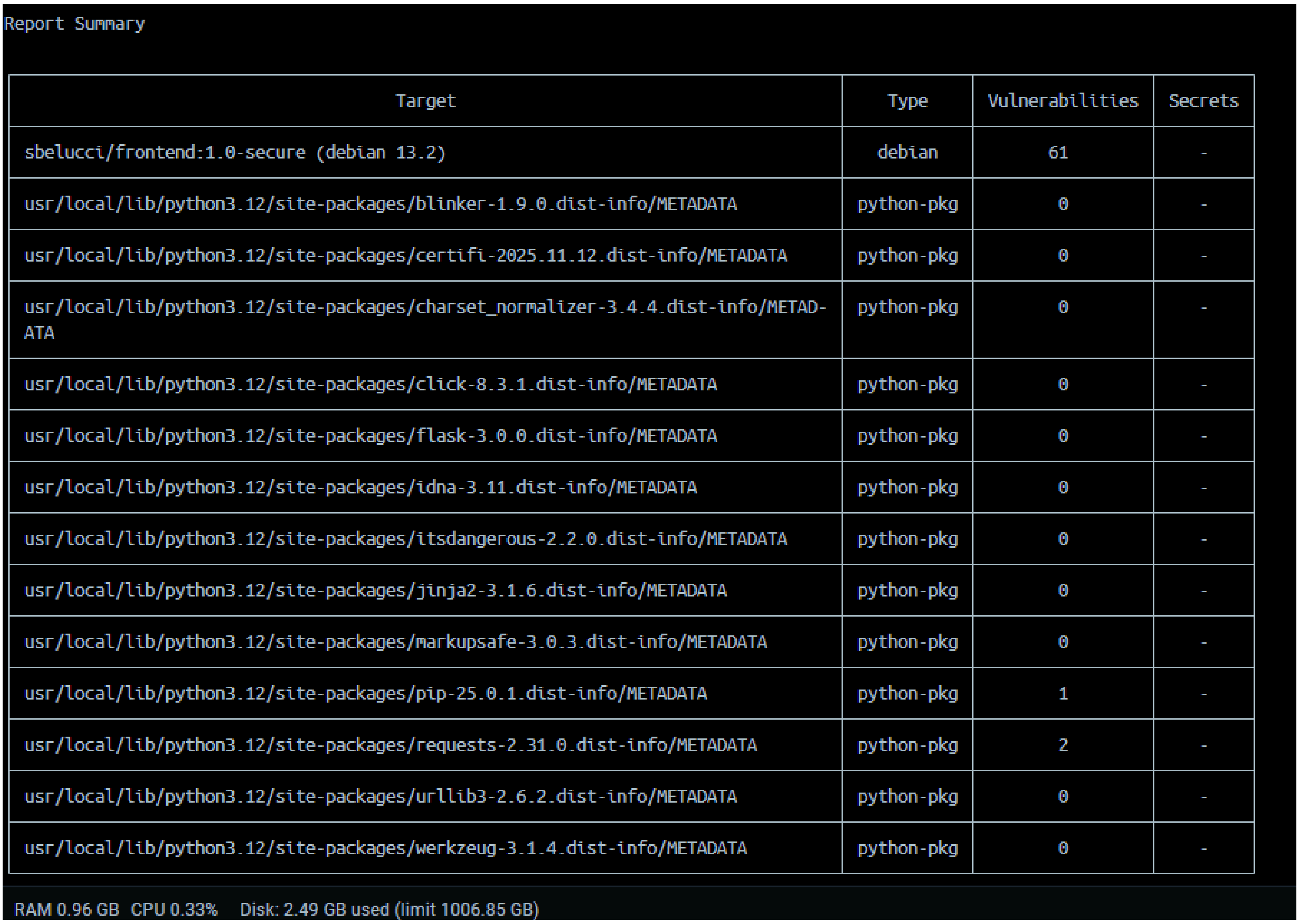
EJ. 2: ESCANEO DE VULNERABILIDADES

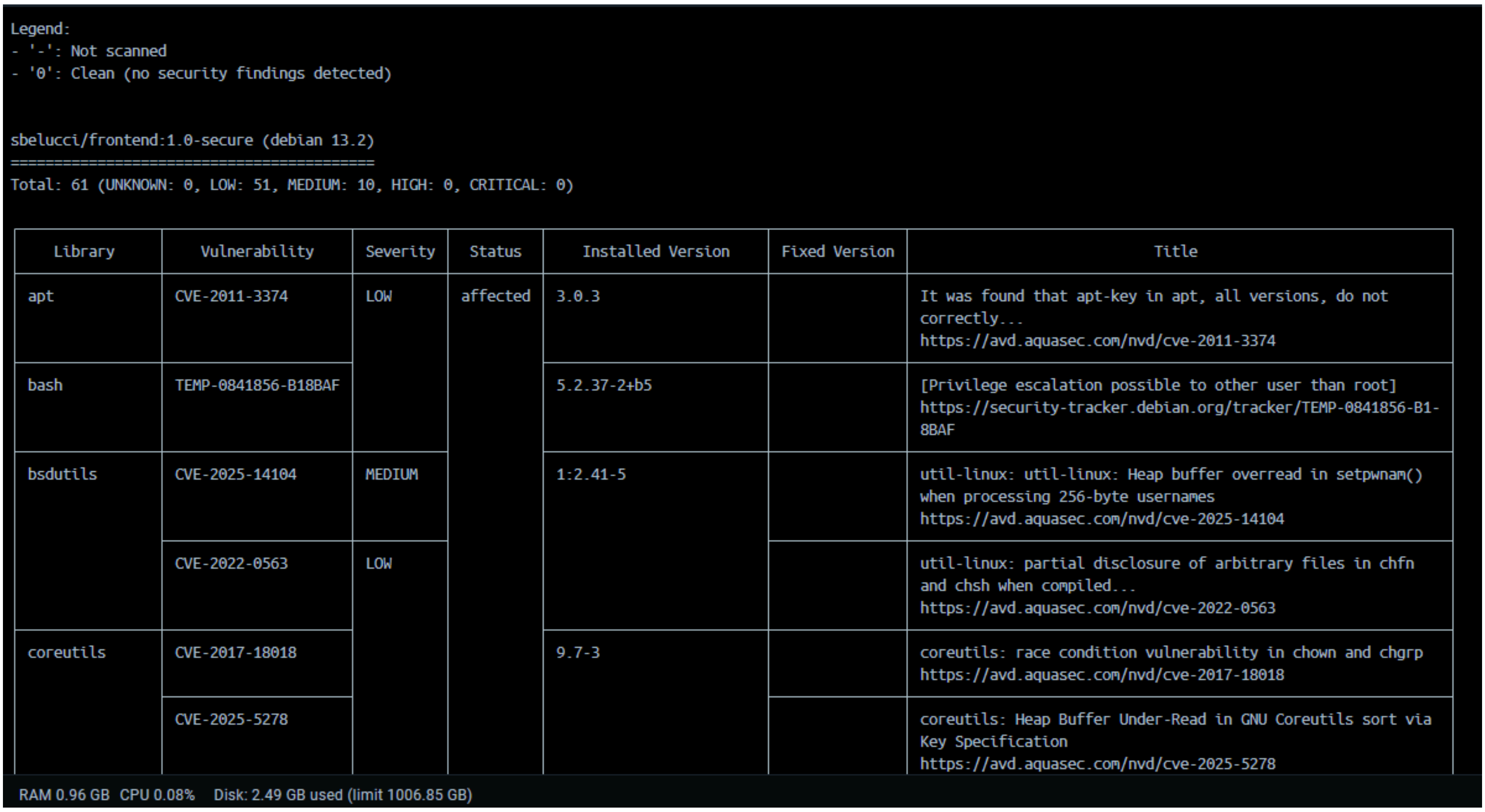
Para los reportes, se ha utilizado Trivy

1) Resultado del reporte de la image sbelucci/frontend:1.0-secure

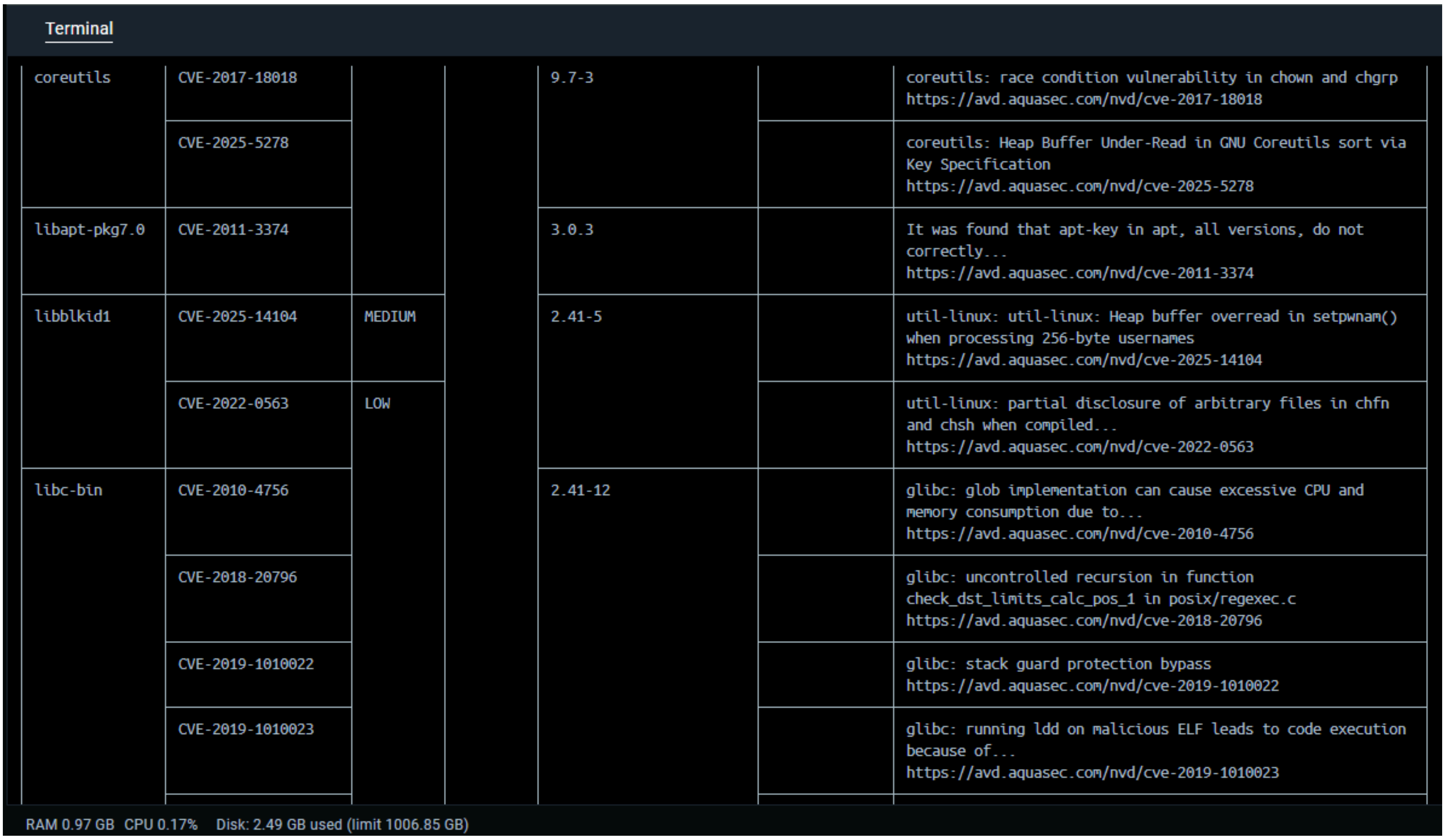
docker run --rm -v /var/run/docker.sock:/var/run/docker.sock aquasec/trivy:latest image sbelucci/frontend:1.0-secure



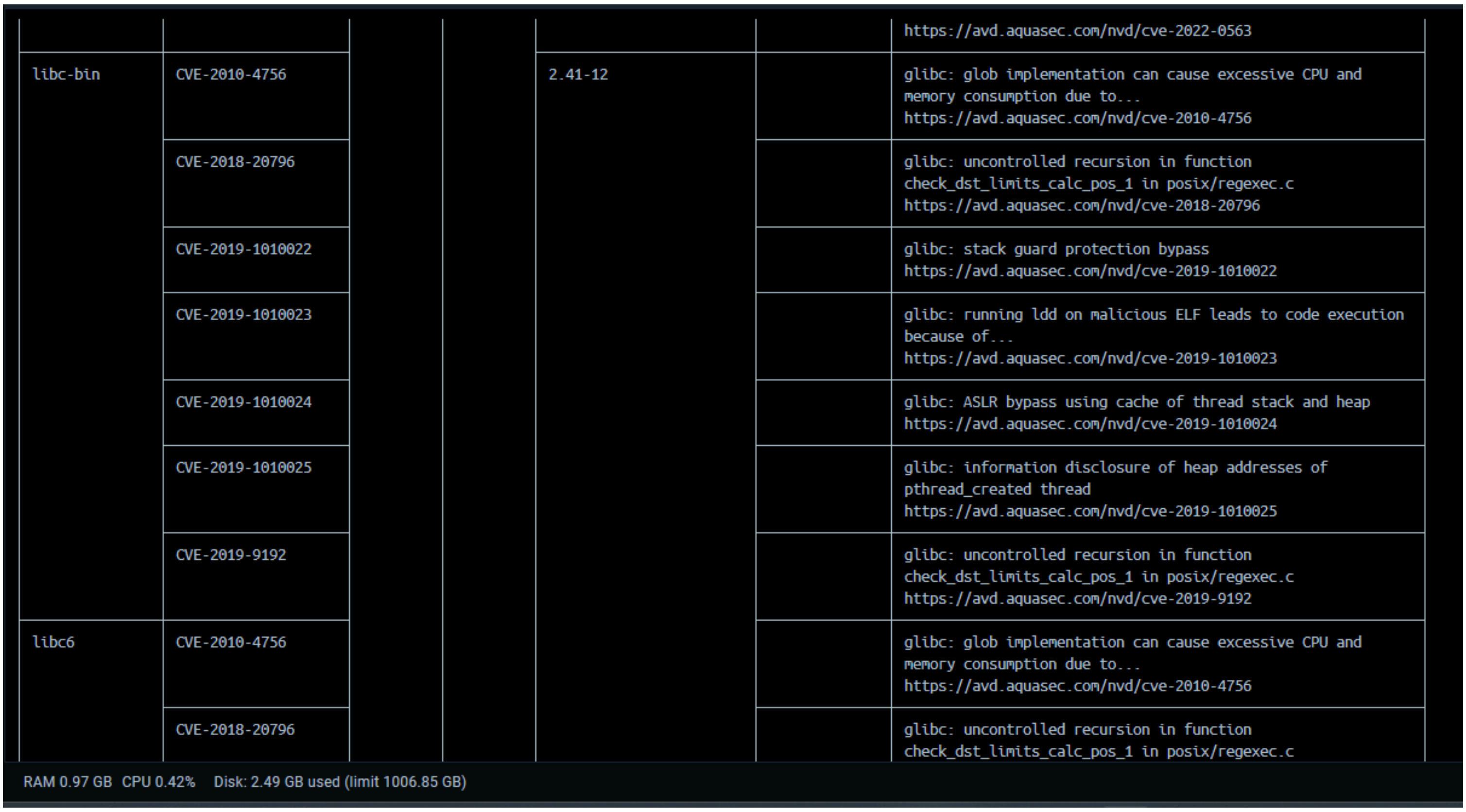
```
Report Summary

┌───────────────────────────────────────────────────────────────────────────────┬────────────┬─────────────────┬─────────┐
│                                    Target                                     │    Type    │ Vulnerabilities │ Secrets │
├───────────────────────────────────────────────────────────────────────────────┼────────────┼─────────────────┼─────────┤
│ sbelucci/frontend:1.0-secure (debian 13.2)                                    │   debian   │       61        │    -    │
├───────────────────────────────────────────────────────────────────────────────┼────────────┼─────────────────┼─────────┤
│ usr/local/lib/python3.12/site-packages/blinker-1.9.0.dist-info/METADATA       │ python-pkg │        0        │    -    │
├───────────────────────────────────────────────────────────────────────────────┼────────────┼─────────────────┼─────────┤
│ usr/local/lib/python3.12/site-packages/certifi-2025.11.12.dist-info/METADATA  │ python-pkg │        0        │    -    │
├───────────────────────────────────────────────────────────────────────────────┼────────────┼─────────────────┼─────────┤
│ usr/local/lib/python3.12/site-packages/charset_normalizer-3.4.4.dist-info/METAD- │ python-pkg │        0        │    -    │
│ ATA                                                                           │            │                 │         │
├───────────────────────────────────────────────────────────────────────────────┼────────────┼─────────────────┼─────────┤
│ usr/local/lib/python3.12/site-packages/click-8.3.1.dist-info/METADATA         │ python-pkg │        0        │    -    │
├───────────────────────────────────────────────────────────────────────────────┼────────────┼─────────────────┼─────────┤
│ usr/local/lib/python3.12/site-packages/flask-3.0.0.dist-info/METADATA         │ python-pkg │        0        │    -    │
├───────────────────────────────────────────────────────────────────────────────┼────────────┼─────────────────┼─────────┤
│ usr/local/lib/python3.12/site-packages/idna-3.11.dist-info/METADATA           │ python-pkg │        0        │    -    │
├───────────────────────────────────────────────────────────────────────────────┼────────────┼─────────────────┼─────────┤
│ usr/local/lib/python3.12/site-packages/itsdangerous-2.2.0.dist-info/METADATA  │ python-pkg │        0        │    -    │
├───────────────────────────────────────────────────────────────────────────────┼────────────┼─────────────────┼─────────┤
│ usr/local/lib/python3.12/site-packages/jinja2-3.1.6.dist-info/METADATA        │ python-pkg │        0        │    -    │
├───────────────────────────────────────────────────────────────────────────────┼────────────┼─────────────────┼─────────┤
│ usr/local/lib/python3.12/site-packages/markupsafe-3.0.3.dist-info/METADATA    │ python-pkg │        0        │    -    │
├───────────────────────────────────────────────────────────────────────────────┼────────────┼─────────────────┼─────────┤
│ usr/local/lib/python3.12/site-packages/pip-25.0.1.dist-info/METADATA          │ python-pkg │        1        │    -    │
├───────────────────────────────────────────────────────────────────────────────┼────────────┼─────────────────┼─────────┤
│ usr/local/lib/python3.12/site-packages/requests-2.31.0.dist-info/METADATA     │ python-pkg │        2        │    -    │
├───────────────────────────────────────────────────────────────────────────────┼────────────┼─────────────────┼─────────┤
│ usr/local/lib/python3.12/site-packages/urllib3-2.6.2.dist-info/METADATA       │ python-pkg │        0        │    -    │
├───────────────────────────────────────────────────────────────────────────────┼────────────┼─────────────────┼─────────┤
│ usr/local/lib/python3.12/site-packages/werkzeug-3.1.4.dist-info/METADATA      │ python-pkg │        0        │    -    │
└───────────────────────────────────────────────────────────────────────────────┴────────────┴─────────────────┴─────────┘
RAM 0.96 GB  CPU 0.33%    Disk: 2.49 GB used (limit 1006.85 GB)
```



```
Legend:
- '-': Not scanned
- '0': Clean (no security findings detected)


sbelucci/frontend:1.0-secure (debian 13.2)
==========================================
Total: 61 (UNKNOWN: 0, LOW: 51, MEDIUM: 10, HIGH: 0, CRITICAL: 0)

| Library   | Vulnerability       | Severity | Status   | Installed Version | Fixed Version | Title                                                        |
|-----------|---------------------|----------|----------|-------------------|---------------|--------------------------------------------------------------|
| apt       | CVE-2011-3374       | LOW      | affected | 3.0.3             |               | 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 |          |          | 5.2.37-2+b5       |               | [Privilege escalation possible to other user than root]      |
|           |                     |          |          |                   |               | https://security-tracker.debian.org/tracker/TEMP-0841856-B1- |
|           |                     |          |          |                   |               | 8BAF                                                         |
|-----------|---------------------|----------|          |-------------------|---------------|--------------------------------------------------------------|
| bsdutils  | CVE-2025-14104      | MEDIUM   |          | 1:2.41-5          |               | util-linux: util-linux: Heap buffer overread in setpwnam()   |
|           |                     |          |          |                   |               | when processing 256-byte usernames                           |
|           |                     |          |          |                   |               | https://avd.aquasec.com/nvd/cve-2025-14104                   |
|           |---------------------|----------|          |                   |---------------|--------------------------------------------------------------|
|           | CVE-2022-0563       | LOW      |          |                   |               | util-linux: partial disclosure of arbitrary files in chfn    |
|           |                     |          |          |                   |               | and chsh when compiled...                                    |
|           |                     |          |          |                   |               | https://avd.aquasec.com/nvd/cve-2022-0563                    |
|-----------|---------------------|          |          |-------------------|---------------|--------------------------------------------------------------|
| coreutils | CVE-2017-18018      |          |          | 9.7-3             |               | coreutils: race condition vulnerability in chown and chgrp   |
|           |                     |          |          |                   |               | https://avd.aquasec.com/nvd/cve-2017-18018                   |
|           |---------------------|          |          |                   |---------------|--------------------------------------------------------------|
|           | CVE-2025-5278       |          |          |                   |               | coreutils: Heap Buffer Under-Read in GNU Coreutils sort via  |
|           |                     |          |          |                   |               | Key Specification                                            |
|           |                     |          |          |                   |               | https://avd.aquasec.com/nvd/cve-2025-5278                    |
```

