.aquasec.com/nvd/cve-2020-15719
|
|-------------------|-----------------------|          |
|-------------------------|---------------|-------------------------------
---------------------------------|
| libmount1         | CVE-2022-0563         |          |              |
2.38.1-5+deb12u3        |               | util-linux: partial disclosure
of arbitrary files in chfn    |
|                    |                       |          |              |
|               | and chsh when compiled...
|
|                    |                       |          |              |
|               | https://avd.aquasec.com/nvd/cve-2022-0563
|
|-------------------|-----------------------|----------|
|-------------------------|---------------|-------------------------------
```

```
──────────────────────────────────┤
│ libpam-modules     │ CVE-2024-10041      │ MEDIUM   │              │
1.5.2-6+deb12u1         │               │ pam: libpam: Libpam vulnerable
to read hashed password       │
│                    │                     │          │              │
│               │ https://avd.aquasec.com/nvd/cve-2024-10041
│
│                    ├─────────────────────┤          │              │
├────────────────┼──────────────────────────────────────────────────────────
────┤
│                    │ CVE-2024-22365      │          │              │
│               │ pam: allowing unprivileged user to block another user
│
│                    │                     │          │              │
│               │ namespace
│
│                    │                     │          │              │
│               │ https://avd.aquasec.com/nvd/cve-2024-22365
│
├──────────────────┼─────────────────────┤          │              │
├────────────────┼──────────────────────────────────────────────────────────
────┤
│ libpam-modules-bin │ CVE-2024-10041      │          │              │
│               │ pam: libpam: Libpam vulnerable to read hashed password
│
│                    │                     │          │              │
│               │ https://avd.aquasec.com/nvd/cve-2024-10041
│
│                    ├─────────────────────┤          │              │
├────────────────┼──────────────────────────────────────────────────────────
──────
```

```
┼─────┤
│                    │ CVE-2024-22365      │          │              │
│                │ pam: allowing unprivileged user to block another user
│
│                    │                     │          │              │
│                │ namespace
│
│                    │                     │          │              │
│                │ https://avd.aquasec.com/nvd/cve-2024-22365
│
├────────────────────┼─────────────────────┤          │              │
├──────────────┼──────────────────────────────────────────────────────────────
┼─────┤
│ libpam-runtime     │ CVE-2024-10041      │          │              │
│                │ pam: libpam: Libpam vulnerable to read hashed password
│
│                    │                     │          │              │
│                │ https://avd.aquasec.com/nvd/cve-2024-10041
│
│                    ├─────────────────────┤          │              │
├──────────────┼──────────────────────────────────────────────────────────────
┼─────┤
│                    │ CVE-2024-22365      │          │              │
│                │ pam: allowing unprivileged user to block another user
│
│                    │                     │          │              │
│                │ namespace
│
│                    │                     │          │              │
│                │ https://avd.aquasec.com/nvd/cve-2024-22365
```

```
|
├──────────────────┼──────────────────────┼──────────┼──────────────┤
├──────────────┼──────────────────────────────────────────────────────
──────┤
| libpam0g           | CVE-2024-10041      |          |              |
|              | pam: libpam: Libpam vulnerable to read hashed password
|
|                  |                      |          |              |
|              | https://avd.aquasec.com/nvd/cve-2024-10041
|
|                  ├──────────────────────┼──────────┼──────────────┤
├──────────────┼──────────────────────────────────────────────────────
──────┤
|                  | CVE-2024-22365      |          |              |
|              | pam: allowing unprivileged user to block another user
|
|                  |                      |          |              |
|              | namespace
|
|                  |                      |          |              |
|              | https://avd.aquasec.com/nvd/cve-2024-22365
|
├──────────────────┼──────────────────────┼──────────┤
├──────────────────────┼──────────────┼──────────────────────────────
──────────────────────┤
| libpcre3           | CVE-2017-11164      | LOW      |              |
2:8.39-15              |              | pcre: OP_KETRMAX feature in the
match function in           |
|                  |                      |          |              |
|              | pcre_exec.c
```