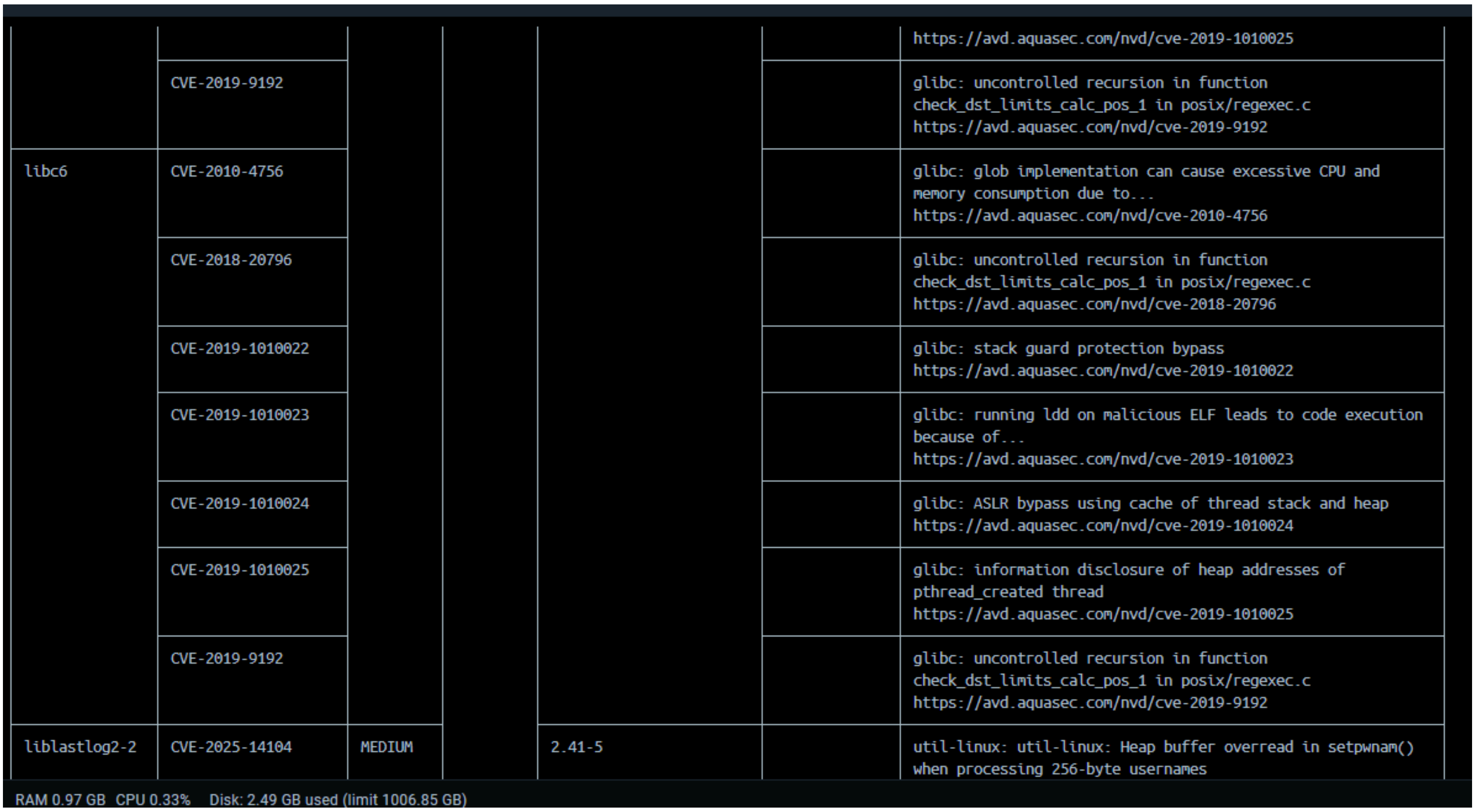


```
| coreutils     | CVE-2017-18018      |          |          | 9.7-3             |               | coreutils: race condition vulnerability in chown and chgrp   |
|               |                     |          |          |                   |               | https://avd.aquasec.com/nvd/cve-2017-18018                   |
|               |---------------------|          |          |                   |---------------|--------------------------------------------------------------|
|               | CVE-2025-5278       |          |          |                   |               | coreutils: Heap Buffer Under-Read in GNU Coreutils sort via  |
|               |                     |          |          |                   |               | Key Specification                                            |
|               |                     |          |          |                   |               | https://avd.aquasec.com/nvd/cve-2025-5278                    |
|---------------|---------------------|          |          |-------------------|---------------|--------------------------------------------------------------|
| libapt-pkg7.0 | CVE-2011-3374       |          |          | 3.0.3             |               | It was found that apt-key in apt, all versions, do not       |
|               |                     |          |          |                   |               | correctly...                                                 |
|               |                     |          |          |                   |               | https://avd.aquasec.com/nvd/cve-2011-3374                    |
|---------------|---------------------|----------|          |-------------------|---------------|--------------------------------------------------------------|
| libblkid1     | CVE-2025-14104      | MEDIUM   |          | 2.41-5            |               | util-linux: util-linux: Heap buffer overread in setpwnam()   |
|               |                     |          |          |                   |               | when processing 256-byte usernames                           |
|               |                     |          |          |                   |               | https://avd.aquasec.com/nvd/cve-2025-14104                   |
|               |---------------------|----------|          |                   |---------------|--------------------------------------------------------------|
|               | CVE-2022-0563       | LOW      |          |                   |               | util-linux: partial disclosure of arbitrary files in chfn    |
|               |                     |          |          |                   |               | and chsh when compiled...                                    |
|               |                     |          |          |                   |               | https://avd.aquasec.com/nvd/cve-2022-0563                    |
|---------------|---------------------|          |          |-------------------|---------------|--------------------------------------------------------------|
| libc-bin      | CVE-2010-4756       |          |          | 2.41-12           |               | 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                 |
|               |---------------------|          |          |                   |---------------|--------------------------------------------------------------|
```



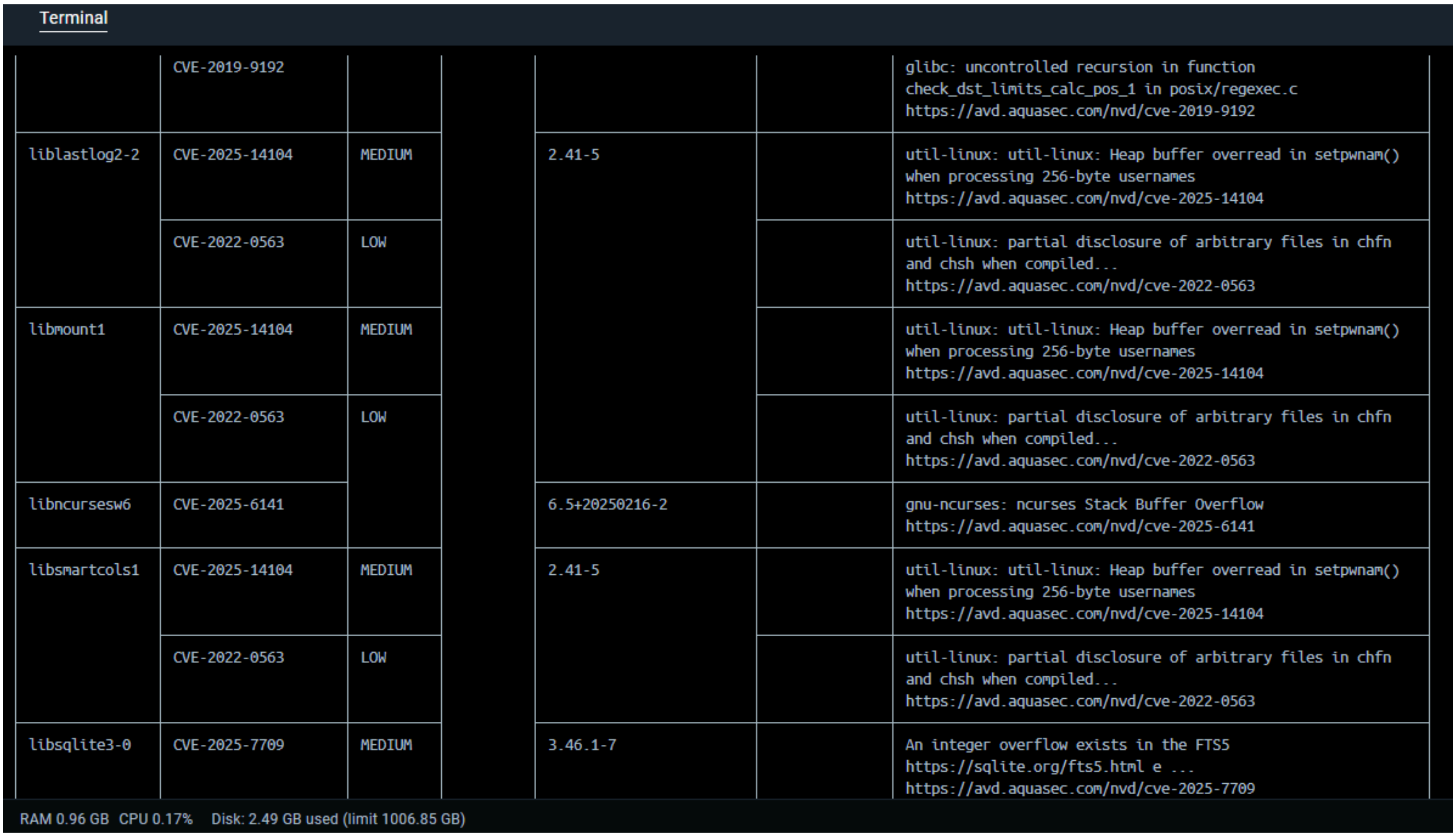
```
                                                         https://avd.aquasec.com/nvd/cve-2022-0563

libc-bin      CVE-2010-4756            2.41-12           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-2010-4756                              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
```

RAM 0.97 GB CPU 0.42% Disk: 2.49 GB used (limit 1006.85 GB)



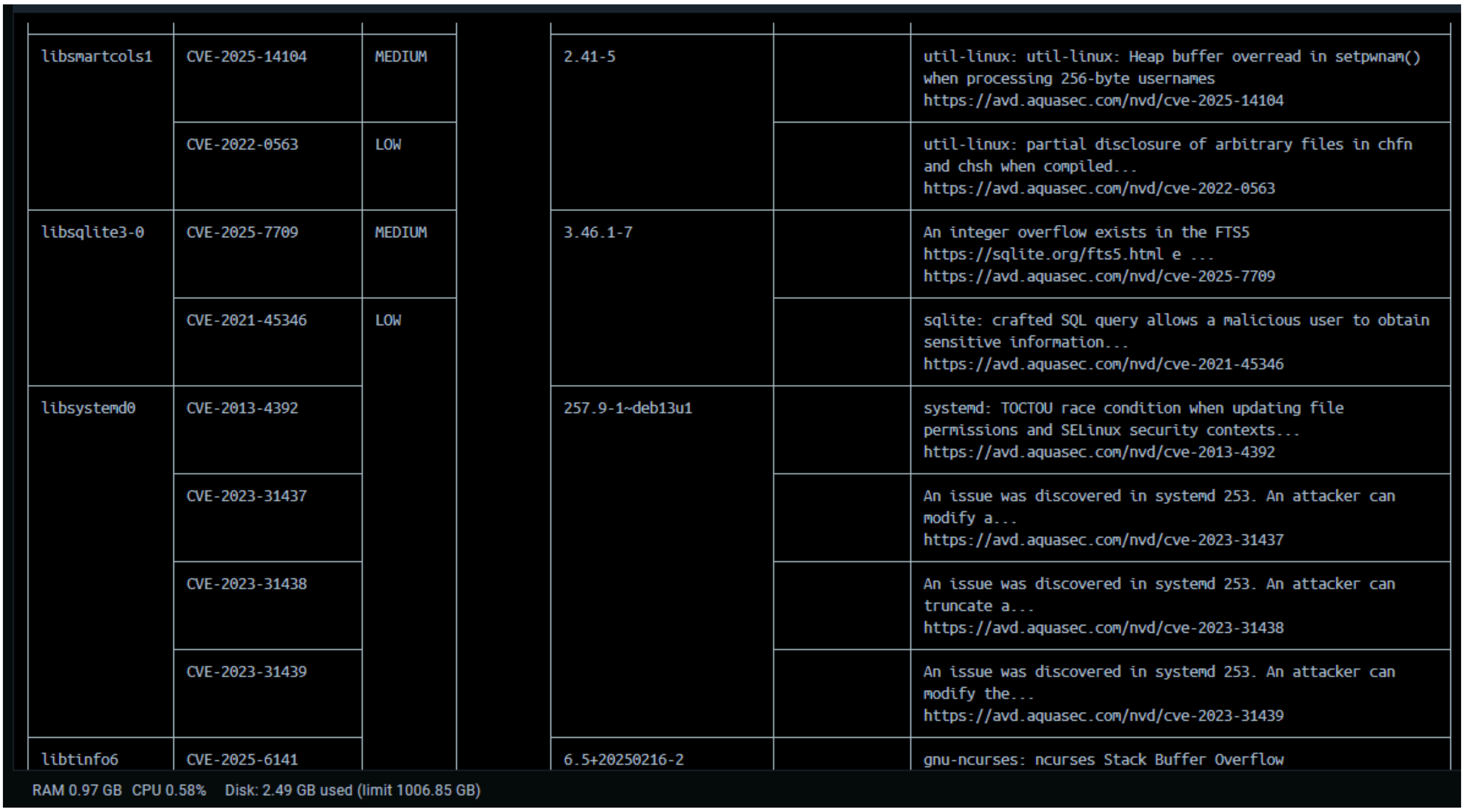
```
                                                         https://avd.aquasec.com/nvd/cve-2019-1010025

              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-2010-4756                              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

liblastlog2-2 CVE-2025-14104  MEDIUM   2.41-5            util-linux: util-linux: Heap buffer overread in setpwnam()
                                                         when processing 256-byte usernames
```

RAM 0.97 GB CPU 0.33% Disk: 2.49 GB used (limit 1006.85 GB)



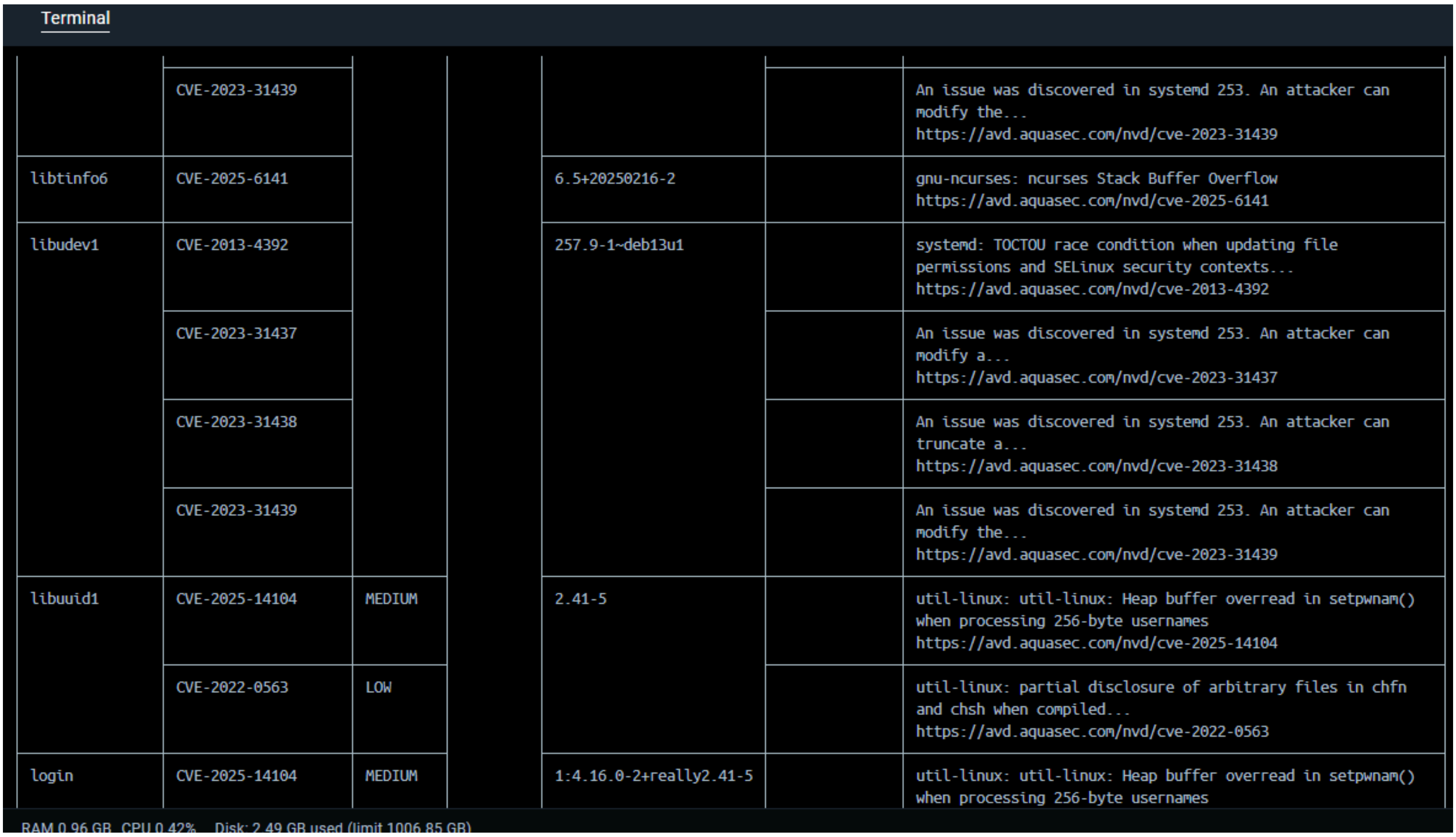
```
│               │ CVE-2019-9192    │        │        │                   │            │ glibc: uncontrolled recursion in function               │
│               │                  │        │        │                   │            │ check_dst_limits_calc_pos_1 in posix/regexec.c          │
│               │                  │        │        │                   │            │ https://avd.aquasec.com/nvd/cve-2019-9192               │
├───────────────┼──────────────────┼────────┤        ├───────────────────┼────────────┼─────────────────────────────────────────────────────────┤
│ liblastlog2-2 │ CVE-2025-14104   │ MEDIUM │        │ 2.41-5            │            │ util-linux: util-linux: Heap buffer overread in setpwnam() │
│               │                  │        │        │                   │            │ when processing 256-byte usernames                      │
│               │                  │        │        │                   │            │ https://avd.aquasec.com/nvd/cve-2025-14104              │
│               ├──────────────────┼────────┤        │                   ├────────────┼─────────────────────────────────────────────────────────┤
│               │ CVE-2022-0563    │ LOW    │        │                   │            │ util-linux: partial disclosure of arbitrary files in chfn │
│               │                  │        │        │                   │            │ and chsh when compiled...                               │
│               │                  │        │        │                   │            │ https://avd.aquasec.com/nvd/cve-2022-0563               │
├───────────────┼──────────────────┼────────┤        │                   ├────────────┼─────────────────────────────────────────────────────────┤
│ libmount1     │ CVE-2025-14104   │ MEDIUM │        │                   │            │ util-linux: util-linux: Heap buffer overread in setpwnam() │
│               │                  │        │        │                   │            │ when processing 256-byte usernames                      │
│               │                  │        │        │                   │            │ https://avd.aquasec.com/nvd/cve-2025-14104              │
│               ├──────────────────┼────────┤        │                   ├────────────┼─────────────────────────────────────────────────────────┤
│               │ CVE-2022-0563    │ LOW    │        │                   │            │ util-linux: partial disclosure of arbitrary files in chfn │
│               │                  │        │        │                   │            │ and chsh when compiled...                               │
│               │                  │        │        │                   │            │ https://avd.aquasec.com/nvd/cve-2022-0563               │
├───────────────┼──────────────────┤        │        ├───────────────────┼────────────┼─────────────────────────────────────────────────────────┤
│ libncursesw6  │ CVE-2025-6141    │        │        │ 6.5+20250216-2    │            │ gnu-ncurses: ncurses Stack Buffer Overflow              │
│               │                  │        │        │                   │            │ https://avd.aquasec.com/nvd/cve-2025-6141               │
├───────────────┼──────────────────┼────────┤        ├───────────────────┼────────────┼─────────────────────────────────────────────────────────┤
│ libsmartcols1 │ CVE-2025-14104   │ MEDIUM │        │ 2.41-5            │            │ util-linux: util-linux: Heap buffer overread in setpwnam() │
│               │                  │        │        │                   │            │ when processing 256-byte usernames                      │
│               │                  │        │        │                   │            │ https://avd.aquasec.com/nvd/cve-2025-14104              │
│               ├──────────────────┼────────┤        │                   ├────────────┼─────────────────────────────────────────────────────────┤
│               │ CVE-2022-0563    │ LOW    │        │                   │            │ util-linux: partial disclosure of arbitrary files in chfn │
│               │                  │        │        │                   │            │ and chsh when compiled...                               │
│               │                  │        │        │                   │            │ https://avd.aquasec.com/nvd/cve-2022-0563               │
├───────────────┼──────────────────┼────────┤        ├───────────────────┼────────────┼─────────────────────────────────────────────────────────┤
│ libsqlite3-0  │ CVE-2025-7709    │ MEDIUM │        │ 3.46.1-7          │            │ An integer overflow exists in the FTS5                  │
│               │                  │        │        │                   │            │ https://sqlite.org/fts5.html e ...                      │
│               │                  │        │        │                   │            │ https://avd.aquasec.com/nvd/cve-2025-7709               │
```

RAM 0.96 GB CPU 0.17% Disk: 2.49 GB used (limit 1006.85 GB)



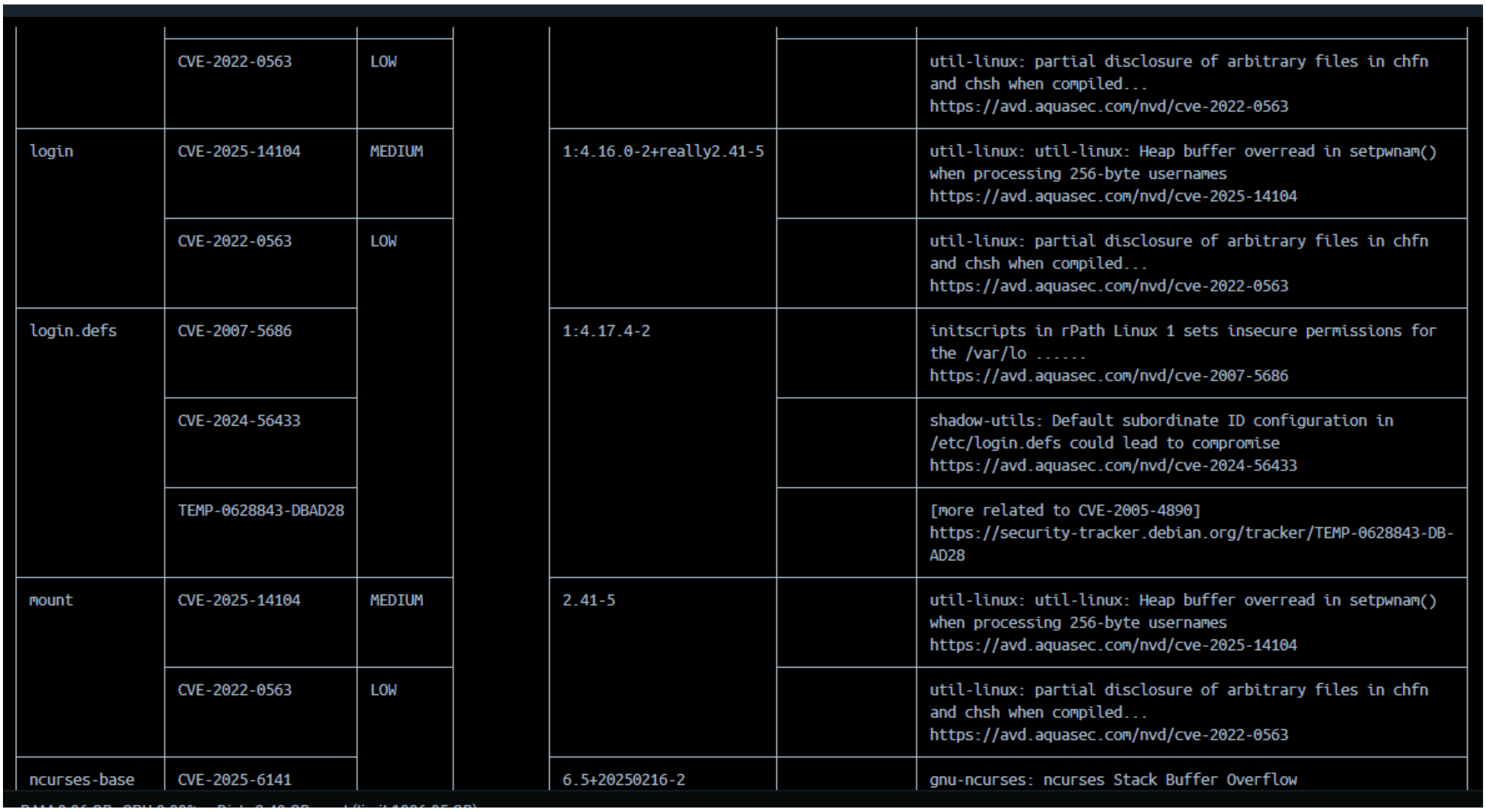
```
│ libsmartcols1 │ CVE-2025-14104   │ MEDIUM │        │ 2.41-5            │            │ util-linux: util-linux: Heap buffer overread in setpwnam() │
│               │                  │        │        │                   │            │ when processing 256-byte usernames                      │
│               │                  │        │        │                   │            │ https://avd.aquasec.com/nvd/cve-2025-14104              │
│               ├──────────────────┼────────┤        │                   ├────────────┼─────────────────────────────────────────────────────────┤
│               │ CVE-2022-0563    │ LOW    │        │                   │            │ util-linux: partial disclosure of arbitrary files in chfn │
│               │                  │        │        │                   │            │ and chsh when compiled...                               │
│               │                  │        │        │                   │            │ https://avd.aquasec.com/nvd/cve-2022-0563               │
├───────────────┼──────────────────┼────────┤        ├───────────────────┼────────────┼─────────────────────────────────────────────────────────┤
│ libsqlite3-0  │ CVE-2025-7709    │ MEDIUM │        │ 3.46.1-7          │            │ An integer overflow exists in the FTS5                  │
│               │                  │        │        │                   │            │ https://sqlite.org/fts5.html e ...                      │
│               │                  │        │        │                   │            │ https://avd.aquasec.com/nvd/cve-2025-7709               │
│               ├──────────────────┼────────┤        │                   ├────────────┼─────────────────────────────────────────────────────────┤
│               │ CVE-2021-45346   │ LOW    │        │                   │            │ sqlite: crafted SQL query allows a malicious user to obtain │
│               │                  │        │        │                   │            │ sensitive information...                                │
│               │                  │        │        │                   │            │ https://avd.aquasec.com/nvd/cve-2021-45346              │
├───────────────┼──────────────────┤        │        ├───────────────────┼────────────┼─────────────────────────────────────────────────────────┤
│ libsystemd0   │ CVE-2013-4392    │        │        │ 257.9-1~deb13u1   │            │ 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              │
├───────────────┼──────────────────┤        │        ├───────────────────┼────────────┼─────────────────────────────────────────────────────────┤
│ libtinfo6     │ CVE-2025-6141    │        │        │ 6.5+20250216-2    │            │ gnu-ncurses: ncurses Stack Buffer Overflow              │
```

RAM 0.97 GB CPU 0.58% Disk: 2.49 GB used (limit 1006.85 GB)

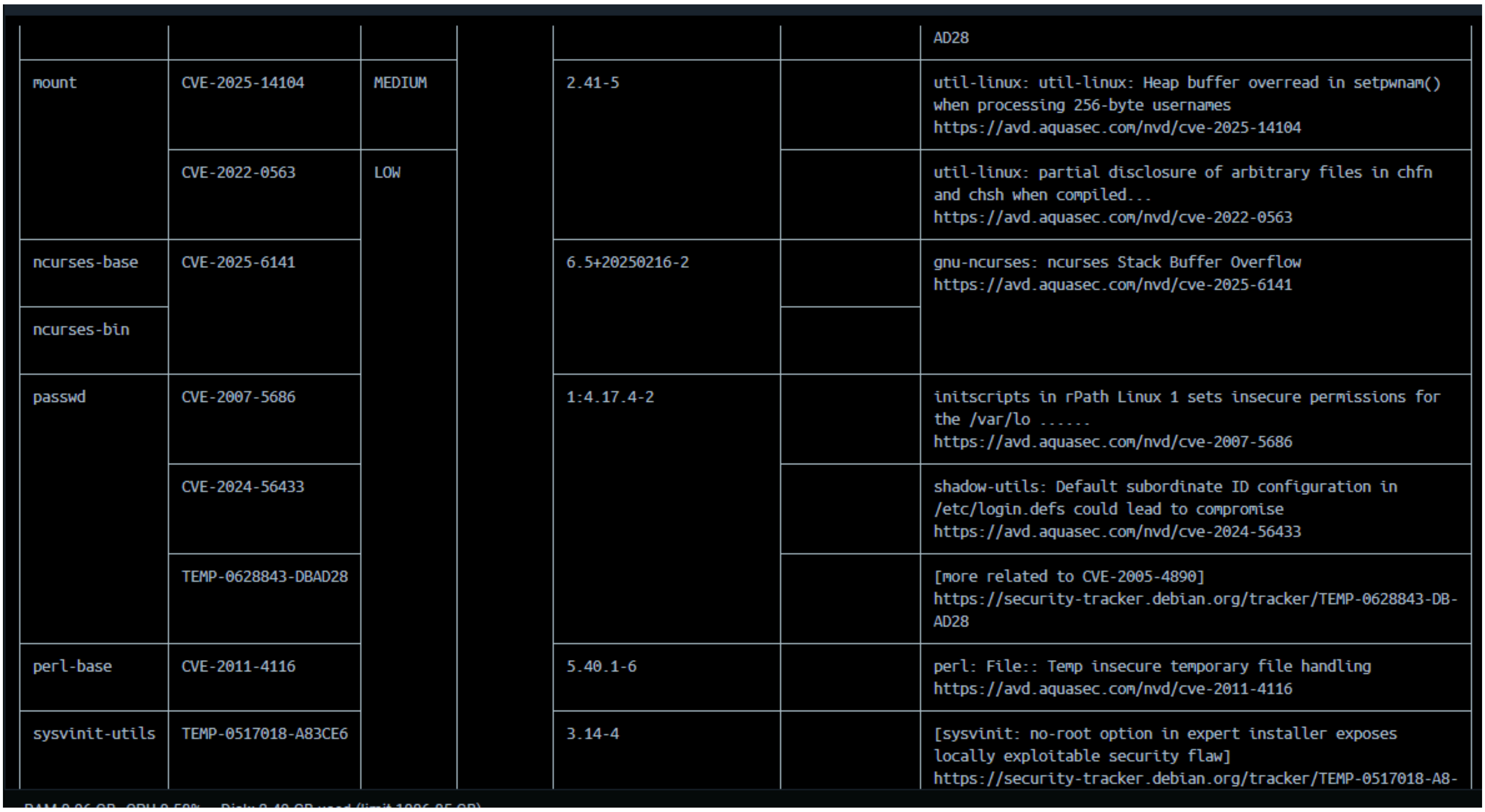


```
│          │ CVE-2023-31439     │        │  │                     │  │ An issue was discovered in systemd 253. An attacker can     │
│          │                    │        │  │                     │  │ modify the...                                               │
│          │                    │        │  │                     │  │ https://avd.aquasec.com/nvd/cve-2023-31439                  │
├──────────┼────────────────────┤        │  ├─────────────────────┼──┼─────────────────────────────────────────────────────────────┤
│ libtinfo6│ CVE-2025-6141      │        │  │ 6.5+20250216-2      │  │ gnu-ncurses: ncurses Stack Buffer Overflow                  │
│          │                    │        │  │                     │  │ https://avd.aquasec.com/nvd/cve-2025-6141                   │
├──────────┼────────────────────┤        │  ├─────────────────────┼──┼─────────────────────────────────────────────────────────────┤
│ libudev1 │ CVE-2013-4392      │        │  │ 257.9-1~deb13u1     │  │ 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-2025-14104     │ MEDIUM │  │ 2.41-5              │  │ util-linux: util-linux: Heap buffer overread in setpwnam()  │
│          │                    │        │  │                     │  │ when processing 256-byte usernames                          │
│          │                    │        │  │                     │  │ https://avd.aquasec.com/nvd/cve-2025-14104                  │
│          ├────────────────────┼────────┤  │                     ├──┼─────────────────────────────────────────────────────────────┤
│          │ CVE-2022-0563      │ LOW    │  │                     │  │ util-linux: partial disclosure of arbitrary files in chfn   │
│          │                    │        │  │                     │  │ and chsh when compiled...                                   │
│          │                    │        │  │                     │  │ https://avd.aquasec.com/nvd/cve-2022-0563                   │
├──────────┼────────────────────┼────────┤  ├─────────────────────┼──┼─────────────────────────────────────────────────────────────┤
│ login    │ CVE-2025-14104     │ MEDIUM │  │ 1:4.16.0-2+really2.41-5 │ util-linux: util-linux: Heap buffer overread in setpwnam()  │
│          │                    │        │  │                     │  │ when processing 256-byte usernames                          │
```

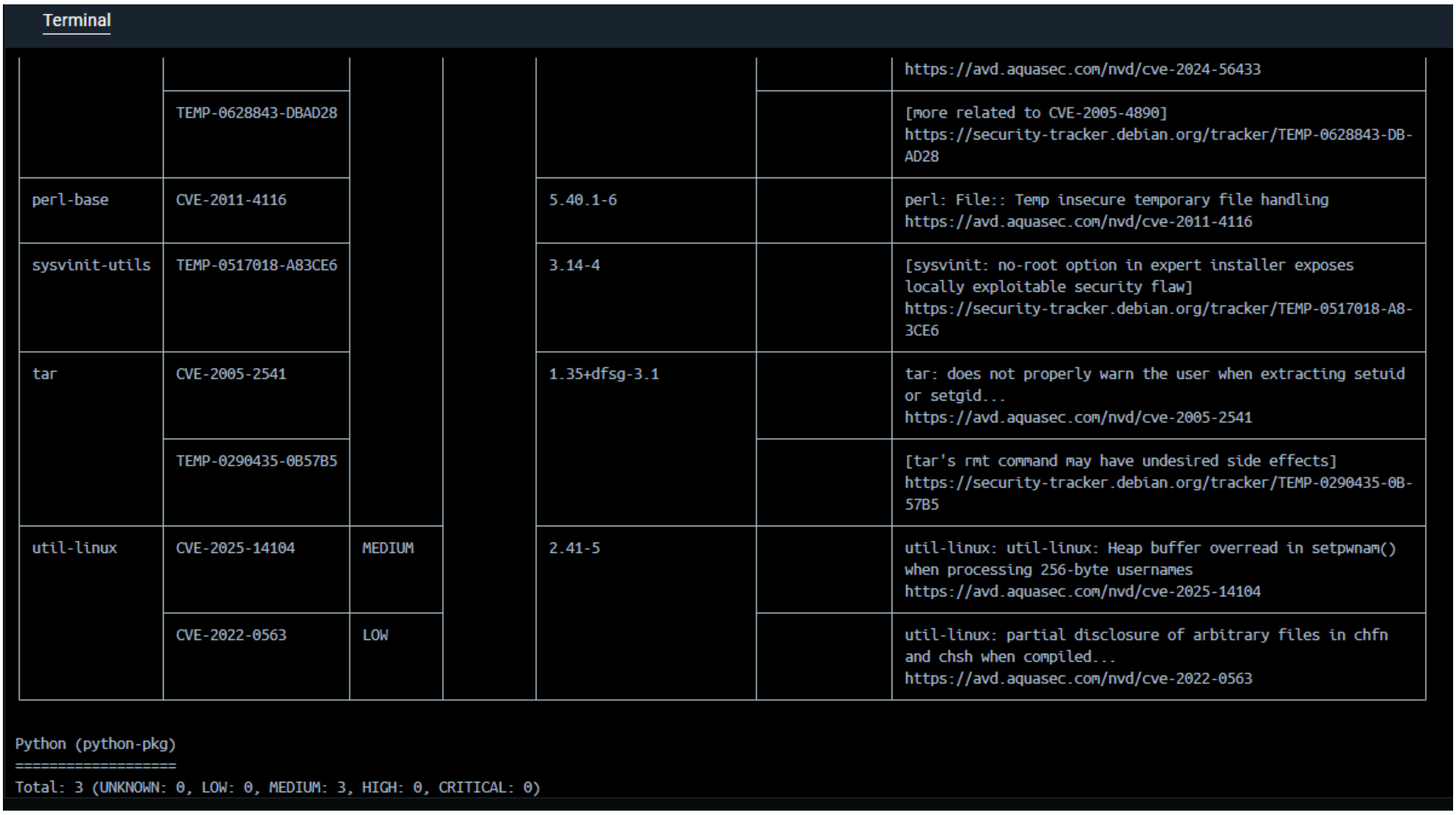
RAM 0.96 GB CPU 0.42% Disk: 2.49 GB used (limit 1006.85 GB)