```
|
|                    |                      |          |              |
|               | https://avd.aquasec.com/nvd/cve-2017-11164
|
|                    |----------------------|          |              |
|---------------|-------------------------------------------------------------
-----|
|                    | CVE-2017-16231       |          |              |
|               | pcre: self-recursive call in match() in pcre_exec.c
leads to |
|                    |                      |          |              |
|               | denial of service...
|
|                    |                      |          |              |
|               | https://avd.aquasec.com/nvd/cve-2017-16231
|
|                    |----------------------|          |              |
|---------------|-------------------------------------------------------------
-----|
|                    | CVE-2017-7245        |          |              |
|               | pcre: stack-based buffer overflow write in
|
|                    |                      |          |              |
|               | pcre32_copy_substring
|
|                    |                      |          |              |
|               | https://avd.aquasec.com/nvd/cve-2017-7245
|
|                    |----------------------|          |              |
|---------------|-------------------------------------------------------------
```

```
────┤
│                   | CVE-2017-7246       |          |              |
│               | pcre: stack-based buffer overflow write in
│
│                   |                     |          |              |
│               | pcre32_copy_substring
│
│                   |                     |          |              |
│               | https://avd.aquasec.com/nvd/cve-2017-7246
│
│                   ├─────────────────────┤          |              |
├─────────────┼──────────────────────────────────────────────────────
────┤
│                   | CVE-2019-20838      |          |              |
│               | pcre: Buffer over-read in JIT when UTF is disabled and
\X    |
│                   |                     |          |              |
│               | or...
│
│                   |                     |          |              |
│               | https://avd.aquasec.com/nvd/cve-2019-20838
│
├─────────────────┼─────────────────────┤          |
├──────────────────────┼──────────────┼──────────────────────────────
──────────────────┤
| libsmartcols1     | CVE-2022-0563       |          |              |
2.38.1-5+deb12u3       |               | util-linux: partial disclosure
of arbitrary files in chfn    |
│                   |                     |          |              |
│               | and chsh when compiled...
```

```
|
|                  |                      |          |              |
|               | https://avd.aquasec.com/nvd/cve-2022-0563
|
├──────────────────┼──────────────────────┼──────────┤
├──────────────────────────┼──────────────┼──────────────────────────────
──────────────────────────┤
| libssl3            | CVE-2024-13176      | MEDIUM   |              |
3.0.15-1~deb12u1        |              | openssl: Timing side-channel in
ECDSA signature computation  |
|                  |                      |          |              |
|               | https://avd.aquasec.com/nvd/cve-2024-13176
|
├──────────────────┼──────────────────────┼──────────┤
├──────────────────────────┼──────────────┼──────────────────────────────
──────────────────────────┤
| libstdc++6         | CVE-2022-27943      | LOW      |              |
12.2.0-14               |              | binutils: libiberty/rust-
demangle.c in GNU GCC 11.2 allows   |
|                  |                      |          |              |
|               | stack exhaustion in demangle_const
|
|                  |                      |          |              |
|               | https://avd.aquasec.com/nvd/cve-2022-27943
|
|                  ├──────────────────────┤          |              |
├──────────────┼──────────────────────────────────────────────────────
────┤
|                  | CVE-2023-4039       |          |              |
|               | gcc: -fstack-protector fails to guard dynamic stack
```

```
|
|                    |                      |          |              |
|               | allocations on ARM64
|
|                    |                      |          |              |
|               | https://avd.aquasec.com/nvd/cve-2023-4039
|
├──────────────────┼──────────────────────┤          |
├──────────────────────┼──────────────┼──────────────────────────────────
──────────────────────────────────┤
| libsystemd0        | CVE-2013-4392       |          |              |
252.33-1~deb12u1        |               | systemd: TOCTOU race condition
when updating file            |
|                    |                      |          |              |
|               | permissions and SELinux security contexts...
|
|                    |                      |          |              |
|               | https://avd.aquasec.com/nvd/cve-2013-4392
|
|                    ├──────────────────────┤          |              |
├──────────────┼──────────────────────────────────────────────────────────
────┤
|                    | CVE-2023-31437       |          |              |
|               | An issue was discovered in systemd 253. An attacker can
|
|                    |                      |          |              |
|               | modify a...
|
|                    |                      |          |              |
|               | https://avd.aquasec.com/nvd/cve-2023-31437
```

```
│
│                    ├───────────────────────────┤             │                  │
├───────────────────┼────────────────────────────────────────────────────────────
───────┤
│                    │ CVE-2023-31438            │             │                  │
│                  │ An issue was discovered in systemd 253. An attacker can
│
│                    │                           │             │                  │
│                  │ truncate a...
│
│                    │                           │             │                  │
│                  │ https://avd.aquasec.com/nvd/cve-2023-31438
│
│                    ├───────────────────────────┤             │                  │
├───────────────────┼────────────────────────────────────────────────────────────
───────┤
│                    │ CVE-2023-31439            │             │                  │
│                  │ An issue was discovered in systemd 253. An attacker can
│
│                    │                           │             │                  │
│                  │ modify the...
│
│                    │                           │             │                  │
│                  │ https://avd.aquasec.com/nvd/cve-2023-31439
│
├────────────────────┼───────────────────────────┼─────────────┤
├──────────────────────────────┼───────────────────┼──────────────────────────────
───────────────────────────────────────┤
│ libtasn1-6         │ CVE-2024-12133            │ MEDIUM      │                  │
4.19.0-2                     │                   │ libtasn1: Inefficient DER
```

```
Decoding in libtasn1 Leading to    │
│                    │                       │          │              │
│               │ Potential Remote DoS
│
│                    │                       │          │              │
│               │ https://avd.aquasec.com/nvd/cve-2024-12133
│
├────────────────────┼───────────────────────┤          │
├──────────────────────────┼──────────────┼──────────────────────────────
──────────────────────────────┤
│ libtinfo6          │ CVE-2023-50495      │          │              │
6.4-4                    │              │ ncurses: segmentation fault via
_nc_wrap_entry()             │
│                    │                       │          │              │
│               │ https://avd.aquasec.com/nvd/cve-2023-50495
│
├────────────────────┼───────────────────────┼──────────┤
├──────────────────────────┼──────────────┼──────────────────────────────
──────────────────────────────┤
│ libudev1           │ CVE-2013-4392       │ LOW      │              │
252.33-1~deb12u1         │              │ systemd: TOCTOU race condition
when updating file           │
│                    │                       │          │              │
│               │ permissions and SELinux security contexts...
│
│                    │                       │          │              │
│               │ https://avd.aquasec.com/nvd/cve-2013-4392
│
│                    ├───────────────────────┤          │              │
├────────────────┼──────────────────────────────────────────────────────
──────────────────────────────┘
```

```
────┤
│                  │ CVE-2023-31437      │          │              │
│               │ An issue was discovered in systemd 253. An attacker can
│
│                  │                     │          │              │
│               │ modify a...
│
│                  │                     │          │              │
│               │ https://avd.aquasec.com/nvd/cve-2023-31437
│
│                  ├─────────────────────┤          │              │
├──────────────┼──────────────────────────────────────────────────────────
────┤
│                  │ CVE-2023-31438      │          │              │
│               │ An issue was discovered in systemd 253. An attacker can
│
│                  │                     │          │              │
│               │ truncate a...
│
│                  │                     │          │              │
│               │ https://avd.aquasec.com/nvd/cve-2023-31438
│
│                  ├─────────────────────┤          │              │
├──────────────┼──────────────────────────────────────────────────────────
────┤
│                  │ CVE-2023-31439      │          │              │
│               │ An issue was discovered in systemd 253. An attacker can
│
│                  │                     │          │              │
│               │ modify the...
```