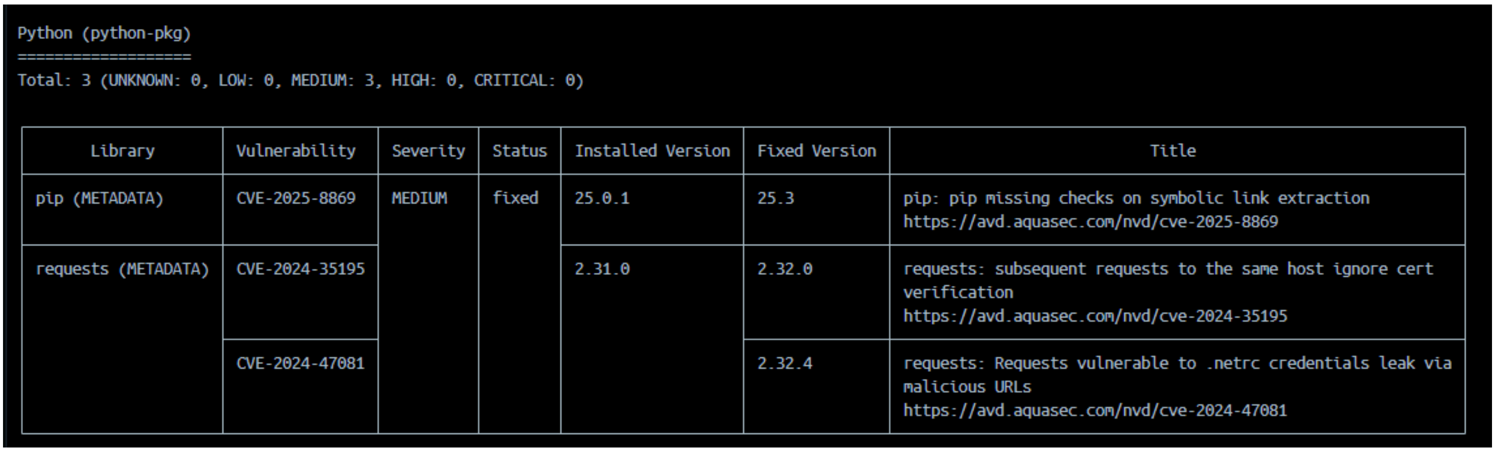
```
│          │ CVE-2022-0563      │ LOW    │  │                     │  │ util-linux: partial disclosure of arbitrary files in chfn   │
│          │                    │        │  │                     │  │ and chsh when compiled...                                   │
│          │                    │        │  │                     │  │ https://avd.aquasec.com/nvd/cve-2022-0563                   │
├──────────┼────────────────────┼────────┤  ├─────────────────────┼──┼─────────────────────────────────────────────────────────────┤
│ login    │ CVE-2025-14104     │ MEDIUM │  │ 1:4.16.0-2+really2.41-5 │ util-linux: util-linux: Heap buffer overread in setpwnam()  │
│          │                    │        │  │                     │  │ when processing 256-byte usernames                          │
│          │                    │        │  │                     │  │ https://avd.aquasec.com/nvd/cve-2025-14104                  │
│          ├────────────────────┼────────┤  │                     ├──┼─────────────────────────────────────────────────────────────┤
│          │ CVE-2022-0563      │ LOW    │  │                     │  │ util-linux: partial disclosure of arbitrary files in chfn   │
│          │                    │        │  │                     │  │ and chsh when compiled...                                   │
│          │                    │        │  │                     │  │ https://avd.aquasec.com/nvd/cve-2022-0563                   │
├──────────┼────────────────────┤        │  ├─────────────────────┼──┼─────────────────────────────────────────────────────────────┤
│login.defs│ CVE-2007-5686      │        │  │ 1:4.17.4-2          │  │ initscripts in rPath Linux 1 sets insecure permissions for  │
│          │                    │        │  │                     │  │ the /var/lo ......                                          │
│          │                    │        │  │                     │  │ https://avd.aquasec.com/nvd/cve-2007-5686                   │
│          ├────────────────────┤        │  │                     ├──┼─────────────────────────────────────────────────────────────┤
│          │ 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-2025-14104     │ MEDIUM │  │ 2.41-5              │  │ util-linux: util-linux: Heap buffer overread in setpwnam()  │
│          │                    │        │  │                     │  │ when processing 256-byte usernames                          │
│          │                    │        │  │                     │  │ https://avd.aquasec.com/nvd/cve-2025-14104                  │
│          ├────────────────────┼────────┤  │                     ├──┼─────────────────────────────────────────────────────────────┤
│          │ CVE-2022-0563      │ LOW    │  │                     │  │ util-linux: partial disclosure of arbitrary files in chfn   │
│          │                    │        │  │                     │  │ and chsh when compiled...                                   │
│          │                    │        │  │                     │  │ https://avd.aquasec.com/nvd/cve-2022-0563                   │
├──────────┼────────────────────┤        │  ├─────────────────────┼──┼─────────────────────────────────────────────────────────────┤
│ncurses-base│ CVE-2025-6141    │        │  │ 6.5+20250216-2      │  │ gnu-ncurses: ncurses Stack Buffer Overflow                  │
```



```
│               │                    │          │         │                       │              │ AD28                                                      │
├───────────────┼────────────────────┼──────────┤         ├───────────────────────┼──────────────┼───────────────────────────────────────────────────────────┤
│ mount         │ CVE-2025-14104     │ MEDIUM   │         │ 2.41-5                │              │ util-linux: util-linux: Heap buffer overread in setpwnam() │
│               │                    │          │         │                       │              │ when processing 256-byte usernames                         │
│               │                    │          │         │                       │              │ https://avd.aquasec.com/nvd/cve-2025-14104                 │
│               ├────────────────────┼──────────┤         │                       ├──────────────┼───────────────────────────────────────────────────────────┤
│               │ CVE-2022-0563      │ LOW      │         │                       │              │ util-linux: partial disclosure of arbitrary files in chfn  │
│               │                    │          │         │                       │              │ and chsh when compiled...                                  │
│               │                    │          │         │                       │              │ https://avd.aquasec.com/nvd/cve-2022-0563                  │
├───────────────┼────────────────────┤          │         ├───────────────────────┼──────────────┼───────────────────────────────────────────────────────────┤
│ ncurses-base  │ CVE-2025-6141      │          │         │ 6.5+20250216-2        │              │ gnu-ncurses: ncurses Stack Buffer Overflow                 │
│               │                    │          │         │                       │              │ https://avd.aquasec.com/nvd/cve-2025-6141                  │
├───────────────┤                    │          │         │                       ├──────────────┤                                                           │
│ ncurses-bin   │                    │          │         │                       │              │                                                           │
│               │                    │          │         │                       │              │                                                           │
├───────────────┼────────────────────┤          │         ├───────────────────────┼──────────────┼───────────────────────────────────────────────────────────┤
│ passwd        │ CVE-2007-5686      │          │         │ 1:4.17.4-2            │              │ initscripts in rPath Linux 1 sets insecure permissions for │
│               │                    │          │         │                       │              │ the /var/lo ......                                         │
│               │                    │          │         │                       │              │ https://avd.aquasec.com/nvd/cve-2007-5686                  │
│               ├────────────────────┤          │         │                       ├──────────────┼───────────────────────────────────────────────────────────┤
│               │ 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-2011-4116      │          │         │ 5.40.1-6              │              │ perl: File:: Temp insecure temporary file handling         │
│               │                    │          │         │                       │              │ https://avd.aquasec.com/nvd/cve-2011-4116                  │
├───────────────┼────────────────────┤          │         ├───────────────────────┼──────────────┼───────────────────────────────────────────────────────────┤
│ sysvinit-utils│ TEMP-0517018-A83CE6│          │         │ 3.14-4                │              │ [sysvinit: no-root option in expert installer exposes      │
│               │                    │          │         │                       │              │ locally exploitable security flaw]                         │
│               │                    │          │         │                       │              │ https://security-tracker.debian.org/tracker/TEMP-0517018-A8-│
```



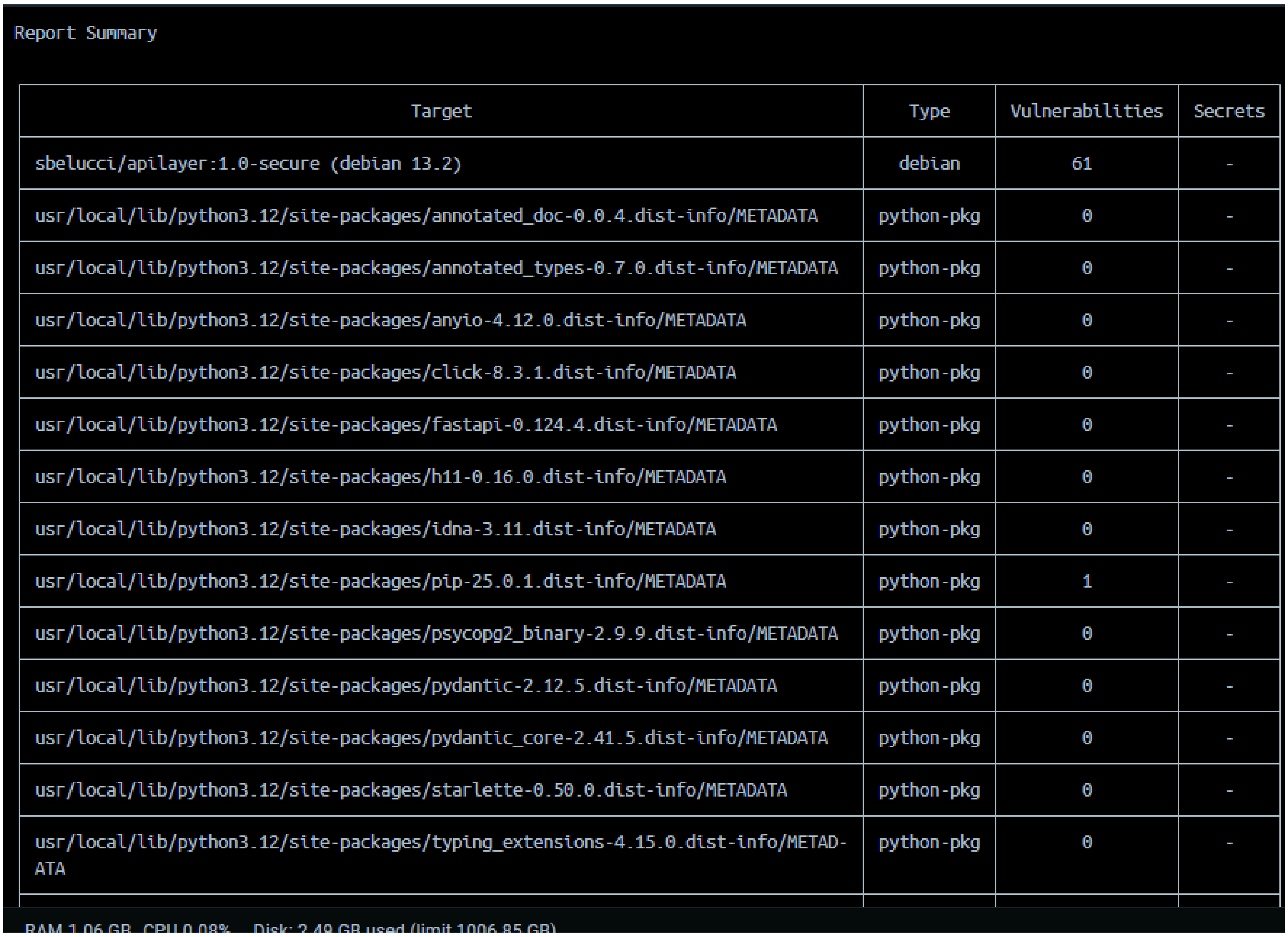
```
│               │                    │          │         │                       │              │ https://avd.aquasec.com/nvd/cve-2024-56433                 │
│               │                    │          │         │                       ├──────────────┼───────────────────────────────────────────────────────────┤
│               │ TEMP-0628843-DBAD28│          │         │                       │              │ [more related to CVE-2005-4890]                            │
│               │                    │          │         │                       │              │ https://security-tracker.debian.org/tracker/TEMP-0628843-DB-│
│               │                    │          │         │                       │              │ AD28                                                       │
├───────────────┼────────────────────┤          │         ├───────────────────────┼──────────────┼───────────────────────────────────────────────────────────┤
│ perl-base     │ CVE-2011-4116      │          │         │ 5.40.1-6              │              │ perl: File:: Temp insecure temporary file handling         │
│               │                    │          │         │                       │              │ https://avd.aquasec.com/nvd/cve-2011-4116                  │
├───────────────┼────────────────────┤          │         ├───────────────────────┼──────────────┼───────────────────────────────────────────────────────────┤
│ sysvinit-utils│ TEMP-0517018-A83CE6│          │         │ 3.14-4                │              │ [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      │          │         │ 1.35+dfsg-3.1         │              │ 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-2025-14104     │ MEDIUM   │         │ 2.41-5                │              │ util-linux: util-linux: Heap buffer overread in setpwnam() │
│               │                    │          │         │                       │              │ when processing 256-byte usernames                         │
│               │                    │          │         │                       │              │ https://avd.aquasec.com/nvd/cve-2025-14104                 │
│               ├────────────────────┼──────────┤         │                       ├──────────────┼───────────────────────────────────────────────────────────┤
│               │ CVE-2022-0563      │ LOW      │         │                       │              │ util-linux: partial disclosure of arbitrary files in chfn  │
│               │                    │          │         │                       │              │ and chsh when compiled...                                  │
│               │                    │          │         │                       │              │ https://avd.aquasec.com/nvd/cve-2022-0563                  │
└───────────────┴────────────────────┴──────────┴─────────┴───────────────────────┴──────────────┴───────────────────────────────────────────────────────────┘

Python (python-pkg)
===================
Total: 3 (UNKNOWN: 0, LOW: 0, MEDIUM: 3, HIGH: 0, CRITICAL: 0)
```



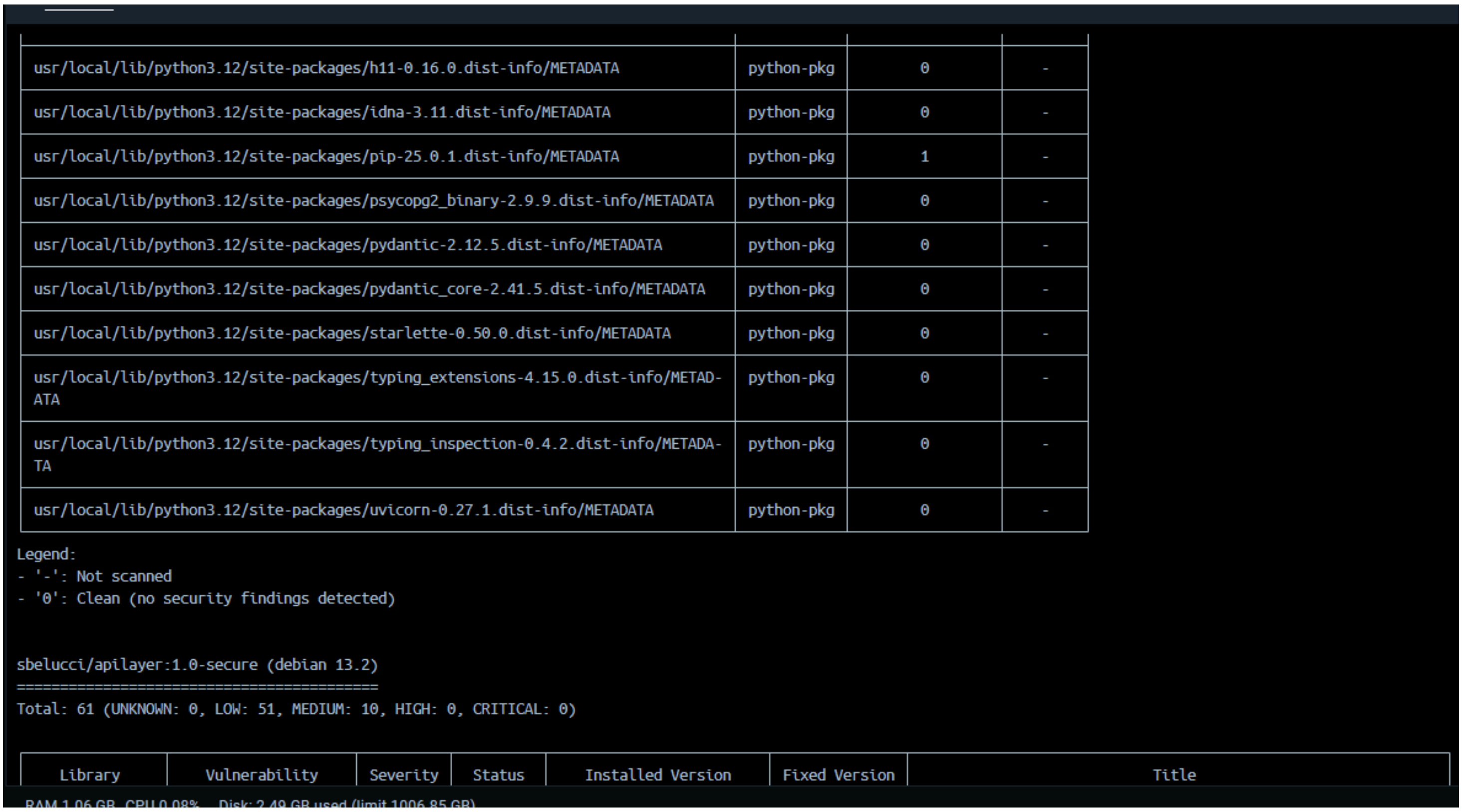
```
Python (python-pkg)
===================
Total: 3 (UNKNOWN: 0, LOW: 0, MEDIUM: 3, HIGH: 0, CRITICAL: 0)

┌─────────────────────┬────────────────┬──────────┬────────┬───────────────────┬───────────────┬──────────────────────────────────────────────────────────────┐
│       Library       │ Vulnerability  │ Severity │ Status │ Installed Version │ Fixed Version │                            Title                             │
├─────────────────────┼────────────────┼──────────┼────────┼───────────────────┼───────────────┼──────────────────────────────────────────────────────────────┤
│ pip (METADATA)      │ CVE-2025-8869  │ MEDIUM   │ fixed  │ 25.0.1            │ 25.3          │ pip: pip missing checks on symbolic link extraction          │
│                     │                │          │        │                   │               │ https://avd.aquasec.com/nvd/cve-2025-8869                    │
├─────────────────────┼────────────────┤          │        ├───────────────────┼───────────────┼──────────────────────────────────────────────────────────────┤
│ requests (METADATA) │ CVE-2024-35195 │          │        │ 2.31.0            │ 2.32.0        │ requests: subsequent requests to the same host ignore cert   │
│                     │                │          │        │                   │               │ verification                                                 │
│                     │                │          │        │                   │               │ https://avd.aquasec.com/nvd/cve-2024-35195                   │
│                     ├────────────────┤          │        │                   ├───────────────┼──────────────────────────────────────────────────────────────┤
│                     │ CVE-2024-47081 │          │        │                   │ 2.32.4        │ requests: Requests vulnerable to .netrc credentials leak via │
│                     │                │          │        │                   │               │ malicious URLs                                               │
│                     │                │          │        │                   │               │ https://avd.aquasec.com/nvd/cve-2024-47081                   │
└─────────────────────┴────────────────┴──────────┴────────┴───────────────────┴───────────────┴──────────────────────────────────────────────────────────────┘
```