```
│
│                    │                     │          │              │
│               │ https://avd.aquasec.com/nvd/cve-2023-31439
│
├────────────────────┼─────────────────────┤          │
├─────────────────────────┼───────────────┼──────────────────────────────
──────────────────────────────┤
│ libuuid1           │ CVE-2022-0563       │          │              │
2.38.1-5+deb12u3        │               │ util-linux: partial disclosure
of arbitrary files in chfn    │
│                    │                     │          │              │
│               │ and chsh when compiled...
│
│                    │                     │          │              │
│               │ https://avd.aquasec.com/nvd/cve-2022-0563
│
├────────────────────┼─────────────────────┼──────────┤
├─────────────────────────┼───────────────┼──────────────────────────────
──────────────────────────────┤
│ libxml2            │ CVE-2022-49043      │ HIGH     │              │
2.9.14+dfsg-1.3~deb12u1 │               │ libxml: use-after-free in
xmlXIncludeAddNode               │
│                    │                     │          │              │
│               │ https://avd.aquasec.com/nvd/cve-2022-49043
│
│                    ├─────────────────────┤          │              │
├───────────────┼──────────────────────────────────────────────────────
─────┤
│                    │ CVE-2024-25062      │          │              │
│               │ libxml2: use-after-free in XMLReader
```


https://avd.aquasec.com/nvd/cve-2024-25062
CVE-2023-39615 MEDIUM
libxml2: crafted xml can cause global buffer overflow
https://avd.aquasec.com/nvd/cve-2023-39615
CVE-2023-45322
libxml2: use-after-free in xmlUnlinkNode() in tree.c
https://avd.aquasec.com/nvd/cve-2023-45322
CVE-2024-34459 LOW
libxml2: buffer over-read in xmlHTMLPrintFileContext in
xmllint.c

```
│
│                    │                     │          │              │
│               │ https://avd.aquasec.com/nvd/cve-2024-34459
│
├────────────────────┼─────────────────────┼──────────┤
├─────────────────────────┼───────────────┼──────────────────────────────
──────────────────────────────┤
│ login              │ CVE-2023-4641       │ MEDIUM   │              │
1:4.13+dfsg1-1+b1       │               │ shadow-utils: possible password
leak during passwd(1) change │
│                    │                     │          │              │
│               │ https://avd.aquasec.com/nvd/cve-2023-4641
│
│                    ├─────────────────────┼──────────┤              │
├───────────────┼──────────────────────────────────────────────────────
─────┤
│                    │ CVE-2007-5686       │ LOW      │              │
│               │ initscripts in rPath Linux 1 sets insecure permissions
for   │
│                    │                     │          │              │
│               │ the /var/lo ......
│
│                    │                     │          │              │
│               │ https://avd.aquasec.com/nvd/cve-2007-5686
│
│                    ├─────────────────────┤          │              │
├───────────────┼──────────────────────────────────────────────────────
─────┤
│                    │ CVE-2023-29383      │          │              │
│               │ shadow: Improper input validation in shadow-utils
```

```
package    |
|                    |                       |          |              |
|               | utility chfn
|
|                    |                       |          |              |
|               | https://avd.aquasec.com/nvd/cve-2023-29383
|
|                    ├───────────────────────┤          |              |
├──────────────┼──────────────────────────────────────────────────────────
──────┤
|                    | CVE-2024-56433        |          |              |
|               | shadow-utils: Default subordinate ID configuration in
|
|                    |                       |          |              |
|               | /etc/login.defs could lead to compromise
|
|                    |                       |          |              |
|               | https://avd.aquasec.com/nvd/cve-2024-56433
|
|                    ├───────────────────────┤          |              |
├──────────────┼──────────────────────────────────────────────────────────
──────┤
|                    | TEMP-0628843-DBAD28   |          |              |
|               | [more related to CVE-2005-4890]
|
|                    |                       |          |              |
|               | https://security-tracker.debian.org/tracker/TEMP-
0628843-DB- |
|                    |                       |          |              |
|               | AD28
```