2) **Resultado del reporte de la image sbelucci/apilayer:1.0-secure**

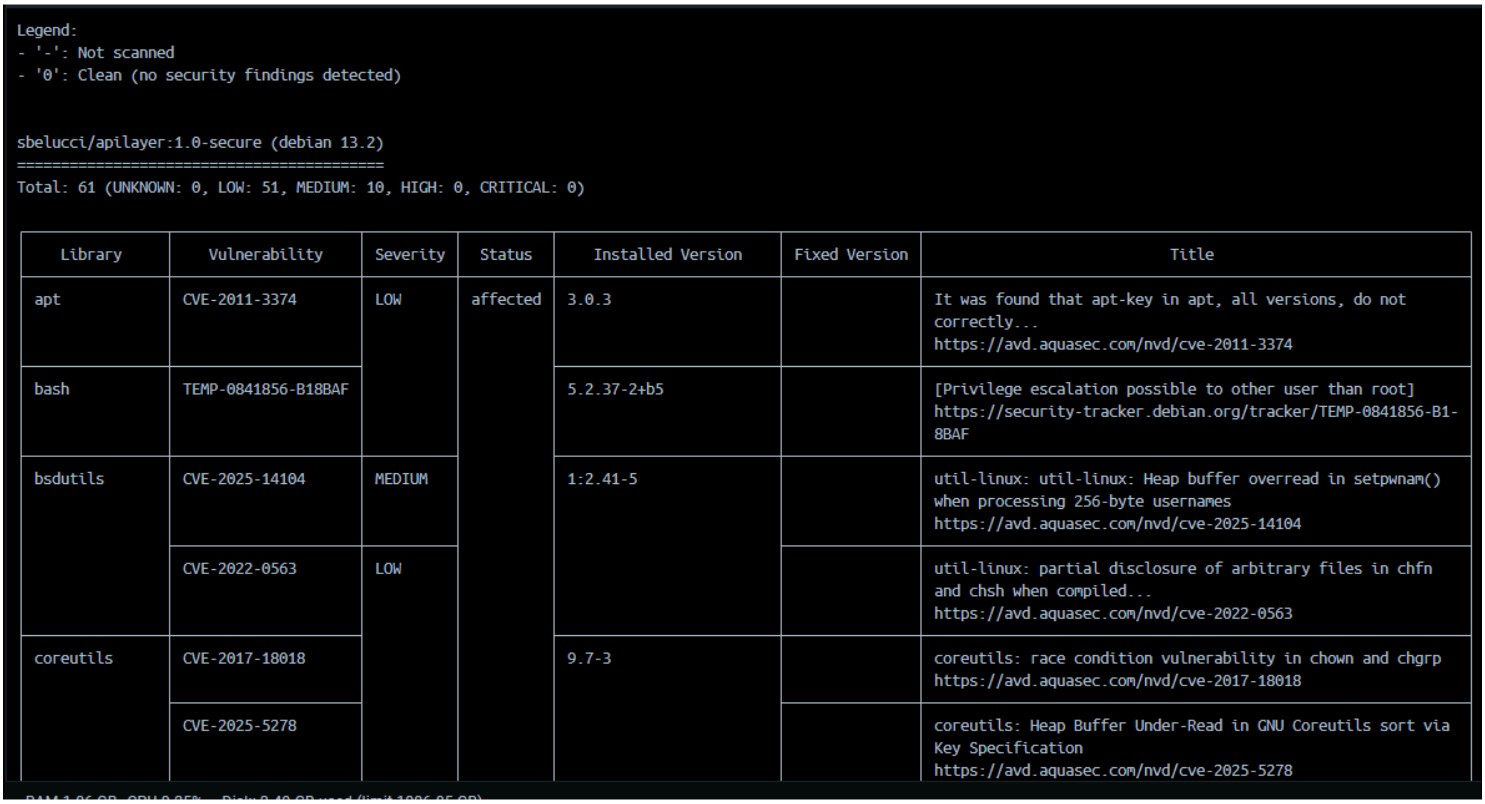
docker run --rm -v /var/run/docker.sock:/var/run/docker.sock aquasec/trivy:latest image sbelucci/apilayer:1.0-secure



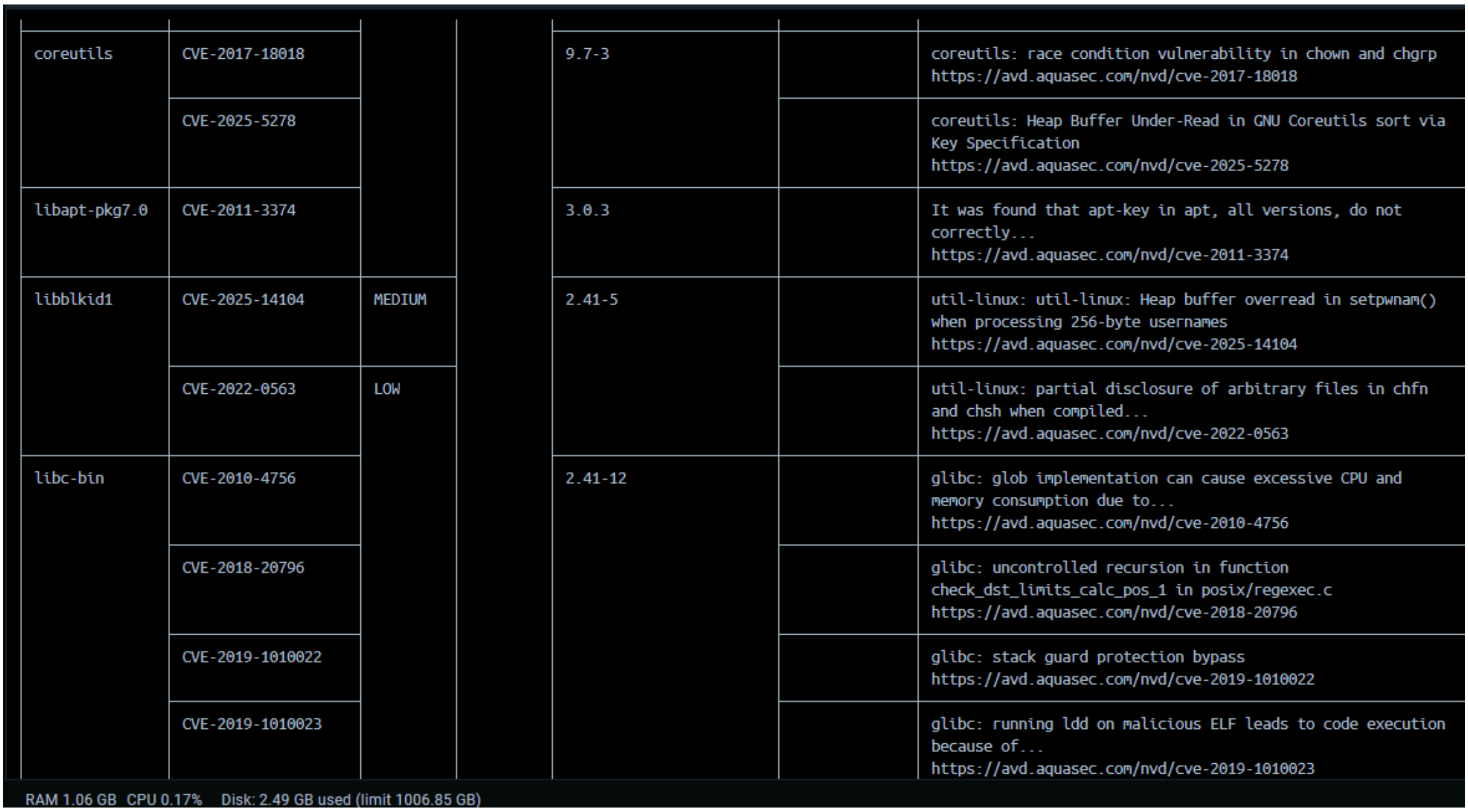
```
Report Summary

┌─────────────────────────────────────────────────────────────────────────────┬────────────┬─────────────────┬─────────┐
│                                   Target                                    │    Type    │ Vulnerabilities │ Secrets │
├─────────────────────────────────────────────────────────────────────────────┼────────────┼─────────────────┼─────────┤
│ sbelucci/apilayer:1.0-secure (debian 13.2)                                  │   debian   │       61        │    -    │
├─────────────────────────────────────────────────────────────────────────────┼────────────┼─────────────────┼─────────┤
│ usr/local/lib/python3.12/site-packages/annotated_doc-0.0.4.dist-info/METADATA │ python-pkg │        0        │    -    │
├─────────────────────────────────────────────────────────────────────────────┼────────────┼─────────────────┼─────────┤
│ usr/local/lib/python3.12/site-packages/annotated_types-0.7.0.dist-info/METADATA │ python-pkg │        0        │    -    │
├─────────────────────────────────────────────────────────────────────────────┼────────────┼─────────────────┼─────────┤
│ usr/local/lib/python3.12/site-packages/anyio-4.12.0.dist-info/METADATA      │ python-pkg │        0        │    -    │
├─────────────────────────────────────────────────────────────────────────────┼────────────┼─────────────────┼─────────┤
│ usr/local/lib/python3.12/site-packages/click-8.3.1.dist-info/METADATA       │ python-pkg │        0        │    -    │
├─────────────────────────────────────────────────────────────────────────────┼────────────┼─────────────────┼─────────┤
│ usr/local/lib/python3.12/site-packages/fastapi-0.124.4.dist-info/METADATA   │ python-pkg │        0        │    -    │
├─────────────────────────────────────────────────────────────────────────────┼────────────┼─────────────────┼─────────┤
│ usr/local/lib/python3.12/site-packages/h11-0.16.0.dist-info/METADATA        │ python-pkg │        0        │    -    │
├─────────────────────────────────────────────────────────────────────────────┼────────────┼─────────────────┼─────────┤
│ usr/local/lib/python3.12/site-packages/idna-3.11.dist-info/METADATA         │ python-pkg │        0        │    -    │
├─────────────────────────────────────────────────────────────────────────────┼────────────┼─────────────────┼─────────┤
│ usr/local/lib/python3.12/site-packages/pip-25.0.1.dist-info/METADATA        │ python-pkg │        1        │    -    │
├─────────────────────────────────────────────────────────────────────────────┼────────────┼─────────────────┼─────────┤
│ usr/local/lib/python3.12/site-packages/psycopg2_binary-2.9.9.dist-info/METADATA │ python-pkg │        0        │    -    │
├─────────────────────────────────────────────────────────────────────────────┼────────────┼─────────────────┼─────────┤
│ usr/local/lib/python3.12/site-packages/pydantic-2.12.5.dist-info/METADATA   │ python-pkg │        0        │    -    │
├─────────────────────────────────────────────────────────────────────────────┼────────────┼─────────────────┼─────────┤
│ usr/local/lib/python3.12/site-packages/pydantic_core-2.41.5.dist-info/METADATA │ python-pkg │        0        │    -    │
├─────────────────────────────────────────────────────────────────────────────┼────────────┼─────────────────┼─────────┤
│ usr/local/lib/python3.12/site-packages/starlette-0.50.0.dist-info/METADATA  │ python-pkg │        0        │    -    │
├─────────────────────────────────────────────────────────────────────────────┼────────────┼─────────────────┼─────────┤
│ usr/local/lib/python3.12/site-packages/typing_extensions-4.15.0.dist-info/METAD- │ python-pkg │        0        │    -    │
│ ATA                                                                         │            │                 │         │
├─────────────────────────────────────────────────────────────────────────────┼────────────┼─────────────────┼─────────┤

RAM 1.06 GB  CPU 0.08%    Disk: 2.49 GB used (limit 1006.85 GB)
```



```
│                                                                              │            │           │         │
├──────────────────────────────────────────────────────────────────────────────┼────────────┼───────────┼─────────┤
│ usr/local/lib/python3.12/site-packages/h11-0.16.0.dist-info/METADATA         │ python-pkg │     0     │    -    │
├──────────────────────────────────────────────────────────────────────────────┼────────────┼───────────┼─────────┤
│ usr/local/lib/python3.12/site-packages/idna-3.11.dist-info/METADATA          │ python-pkg │     0     │    -    │
├──────────────────────────────────────────────────────────────────────────────┼────────────┼───────────┼─────────┤
│ usr/local/lib/python3.12/site-packages/pip-25.0.1.dist-info/METADATA         │ python-pkg │     1     │    -    │
├──────────────────────────────────────────────────────────────────────────────┼────────────┼───────────┼─────────┤
│ usr/local/lib/python3.12/site-packages/psycopg2_binary-2.9.9.dist-info/METADATA │ python-pkg │     0     │    -    │
├──────────────────────────────────────────────────────────────────────────────┼────────────┼───────────┼─────────┤
│ usr/local/lib/python3.12/site-packages/pydantic-2.12.5.dist-info/METADATA    │ python-pkg │     0     │    -    │
├──────────────────────────────────────────────────────────────────────────────┼────────────┼───────────┼─────────┤
│ usr/local/lib/python3.12/site-packages/pydantic_core-2.41.5.dist-info/METADATA │ python-pkg │     0     │    -    │
├──────────────────────────────────────────────────────────────────────────────┼────────────┼───────────┼─────────┤
│ usr/local/lib/python3.12/site-packages/starlette-0.50.0.dist-info/METADATA   │ python-pkg │     0     │    -    │
├──────────────────────────────────────────────────────────────────────────────┼────────────┼───────────┼─────────┤
│ usr/local/lib/python3.12/site-packages/typing_extensions-4.15.0.dist-info/METAD- │ python-pkg │     0     │    -    │
│ ATA                                                                          │            │           │         │
├──────────────────────────────────────────────────────────────────────────────┼────────────┼───────────┼─────────┤
│ usr/local/lib/python3.12/site-packages/typing_inspection-0.4.2.dist-info/METADA- │ python-pkg │     0     │    -    │
│ TA                                                                           │            │           │         │
├──────────────────────────────────────────────────────────────────────────────┼────────────┼───────────┼─────────┤
│ usr/local/lib/python3.12/site-packages/uvicorn-0.27.1.dist-info/METADATA     │ python-pkg │     0     │    -    │
└──────────────────────────────────────────────────────────────────────────────┴────────────┴───────────┴─────────┘
Legend:
- '-': Not scanned
- '0': Clean (no security findings detected)


sbelucci/apilayer:1.0-secure (debian 13.2)
==========================================
Total: 61 (UNKNOWN: 0, LOW: 51, MEDIUM: 10, HIGH: 0, CRITICAL: 0)

┌───────────┬───────────────┬──────────┬────────┬───────────────────┬───────────────┬──────────────────────────────────────┐
│  Library  │ Vulnerability │ Severity │ Status │ Installed Version │ Fixed Version │                Title                 │
```

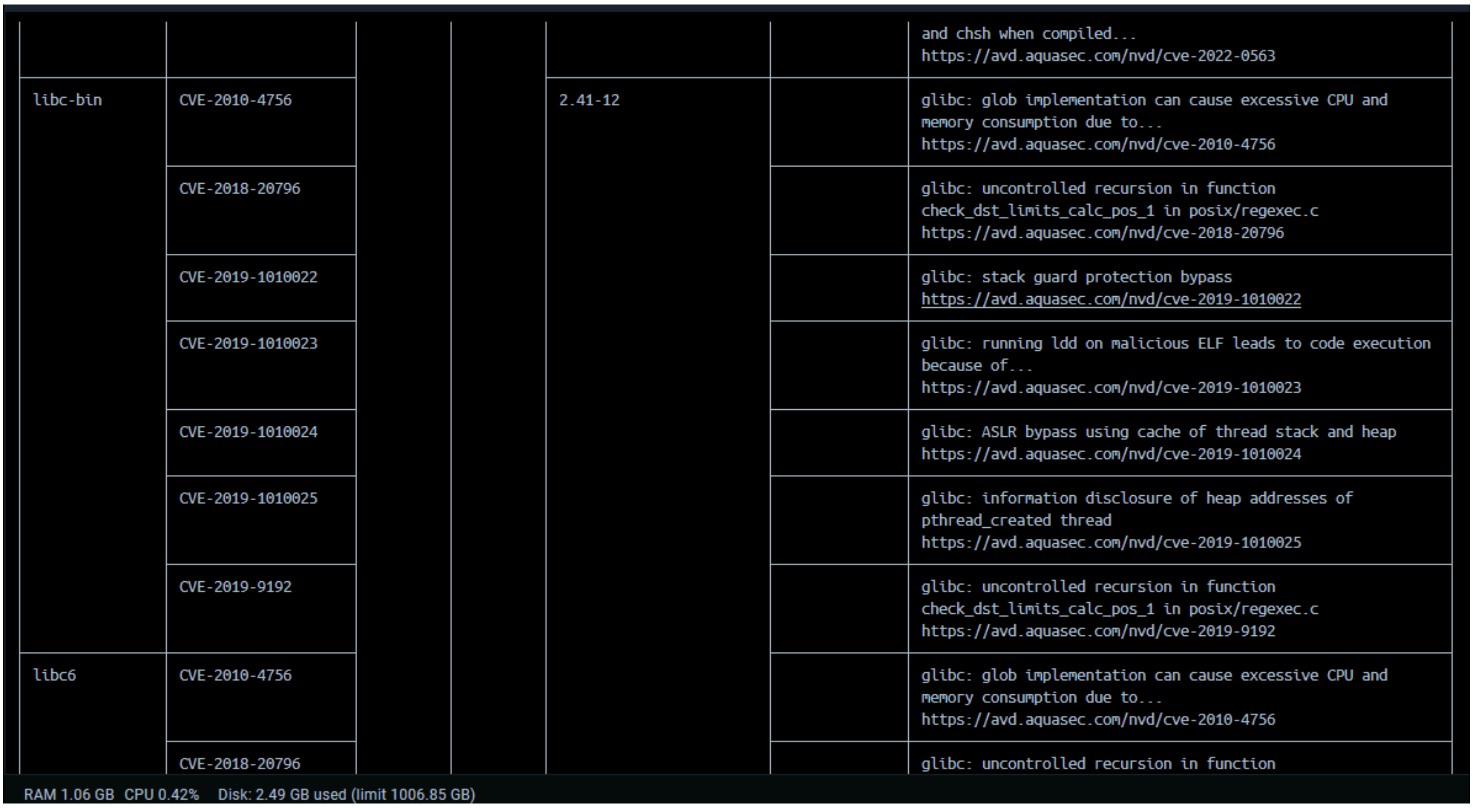


```
Legend:
- '-': Not scanned
- '0': Clean (no security findings detected)


sbelucci/apilayer:1.0-secure (debian 13.2)
==========================================
Total: 61 (UNKNOWN: 0, LOW: 51, MEDIUM: 10, HIGH: 0, CRITICAL: 0)

┌───────────┬─────────────────────┬──────────┬──────────┬───────────────────┬───────────────┬──────────────────────────────────────────────────────────────┐
│  Library  │    Vulnerability    │ Severity │  Status  │ Installed Version │ Fixed Version │                            Title                             │
├───────────┼─────────────────────┼──────────┼──────────┼───────────────────┼───────────────┼──────────────────────────────────────────────────────────────┤
│ apt       │ CVE-2011-3374       │ LOW      │ affected │ 3.0.3             │               │ 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 │          │          │ 5.2.37-2+b5       │               │ [Privilege escalation possible to other user than root]      │
│           │                     │          │          │                   │               │ https://security-tracker.debian.org/tracker/TEMP-0841856-B1- │
│           │                     │          │          │                   │               │ 8BAF                                                         │
├───────────┼─────────────────────┼──────────┤          ├───────────────────┼───────────────┼──────────────────────────────────────────────────────────────┤
│ bsdutils  │ CVE-2025-14104      │ MEDIUM   │          │ 1:2.41-5          │               │ util-linux: util-linux: Heap buffer overread in setpwnam()   │
│           │                     │          │          │                   │               │ when processing 256-byte usernames                           │
│           │                     │          │          │                   │               │ https://avd.aquasec.com/nvd/cve-2025-14104                   │
│           ├─────────────────────┼──────────┤          │                   ├───────────────┼──────────────────────────────────────────────────────────────┤
│           │ CVE-2022-0563       │ LOW      │          │                   │               │ util-linux: partial disclosure of arbitrary files in chfn    │
│           │                     │          │          │                   │               │ and chsh when compiled...                                    │
│           │                     │          │          │                   │               │ https://avd.aquasec.com/nvd/cve-2022-0563                    │
├───────────┼─────────────────────┤          │          ├───────────────────┼───────────────┼──────────────────────────────────────────────────────────────┤
│ coreutils │ CVE-2017-18018      │          │          │ 9.7-3             │               │ coreutils: race condition vulnerability in chown and chgrp   │
│           │                     │          │          │                   │               │ https://avd.aquasec.com/nvd/cve-2017-18018                   │
│           ├─────────────────────┤          │          │                   ├───────────────┼──────────────────────────────────────────────────────────────┤
│           │ CVE-2025-5278       │          │          │                   │               │ coreutils: Heap Buffer Under-Read in GNU Coreutils sort via  │
│           │                     │          │          │                   │               │ Key Specification                                            │
│           │                     │          │          │                   │               │ https://avd.aquasec.com/nvd/cve-2025-5278                    │
```



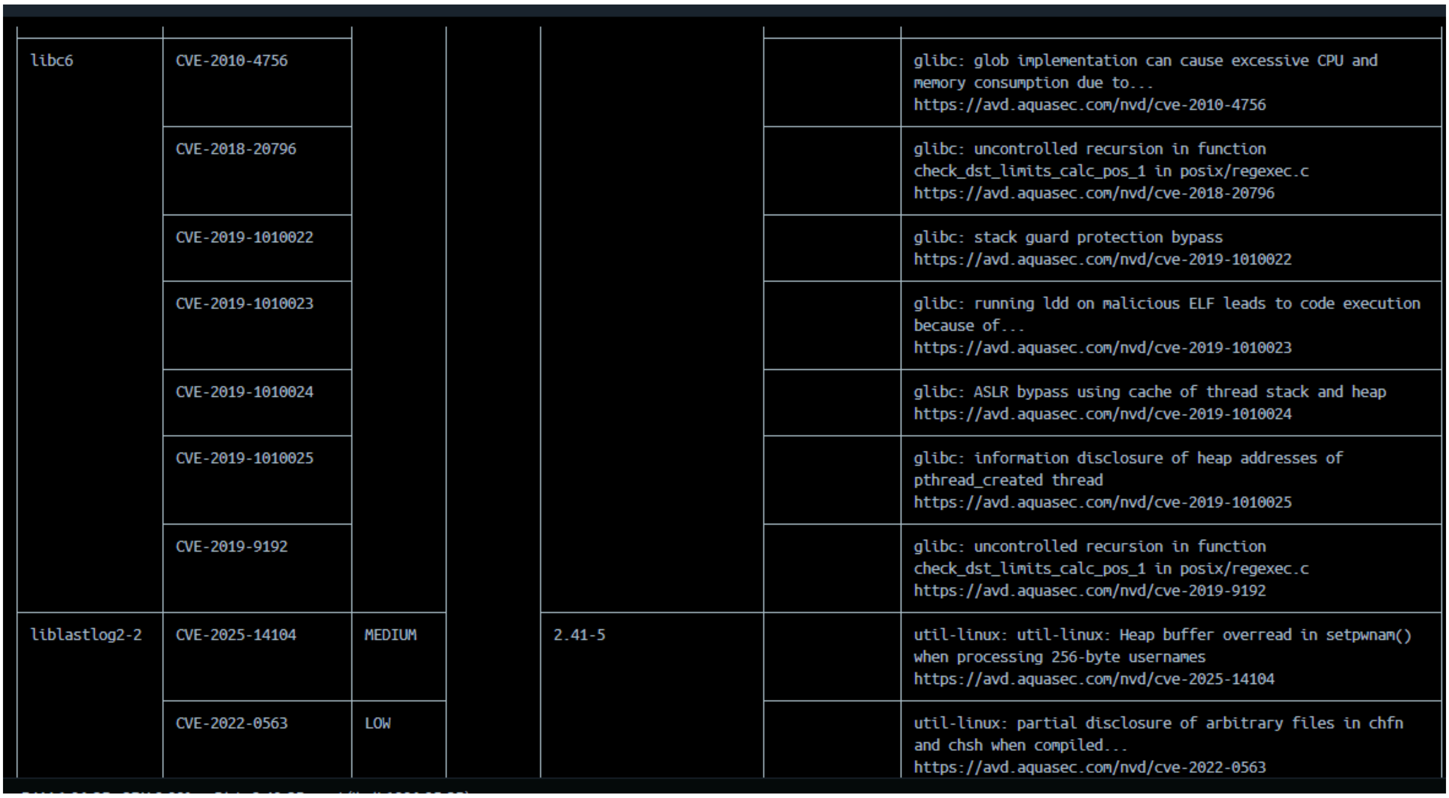
```
│ coreutils     │ CVE-2017-18018   │        │  │ 9.7-3    │  │ coreutils: race condition vulnerability in chown and chgrp  │
│               │                  │        │  │          │  │ https://avd.aquasec.com/nvd/cve-2017-18018                  │
│               ├──────────────────┤        │  │          ├──┼─────────────────────────────────────────────────────────────┤
│               │ CVE-2025-5278    │        │  │          │  │ coreutils: Heap Buffer Under-Read in GNU Coreutils sort via │
│               │                  │        │  │          │  │ Key Specification                                           │
│               │                  │        │  │          │  │ https://avd.aquasec.com/nvd/cve-2025-5278                   │
├───────────────┼──────────────────┤        │  ├──────────┼──┼─────────────────────────────────────────────────────────────┤
│ libapt-pkg7.0 │ CVE-2011-3374    │        │  │ 3.0.3    │  │ It was found that apt-key in apt, all versions, do not      │
│               │                  │        │  │          │  │ correctly...                                                │
│               │                  │        │  │          │  │ https://avd.aquasec.com/nvd/cve-2011-3374                   │
├───────────────┼──────────────────┼────────┤  ├──────────┼──┼─────────────────────────────────────────────────────────────┤
│ libblkid1     │ CVE-2025-14104   │ MEDIUM │  │ 2.41-5   │  │ util-linux: util-linux: Heap buffer overread in setpwnam()  │
│               │                  │        │  │          │  │ when processing 256-byte usernames                          │
│               │                  │        │  │          │  │ https://avd.aquasec.com/nvd/cve-2025-14104                  │
│               ├──────────────────┼────────┤  │          ├──┼─────────────────────────────────────────────────────────────┤
│               │ CVE-2022-0563    │ LOW    │  │          │  │ util-linux: partial disclosure of arbitrary files in chfn   │
│               │                  │        │  │          │  │ and chsh when compiled...                                   │
│               │                  │        │  │          │  │ https://avd.aquasec.com/nvd/cve-2022-0563                   │
├───────────────┼──────────────────┤        │  ├──────────┼──┼─────────────────────────────────────────────────────────────┤
│ libc-bin      │ CVE-2010-4756    │        │  │ 2.41-12  │  │ 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                │
```

RAM 1.06 GB CPU 0.17% Disk: 2.49 GB used (limit 1006.85 GB)

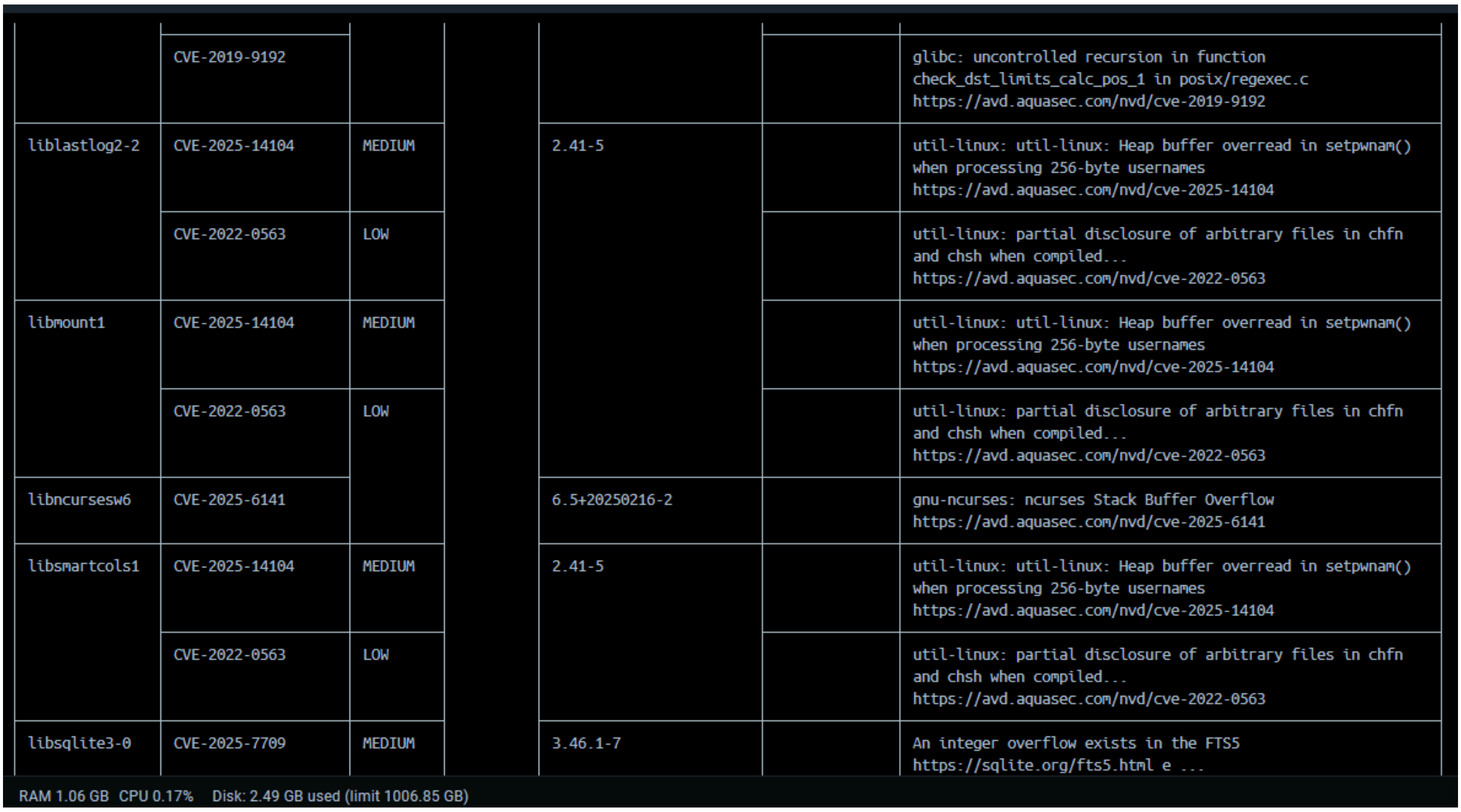


```
│               │                  │        │  │          │  │ and chsh when compiled...                                   │
│               │                  │        │  │          │  │ https://avd.aquasec.com/nvd/cve-2022-0563                   │
├───────────────┼──────────────────┤        │  ├──────────┼──┼─────────────────────────────────────────────────────────────┤
│ libc-bin      │ CVE-2010-4756    │        │  │ 2.41-12  │  │ 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-2010-4756    │        │  │          │  │ 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                   │
```

RAM 1.06 GB CPU 0.42% Disk: 2.49 GB used (limit 1006.85 GB)

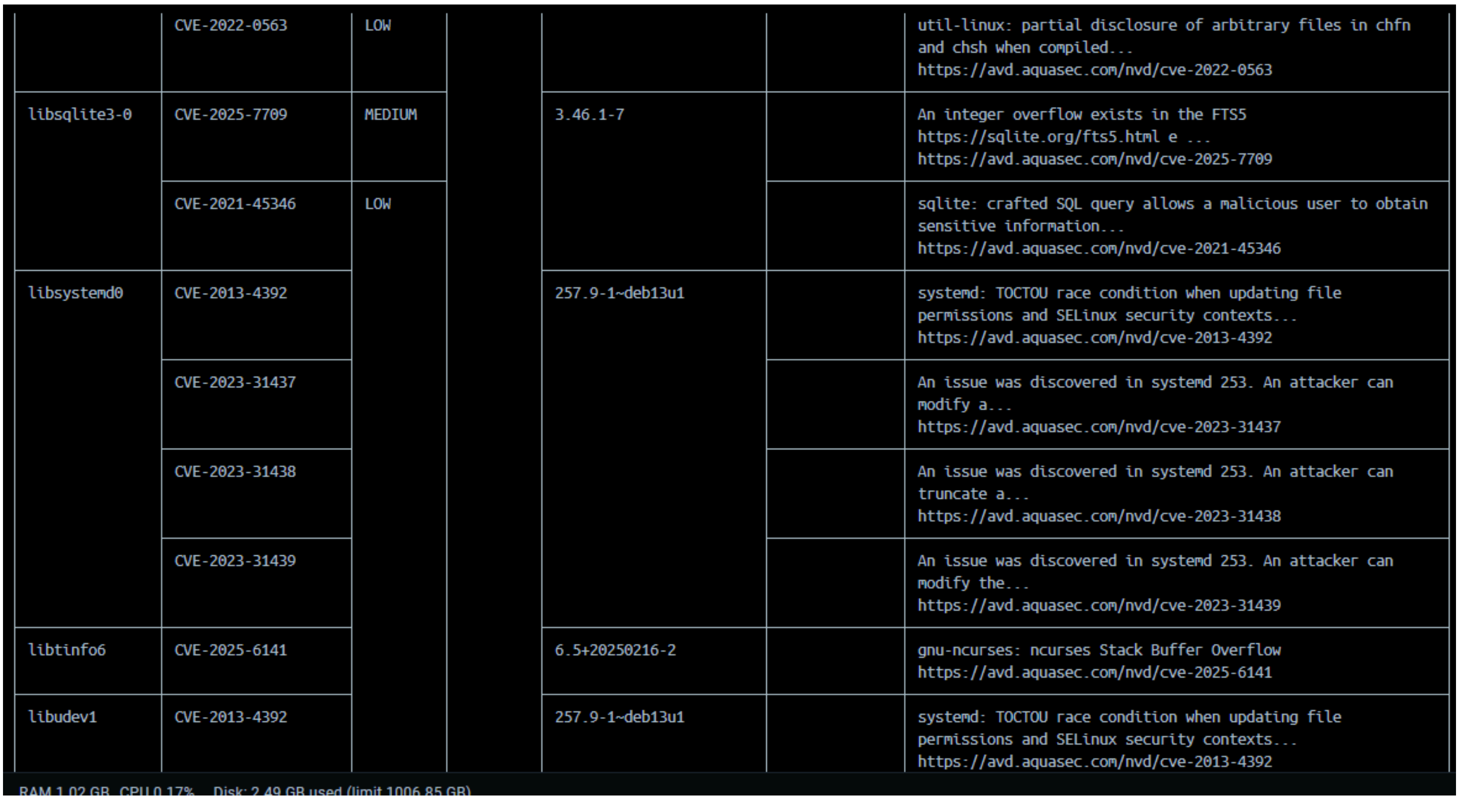


```
│ libc6         │ CVE-2010-4756    │        │ │                │ │ glibc: glob implementation can cause excessive CPU and      │
│               │                  │        │ │                │ │ memory consumption due to...                                │
│               │                  │        │ │                │ │ 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                   │
├───────────────┼──────────────────┼────────┤ ├────────────────┼─┼─────────────────────────────────────────────────────────────┤
│ liblastlog2-2 │ CVE-2025-14104   │ MEDIUM │ │ 2.41-5         │ │ util-linux: util-linux: Heap buffer overread in setpwnam()  │
│               │                  │        │ │                │ │ when processing 256-byte usernames                          │
│               │                  │        │ │                │ │ https://avd.aquasec.com/nvd/cve-2025-14104                  │
│               ├──────────────────┼────────┤ │                ├─┼─────────────────────────────────────────────────────────────┤
│               │ CVE-2022-0563    │ LOW    │ │                │ │ util-linux: partial disclosure of arbitrary files in chfn   │
│               │                  │        │ │                │ │ and chsh when compiled...                                   │
│               │                  │        │ │                │ │ https://avd.aquasec.com/nvd/cve-2022-0563                   │
```



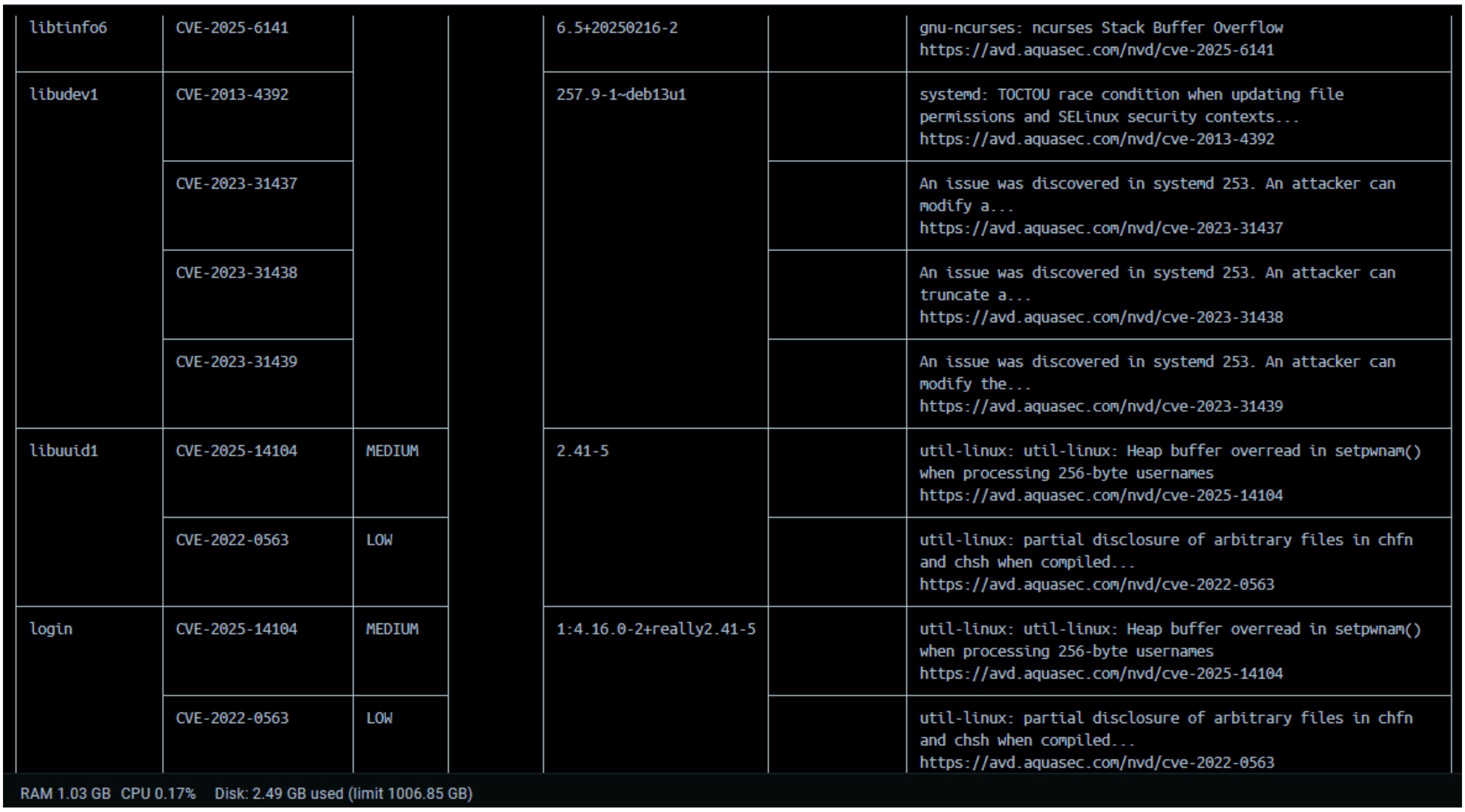
```
│               │ CVE-2019-9192    │        │ │                │ │ glibc: uncontrolled recursion in function                   │
│               │                  │        │ │                │ │ check_dst_limits_calc_pos_1 in posix/regexec.c              │
│               │                  │        │ │                │ │ https://avd.aquasec.com/nvd/cve-2019-9192                   │
├───────────────┼──────────────────┼────────┤ ├────────────────┼─┼─────────────────────────────────────────────────────────────┤
│ liblastlog2-2 │ CVE-2025-14104   │ MEDIUM │ │ 2.41-5         │ │ util-linux: util-linux: Heap buffer overread in setpwnam()  │
│               │                  │        │ │                │ │ when processing 256-byte usernames                          │
│               │                  │        │ │                │ │ https://avd.aquasec.com/nvd/cve-2025-14104                  │
│               ├──────────────────┼────────┤ │                ├─┼─────────────────────────────────────────────────────────────┤
│               │ CVE-2022-0563    │ LOW    │ │                │ │ util-linux: partial disclosure of arbitrary files in chfn   │
│               │                  │        │ │                │ │ and chsh when compiled...                                   │
│               │                  │        │ │                │ │ https://avd.aquasec.com/nvd/cve-2022-0563                   │
├───────────────┼──────────────────┼────────┤ │                ├─┼─────────────────────────────────────────────────────────────┤
│ libmount1     │ CVE-2025-14104   │ MEDIUM │ │                │ │ util-linux: util-linux: Heap buffer overread in setpwnam()  │
│               │                  │        │ │                │ │ when processing 256-byte usernames                          │
│               │                  │        │ │                │ │ https://avd.aquasec.com/nvd/cve-2025-14104                  │
│               ├──────────────────┼────────┤ │                ├─┼─────────────────────────────────────────────────────────────┤
│               │ CVE-2022-0563    │ LOW    │ │                │ │ util-linux: partial disclosure of arbitrary files in chfn   │
│               │                  │        │ │                │ │ and chsh when compiled...                                   │
│               │                  │        │ │                │ │ https://avd.aquasec.com/nvd/cve-2022-0563                   │
├───────────────┼──────────────────┤        │ ├────────────────┼─┼─────────────────────────────────────────────────────────────┤
│ libncursesw6  │ CVE-2025-6141    │        │ │ 6.5+20250216-2 │ │ gnu-ncurses: ncurses Stack Buffer Overflow                  │
│               │                  │        │ │                │ │ https://avd.aquasec.com/nvd/cve-2025-6141                   │
├───────────────┼──────────────────┼────────┤ ├────────────────┼─┼─────────────────────────────────────────────────────────────┤
│ libsmartcols1 │ CVE-2025-14104   │ MEDIUM │ │ 2.41-5         │ │ util-linux: util-linux: Heap buffer overread in setpwnam()  │
│               │                  │        │ │                │ │ when processing 256-byte usernames                          │
│               │                  │        │ │                │ │ https://avd.aquasec.com/nvd/cve-2025-14104                  │
│               ├──────────────────┼────────┤ │                ├─┼─────────────────────────────────────────────────────────────┤
│               │ CVE-2022-0563    │ LOW    │ │                │ │ util-linux: partial disclosure of arbitrary files in chfn   │
│               │                  │        │ │                │ │ and chsh when compiled...                                   │
│               │                  │        │ │                │ │ https://avd.aquasec.com/nvd/cve-2022-0563                   │
├───────────────┼──────────────────┼────────┤ ├────────────────┼─┼─────────────────────────────────────────────────────────────┤
│ libsqlite3-0  │ CVE-2025-7709    │ MEDIUM │ │ 3.46.1-7       │ │ An integer overflow exists in the FTS5                      │
│               │                  │        │ │                │ │ https://sqlite.org/fts5.html e ...                          │
```