```
│
├──────────────────────┼──────────────────────────┼──────────┼
├──────────────────────┼──────────────┼──────────────────────────────
──────────────────────────────────┤
│ mount                │ CVE-2022-0563        │          │
2.38.1-5+deb12u3        │              │ util-linux: partial disclosure
of arbitrary files in chfn    │
│                      │                      │          │
│              │ and chsh when compiled...
│
│                      │                      │          │
│              │ https://avd.aquasec.com/nvd/cve-2022-0563
│
├──────────────────────┼──────────────────────────┼──────────┼
├──────────────────────┼──────────────┼──────────────────────────────
──────────────────────────────────┤
│ ncurses-base         │ CVE-2023-50495       │ MEDIUM   │
6.4-4                   │              │ ncurses: segmentation fault via
_nc_wrap_entry()             │
│                      │                      │          │
│              │ https://avd.aquasec.com/nvd/cve-2023-50495
│
├──────────────────────┤                      │          │
├──────────────┤
│
│ ncurses-bin          │                      │          │
│              │
│
│                      │                      │          │
│              │
```

```
|
├──────────────────┼──────────────────────┼──────────┼──────────────┼
──────────────────────────────────┤
| openssl          | CVE-2024-13176       |          |              |
3.0.15-1~deb12u1      |               | openssl: Timing side-channel in
ECDSA signature computation  |
|                  |                      |          |              |
|              | https://avd.aquasec.com/nvd/cve-2024-13176
|
├──────────────────┼──────────────────────┼──────────┼──────────────┼
──────────────────────────────────┤
| passwd           | CVE-2023-4641        |          |              |
1:4.13+dfsg1-1+b1      |               | shadow-utils: possible password
leak during passwd(1) change |
|                  |                      |          |              |
|              | https://avd.aquasec.com/nvd/cve-2023-4641
|
|                  ├──────────────────────┼──────────┤              |
├──────────────┼──────────────────────────────────────────────────────
────┤
|                  | CVE-2007-5686        | LOW      |              |
|              | initscripts in rPath Linux 1 sets insecure permissions
for   |
|                  |                      |          |              |
|              | the /var/lo ......
|
|                  |                      |          |              |
|              | https://avd.aquasec.com/nvd/cve-2007-5686
```

```
|
|                    ├──────────────────────┤          |              |
├──────────────┼──────────────────────────────────────────────────────────────
──┤
|                    | CVE-2023-29383       |          |              |
|                | shadow: Improper input validation in shadow-utils
package    |
|                    |                      |          |              |
|                | utility chfn
|
|                    |                      |          |              |
|                | https://avd.aquasec.com/nvd/cve-2023-29383
|
|                    ├──────────────────────┤          |              |
├──────────────┼──────────────────────────────────────────────────────────────
──┤
|                    | CVE-2024-56433       |          |              |
|                | shadow-utils: Default subordinate ID configuration in
|
|                    |                      |          |              |
|                | /etc/login.defs could lead to compromise
|
|                    |                      |          |              |
|                | https://avd.aquasec.com/nvd/cve-2024-56433
|
|                    ├──────────────────────┤          |              |
├──────────────┼──────────────────────────────────────────────────────────────
──┤
|                    | TEMP-0628843-DBAD28  |          |              |
|                | [more related to CVE-2005-4890]
```

```
│
│                    │                           │             │                  │
│                    │ https://security-tracker.debian.org/tracker/TEMP-
0628843-DB- │
│                    │                           │             │                  │
│                    │ AD28
│
├────────────────────┼───────────────────────────┼─────────────┤
├────────────────────────────────┼───────────────────┼──────────────────────────────
──────────────────────────────────────┤
│ perl-base          │ CVE-2023-31484            │ HIGH        │                  │
5.36.0-7+deb12u1        │                   │ perl: CPAN.pm does not verify
TLS certificates when         │
│                    │                           │             │                  │
│                    │ downloading distributions over HTTPS...
│
│                    │                           │             │                  │
│                    │ https://avd.aquasec.com/nvd/cve-2023-31484
│
│                    ├───────────────────────────┼─────────────┤                  │
├────────────────────┼──────────────────────────────────────────────────────────────
──────┤
│                    │ CVE-2011-4116             │ LOW         │                  │
│                    │ perl: File:: Temp insecure temporary file handling
│
│                    │                           │             │                  │
│                    │ https://avd.aquasec.com/nvd/cve-2011-4116
│
│                    ├───────────────────────────┤             │                  │
├────────────────────┼──────────────────────────────────────────────────────────────
```