RAM 1.06 GB CPU 0.17% Disk: 2.49 GB used (limit 1006.85 GB)



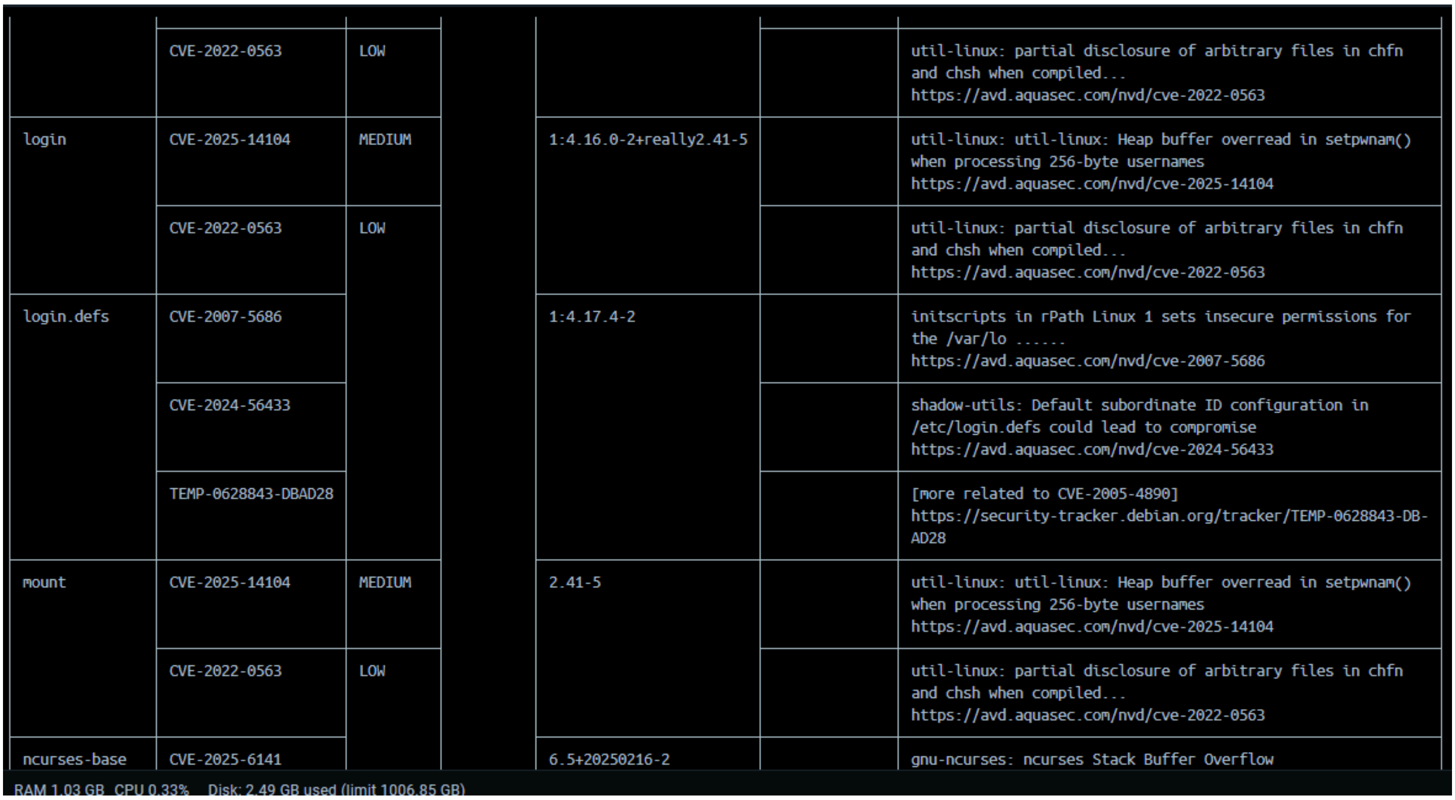
```
│            │ CVE-2022-0563  │ LOW    │ │                 │ │ util-linux: partial disclosure of arbitrary files in chfn
│            │                │        │ │                 │ │ and chsh when compiled...
│            │                │        │ │                 │ │ https://avd.aquasec.com/nvd/cve-2022-0563
├────────────┼────────────────┼────────┤ ├─────────────────┤ ├──────────────────────────────────────────────────────────
│ libsqlite3-0 │ CVE-2025-7709 │ MEDIUM │ │ 3.46.1-7        │ │ An integer overflow exists in the FTS5
│            │                │        │ │                 │ │ https://sqlite.org/fts5.html e ...
│            │                │        │ │                 │ │ https://avd.aquasec.com/nvd/cve-2025-7709
│            ├────────────────┼────────┤ │                 ├─┼──────────────────────────────────────────────────────────
│            │ CVE-2021-45346 │ LOW    │ │                 │ │ sqlite: crafted SQL query allows a malicious user to obtain
│            │                │        │ │                 │ │ sensitive information...
│            │                │        │ │                 │ │ https://avd.aquasec.com/nvd/cve-2021-45346
├────────────┼────────────────┤        │ ├─────────────────┤ ├──────────────────────────────────────────────────────────
│ libsystemd0 │ CVE-2013-4392 │        │ │ 257.9-1~deb13u1 │ │ 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
├────────────┼────────────────┤        │ ├─────────────────┤ ├──────────────────────────────────────────────────────────
│ libtinfo6  │ CVE-2025-6141  │        │ │ 6.5+20250216-2  │ │ gnu-ncurses: ncurses Stack Buffer Overflow
│            │                │        │ │                 │ │ https://avd.aquasec.com/nvd/cve-2025-6141
├────────────┼────────────────┤        │ ├─────────────────┤ ├──────────────────────────────────────────────────────────
│ libudev1   │ CVE-2013-4392  │        │ │ 257.9-1~deb13u1 │ │ systemd: TOCTOU race condition when updating file
│            │                │        │ │                 │ │ permissions and SELinux security contexts...
│            │                │        │ │                 │ │ https://avd.aquasec.com/nvd/cve-2013-4392
```

RAM 1.02 GB CPU 0.17% Disk: 2.49 GB used (limit 1006.85 GB)



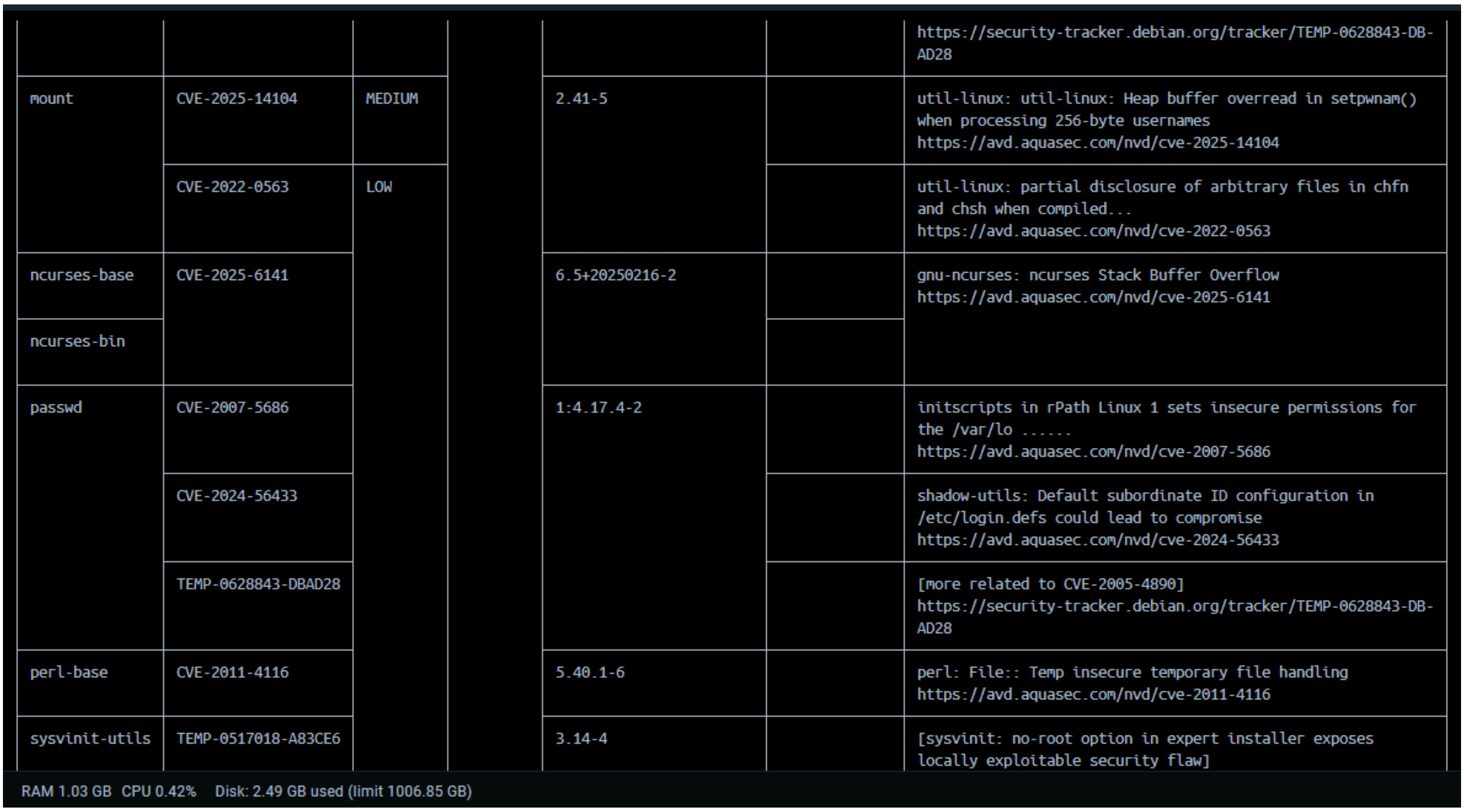
```
│ libtinfo6  │ CVE-2025-6141  │        │ │ 6.5+20250216-2  │ │ gnu-ncurses: ncurses Stack Buffer Overflow
│            │                │        │ │                 │ │ https://avd.aquasec.com/nvd/cve-2025-6141
├────────────┼────────────────┤        │ ├─────────────────┤ ├──────────────────────────────────────────────────────────
│ libudev1   │ CVE-2013-4392  │        │ │ 257.9-1~deb13u1 │ │ 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-2025-14104 │ MEDIUM │ │ 2.41-5          │ │ util-linux: util-linux: Heap buffer overread in setpwnam()
│            │                │        │ │                 │ │ when processing 256-byte usernames
│            │                │        │ │                 │ │ https://avd.aquasec.com/nvd/cve-2025-14104
│            ├────────────────┼────────┤ │                 ├─┼──────────────────────────────────────────────────────────
│            │ CVE-2022-0563  │ LOW    │ │                 │ │ util-linux: partial disclosure of arbitrary files in chfn
│            │                │        │ │                 │ │ and chsh when compiled...
│            │                │        │ │                 │ │ https://avd.aquasec.com/nvd/cve-2022-0563
├────────────┼────────────────┼────────┤ ├─────────────────┤ ├──────────────────────────────────────────────────────────
│ login      │ CVE-2025-14104 │ MEDIUM │ │ 1:4.16.0-2+really2.41-5 │ │ util-linux: util-linux: Heap buffer overread in setpwnam()
│            │                │        │ │                 │ │ when processing 256-byte usernames
│            │                │        │ │                 │ │ https://avd.aquasec.com/nvd/cve-2025-14104
│            ├────────────────┼────────┤ │                 ├─┼──────────────────────────────────────────────────────────
│            │ CVE-2022-0563  │ LOW    │ │                 │ │ util-linux: partial disclosure of arbitrary files in chfn
│            │                │        │ │                 │ │ and chsh when compiled...
│            │                │        │ │                 │ │ https://avd.aquasec.com/nvd/cve-2022-0563
```

RAM 1.03 GB CPU 0.17% Disk: 2.49 GB used (limit 1006.85 GB)



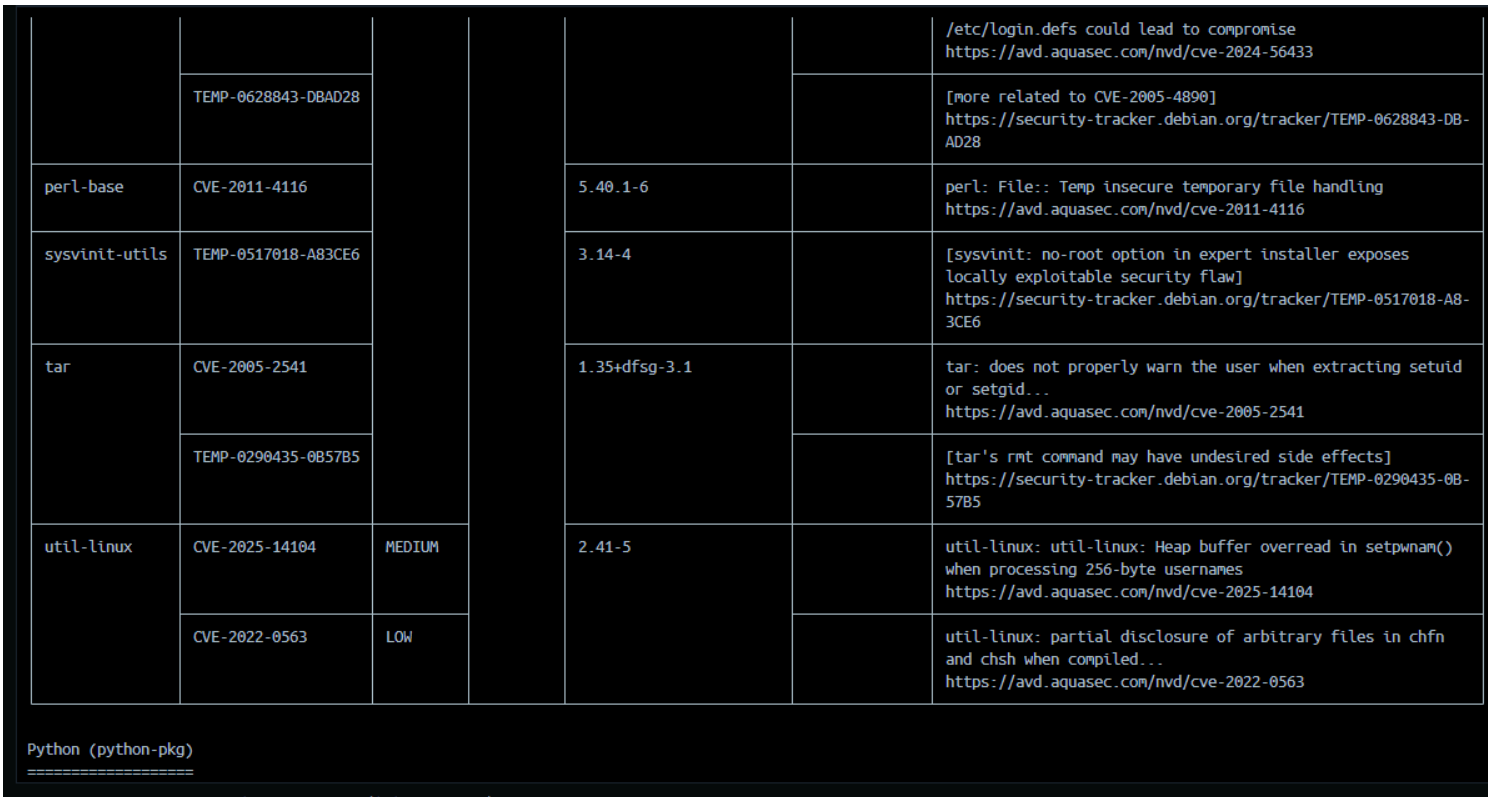
	CVE-2022-0563	LOW				util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled... https://avd.aquasec.com/nvd/cve-2022-0563
login	CVE-2025-14104	MEDIUM		1:4.16.0-2+really2.41-5		util-linux: util-linux: Heap buffer overread in setpwnam() when processing 256-byte usernames https://avd.aquasec.com/nvd/cve-2025-14104
	CVE-2022-0563	LOW				util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled... https://avd.aquasec.com/nvd/cve-2022-0563
login.defs	CVE-2007-5686			1:4.17.4-2		initscripts in rPath Linux 1 sets insecure permissions for the /var/lo https://avd.aquasec.com/nvd/cve-2007-5686
	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-2025-14104	MEDIUM		2.41-5		util-linux: util-linux: Heap buffer overread in setpwnam() when processing 256-byte usernames https://avd.aquasec.com/nvd/cve-2025-14104
	CVE-2022-0563	LOW				util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled... https://avd.aquasec.com/nvd/cve-2022-0563
ncurses-base	CVE-2025-6141			6.5+20250216-2		gnu-ncurses: ncurses Stack Buffer Overflow

RAM 1.03 GB CPU 0.33% Disk: 2.49 GB used (limit 1006.85 GB)