```
──────┤
│                    | CVE-2023-31486      |          |              |
│                | http-tiny: insecure TLS cert default
│
│                    |                     |          |              |
│                | https://avd.aquasec.com/nvd/cve-2023-31486
│
├──────────────────┼─────────────────────┤          |
├──────────────────────────┼──────────────┼──────────────────────────────
──────────────────────────────┤
| sysvinit-utils     | TEMP-0517018-A83CE6 |          |              |
3.06-4                   |               | [sysvinit: no-root option in
expert installer exposes        |
│                    |                     |          |              |
│                | locally exploitable security flaw]
│
│                    |                     |          |              |
│                | https://security-tracker.debian.org/tracker/TEMP-
0517018-A8- |
│                    |                     |          |              |
│                | 3CE6
│
├──────────────────┼─────────────────────┤          |
├──────────────────────────┼──────────────┼──────────────────────────────
──────────────────────────────┤
| tar                | CVE-2005-2541       |          |              |
1.34+dfsg-1.2+deb12u1   |               | tar: does not properly warn the
user when extracting setuid  |
│                    |                     |          |              |
│                | or setgid...
```


https://avd.aquasec.com/nvd/cve-2005-2541
TEMP-0290435-0B57B5
[tar's rmt command may have undesired side effects]
https://security-tracker.debian.org/tracker/TEMP-0290435-0B-
57B5
util-linux
CVE-2022-0563
2.38.1-5+deb12u3
util-linux: partial disclosure of arbitrary files in chfn
and chsh when compiled...
https://avd.aquasec.com/nvd/cve-2022-0563

```
|
| util-linux-extra   |                     |          |              |
|               |
|
|                    |                     |          |              |
|               |
|
|                    |                     |          |              |
|               |
|
├──────────────────┼─────────────────────┼──────────┼──────────────┼──
──────────────────┼─────────────────┼──────────────────────────────────
──────────────────────────┤
| zlib1g             | CVE-2023-45853      | CRITICAL | will_not_fix |
1:1.2.13.dfsg-1         |               | zlib: integer overflow and
resultant heap-based buffer       |
|                    |                     |          |              |
|               | overflow in zipOpenNewFileInZip4_6
|
|                    |                     |          |              |
|               | https://avd.aquasec.com/nvd/cve-2023-45853
|
└──────────────────┴─────────────────────┴──────────┴──────────────┴──
──────────────────┴─────────────────┴──────────────────────────────────
──────────────────────────┘
[Pipeline] }
[Pipeline] // script
[Pipeline] }
[Pipeline] // stage
[Pipeline] stage
```

```
[Pipeline] { (Push Docker Image to DockerHub)
[Pipeline] withCredentials
Masking supported pattern matches of $DOCKER_HUB_TOKEN
[Pipeline] {
[Pipeline] script
[Pipeline] {
[Pipeline] sh
+ docker login -u srush634 --password-stdin
+ echo ****
WARNING! Your password will be stored unencrypted in
/var/lib/jenkins/.docker/config.json.
Configure a credential helper to remove this warning. See
https://docs.docker.com/engine/reference/commandline/login/#credential-
stores

Login Succeeded
+ docker push srush634/docker-webapp:latest
The push refers to repository [docker.io/srush634/docker-webapp]
cb07b3a6e720: Preparing
e48683950315: Preparing
1b533b3f600d: Preparing
45d2a6f2a0b1: Preparing
5f70bf18a086: Preparing
d465f9c6793b: Preparing
7914c8f600f5: Preparing
7914c8f600f5: Waiting
d465f9c6793b: Waiting
45d2a6f2a0b1: Layer already exists
1b533b3f600d: Layer already exists
e48683950315: Layer already exists
```

```
5f70bf18a086: Layer already exists
cb07b3a6e720: Layer already exists
d465f9c6793b: Layer already exists
7914c8f600f5: Layer already exists
latest: digest:
sha256:d59c56d079af0f9345d2efe4962f998f1a6f930e3aab3cbb2dc0fff8b0a7440b
size: 1780
[Pipeline] }
[Pipeline] // script
[Pipeline] }
[Pipeline] // withCredentials
[Pipeline] }
[Pipeline] // stage
[Pipeline] stage
[Pipeline] { (Deploy to Minikube)
[Pipeline] script
[Pipeline] {
[Pipeline] sh
+ export KUBECONFIG=/var/lib/jenkins/.kube/config
+ echo Deploying application to Minikube...
Deploying application to Minikube...
+ kubectl delete deployment webapp --ignore-not-found=true
+ kubectl apply -f deployment.yaml
deployment.apps/webapp-deployment created
+ kubectl apply -f service.yaml
service/webapp-service created
+ echo Waiting for pods to be ready...
Waiting for pods to be ready...
+ kubectl wait --for=condition=ready pod -l app=webapp --timeout=90s
pod/webapp-deployment-7d4468f78c-6fvrc condition met
```

```
pod/webapp-deployment-7d4468f78c-x9hcb condition met
[Pipeline] }
[Pipeline] // script
[Pipeline] }
[Pipeline] // stage
[Pipeline] stage
[Pipeline] { (Expose Minikube Service)
[Pipeline] script
[Pipeline] {
[Pipeline] sh
+ echo Checking if service exists...
Checking if service exists...
+ kubectl get svc webapp-service
NAME             TYPE       CLUSTER-IP       EXTERNAL-IP   PORT(S)
AGE
webapp-service   NodePort   10.110.133.234   <none>        80:30006/TCP
22s
+ echo Retrieving running pod name...
Retrieving running pod name...
+ kubectl get pods -l app=webapp -o jsonpath={.items[0].metadata.name}
+ POD_NAME=webapp-deployment-7d4468f78c-6fvrc
+ [[ -z webapp-deployment-7d4468f78c-6fvrc ]]
/var/lib/jenkins/workspace/test@tmp/durable-462a0c52/script.sh.copy: 8:
[[: not found
+ echo Exposing service...
Exposing service...
+ minikube service webapp-service --url
http://192.168.49.2:30006
[Pipeline] }
[Pipeline] // script
```

```
[Pipeline] }
[Pipeline] // stage
[Pipeline] stage
[Pipeline] { (Verify Deployment)
[Pipeline] script
[Pipeline] {
[Pipeline] sh
+ echo Checking pods...
Checking pods...
+ kubectl get pods
NAME                                  READY   STATUS    RESTARTS   AGE
webapp-deployment-7d4468f78c-6fvrc   1/1     Running   0          27s
webapp-deployment-7d4468f78c-x9hcb   1/1     Running   0          27s
+ echo Checking deployments...
Checking deployments...
+ kubectl get deployments
NAME                READY   UP-TO-DATE   AVAILABLE   AGE
webapp-deployment   2/2     2            2           27s
+ echo Checking services...
Checking services...
+ kubectl get services
NAME             TYPE        CLUSTER-IP       EXTERNAL-IP   PORT(S)
AGE
kubernetes       ClusterIP   10.96.0.1        <none>        443/TCP
74s
webapp-service   NodePort    10.110.133.234   <none>        80:30006/TCP
26s
[Pipeline] }
[Pipeline] // script
[Pipeline] }
```

```
[Pipeline] // stage
[Pipeline] stage
[Pipeline] { (Access Website)
[Pipeline] script
[Pipeline] {
[Pipeline] sh
+ echo Fetching Minikube service URL...
Fetching Minikube service URL...
+ minikube service webapp-service --url
+ URL=http://192.168.49.2:30006
+ echo Your website is available at: http://192.168.49.2:30006
Your website is available at: http://192.168.49.2:30006
[Pipeline] }
[Pipeline] // script
[Pipeline] }
[Pipeline] // stage
[Pipeline] }
[Pipeline] // withEnv
[Pipeline] }
[Pipeline] // node
[Pipeline] End of Pipeline
Finished: SUCCESS
```

REST API Jenkins 2.495