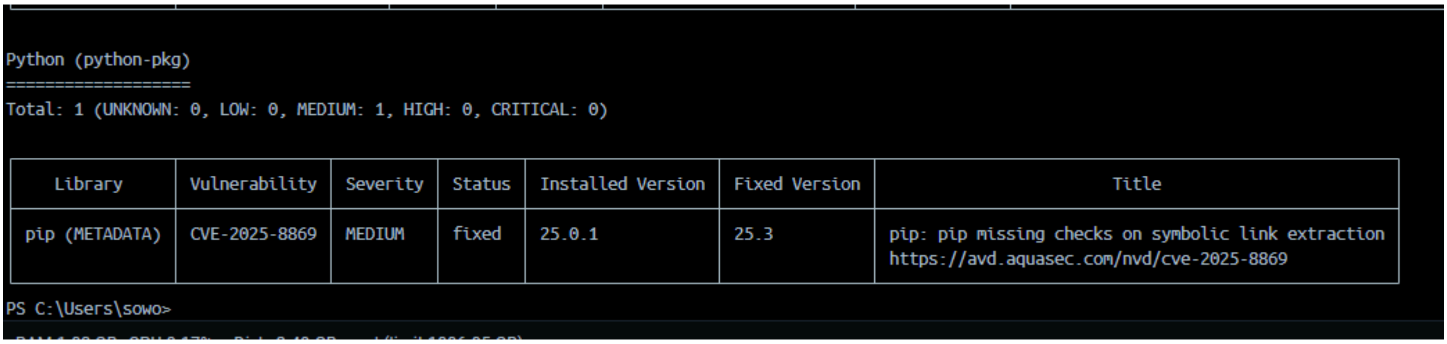


						https://security-tracker.debian.org/tracker/TEMP-0628843-DB-AD28
mount	CVE-2025-14104	MEDIUM		2.41-5		util-linux: util-linux: Heap buffer overread in setpwnam() when processing 256-byte usernames https://avd.aquasec.com/nvd/cve-2025-14104
	CVE-2022-0563	LOW				util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled... https://avd.aquasec.com/nvd/cve-2022-0563
ncurses-base	CVE-2025-6141			6.5+20250216-2		gnu-ncurses: ncurses Stack Buffer Overflow https://avd.aquasec.com/nvd/cve-2025-6141
ncurses-bin						
passwd	CVE-2007-5686			1:4.17.4-2		initscripts in rPath Linux 1 sets insecure permissions for the /var/lo https://avd.aquasec.com/nvd/cve-2007-5686
	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-2011-4116			5.40.1-6		perl: File:: Temp insecure temporary file handling https://avd.aquasec.com/nvd/cve-2011-4116
sysvinit-utils	TEMP-0517018-A83CE6			3.14-4		[sysvinit: no-root option in expert installer exposes locally exploitable security flaw]

RAM 1.03 GB CPU 0.42% Disk: 2.49 GB used (limit 1006.85 GB)



```
│               │                    │        │        │                      │              │ /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-2011-4116      │        │        │ 5.40.1-6             │              │ perl: File:: Temp insecure temporary file handling      │
│               │                    │        │        │                      │              │ https://avd.aquasec.com/nvd/cve-2011-4116               │
├───────────────┼────────────────────┤        │        ├──────────────────────┼──────────────┼─────────────────────────────────────────────────────────┤
│ sysvinit-utils│ TEMP-0517018-A83CE6│        │        │ 3.14-4               │              │ [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      │        │        │ 1.35+dfsg-3.1        │              │ 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-2025-14104     │ MEDIUM │        │ 2.41-5               │              │ util-linux: util-linux: Heap buffer overread in setpwnam() │
│               │                    │        │        │                      │              │ when processing 256-byte usernames                      │
│               │                    │        │        │                      │              │ https://avd.aquasec.com/nvd/cve-2025-14104              │
│               ├────────────────────┼────────┤        │                      ├──────────────┼─────────────────────────────────────────────────────────┤
│               │ CVE-2022-0563      │ LOW    │        │                      │              │ util-linux: partial disclosure of arbitrary files in chfn │
│               │                    │        │        │                      │              │ and chsh when compiled...                               │
│               │                    │        │        │                      │              │ https://avd.aquasec.com/nvd/cve-2022-0563               │
└───────────────┴────────────────────┴────────┴────────┴──────────────────────┴──────────────┴─────────────────────────────────────────────────────────┘

Python (python-pkg)
===================
```

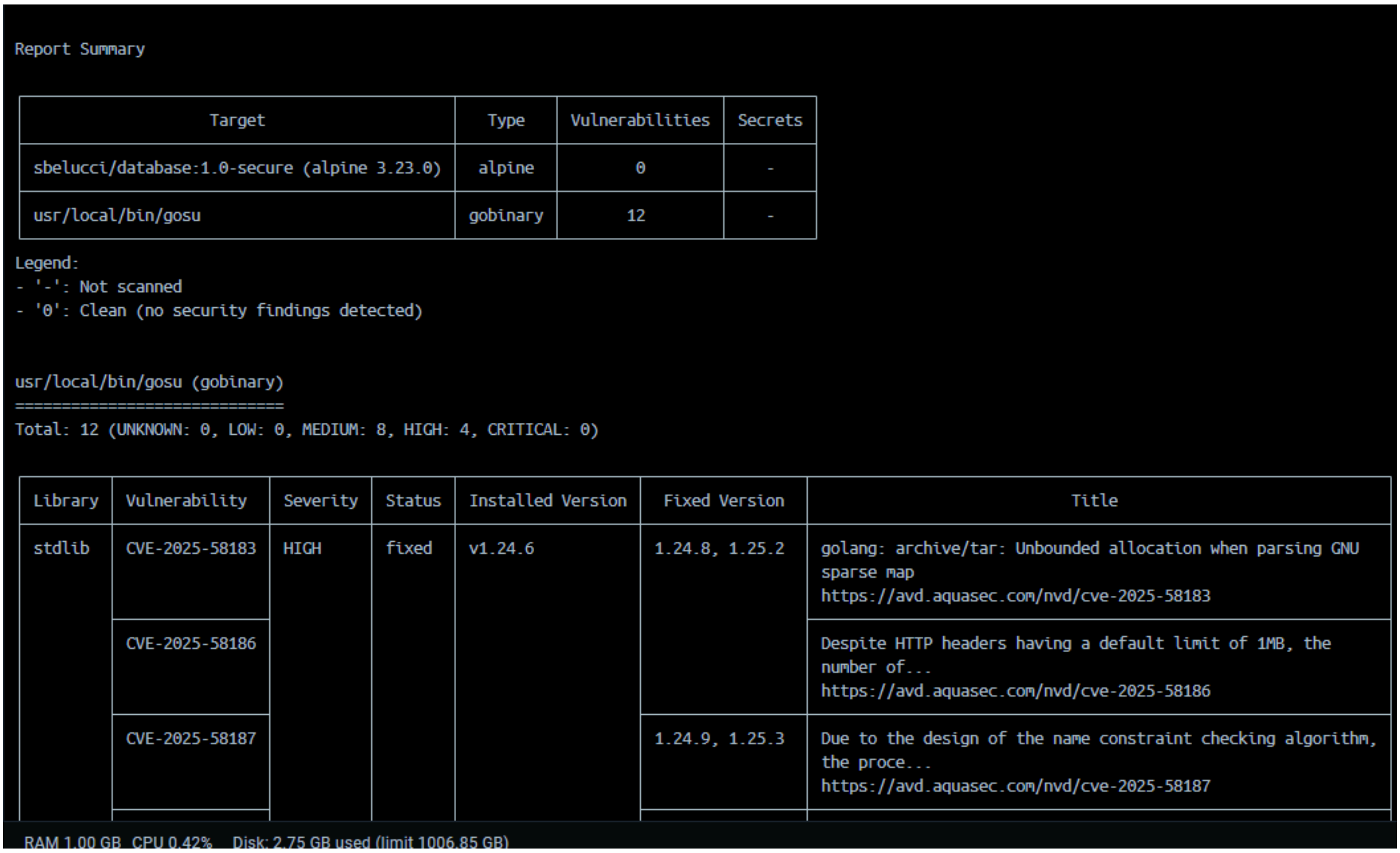


```
Python (python-pkg)
===================
Total: 1 (UNKNOWN: 0, LOW: 0, MEDIUM: 1, HIGH: 0, CRITICAL: 0)

┌──────────────┬───────────────┬──────────┬────────┬───────────────────┬───────────────┬──────────────────────────────────────────────┐
│   Library    │ Vulnerability │ Severity │ Status │ Installed Version │ Fixed Version │                    Title                     │
├──────────────┼───────────────┼──────────┼────────┼───────────────────┼───────────────┼──────────────────────────────────────────────┤
│ pip (METADATA)│ CVE-2025-8869 │ MEDIUM   │ fixed  │ 25.0.1            │ 25.3          │ pip: pip missing checks on symbolic link extraction │
│              │               │          │        │                   │               │ https://avd.aquasec.com/nvd/cve-2025-8869    │
└──────────────┴───────────────┴──────────┴────────┴───────────────────┴───────────────┴──────────────────────────────────────────────┘
PS C:\Users\sowo>
```

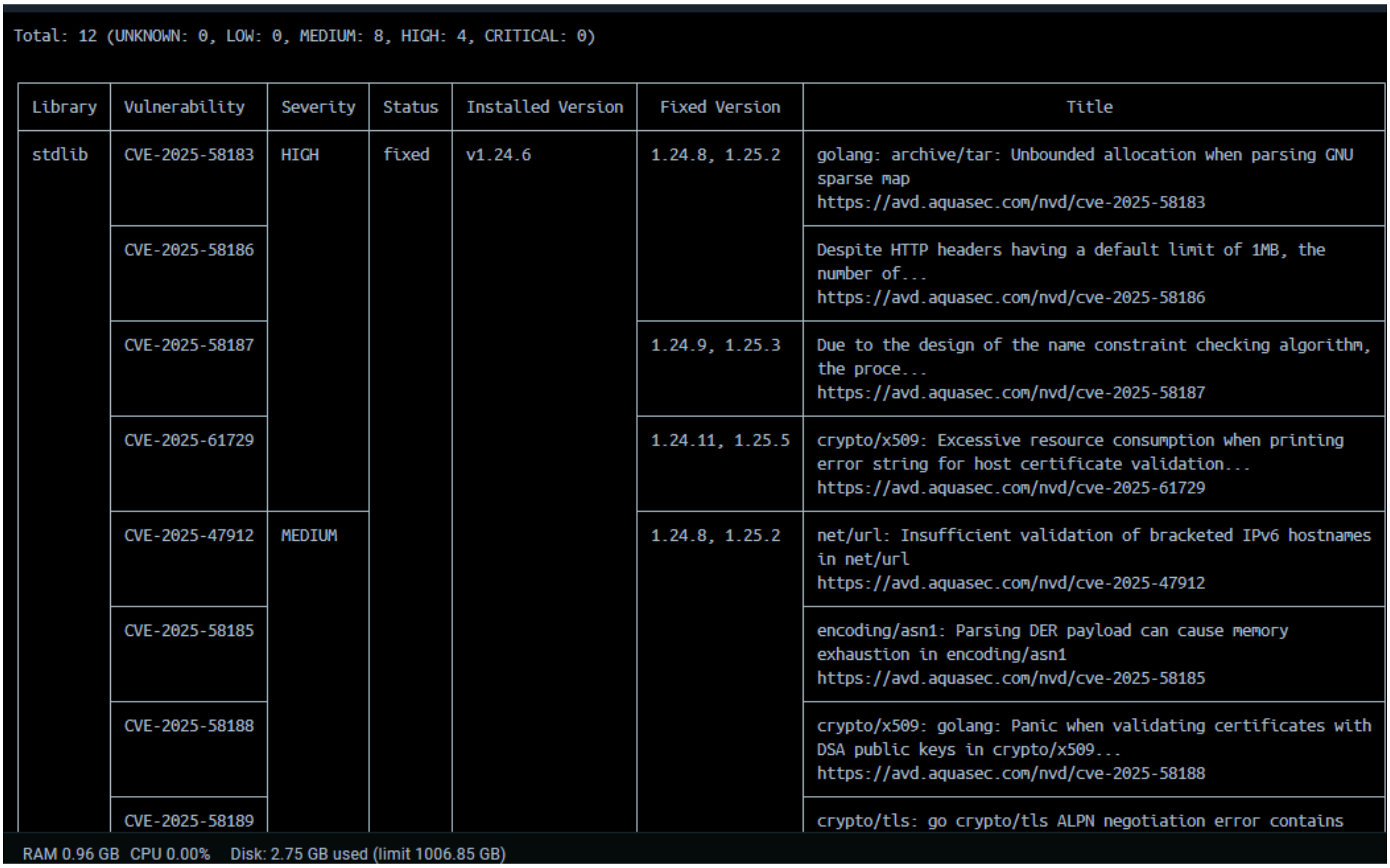
3) Resultado del reporte de la image sbelucci/database:1.0-secure

docker run --rm -v /var/run/docker.sock:/var/run/docker.sock aquasec/trivy:latest image sbelucci/database:1.0-secure

Aclaración: Si bien figura HIGH, el status es ‘fixed’ ya que el Dockerfile usa postgres:16-alpine. Esta imagen base ya viene con librerías actualizadas que incluyen correcciones de seguridad. Se actualizó la versión de la librería en el Dockerfile y ya estaría arreglada la vulnerabilidad.

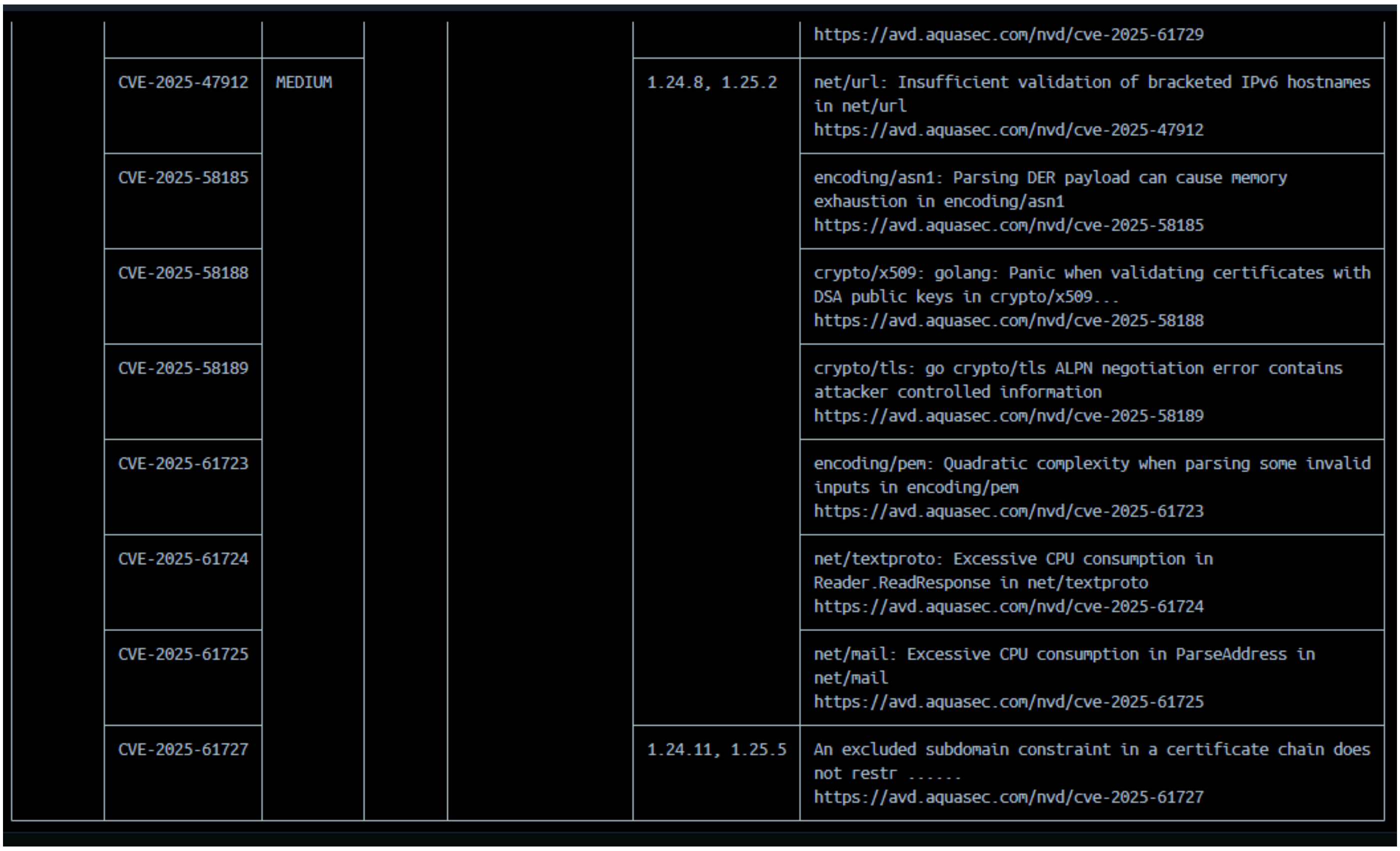


```
Report Summary

┌──────────────────────────────────────────────┬───────────┬─────────────────┬─────────┐
│                    Target                    │   Type    │ Vulnerabilities │ Secrets │
├──────────────────────────────────────────────┼───────────┼─────────────────┼─────────┤
│ sbelucci/database:1.0-secure (alpine 3.23.0) │  alpine   │        0        │    -    │
├──────────────────────────────────────────────┼───────────┼─────────────────┼─────────┤
│ usr/local/bin/gosu                           │ gobinary  │       12        │    -    │
└──────────────────────────────────────────────┴───────────┴─────────────────┴─────────┘
Legend:
- '-': Not scanned
- '0': Clean (no security findings detected)


usr/local/bin/gosu (gobinary)
=============================
Total: 12 (UNKNOWN: 0, LOW: 0, MEDIUM: 8, HIGH: 4, CRITICAL: 0)

┌─────────┬────────────────┬──────────┬────────┬───────────────────┬──────────────────┬──────────────────────────────────────────────────────────────┐
│ Library │ Vulnerability  │ Severity │ Status │ Installed Version │  Fixed Version   │                            Title                             │
├─────────┼────────────────┼──────────┼────────┼───────────────────┼──────────────────┼──────────────────────────────────────────────────────────────┤
│ stdlib  │ CVE-2025-58183 │ HIGH     │ fixed  │ v1.24.6           │ 1.24.8, 1.25.2   │ golang: archive/tar: Unbounded allocation when parsing GNU   │
│         │                │          │        │                   │                  │ sparse map                                                   │
│         │                │          │        │                   │                  │ https://avd.aquasec.com/nvd/cve-2025-58183                   │
│         ├────────────────┤          │        │                   │                  ├──────────────────────────────────────────────────────────────┤
│         │ CVE-2025-58186 │          │        │                   │                  │ Despite HTTP headers having a default limit of 1MB, the      │
│         │                │          │        │                   │                  │ number of...                                                 │
│         │                │          │        │                   │                  │ https://avd.aquasec.com/nvd/cve-2025-58186                   │
│         ├────────────────┤          │        │                   ├──────────────────┼──────────────────────────────────────────────────────────────┤
│         │ CVE-2025-58187 │          │        │                   │ 1.24.9, 1.25.3   │ Due to the design of the name constraint checking algorithm, │
│         │                │          │        │                   │                  │ the proce...                                                 │
│         │                │          │        │                   │                  │ https://avd.aquasec.com/nvd/cve-2025-58187                   │
│         ├────────────────┤          │        │                   ├──────────────────┼──────────────────────────────────────────────────────────────┤
RAM 1.00 GB  CPU 0.42%   Disk: 2.75 GB used (limit 1006.85 GB)
```



```
Total: 12 (UNKNOWN: 0, LOW: 0, MEDIUM: 8, HIGH: 4, CRITICAL: 0)

┌─────────┬────────────────┬──────────┬────────┬───────────────────┬─────────────────┬───────────────────────────────────────────────────────────────┐
│ Library │ Vulnerability  │ Severity │ Status │ Installed Version │  Fixed Version  │                             Title                             │
├─────────┼────────────────┼──────────┼────────┼───────────────────┼─────────────────┼───────────────────────────────────────────────────────────────┤
│ stdlib  │ CVE-2025-58183 │ HIGH     │ fixed  │ v1.24.6           │ 1.24.8, 1.25.2  │ golang: archive/tar: Unbounded allocation when parsing GNU    │
│         │                │          │        │                   │                 │ sparse map                                                    │
│         │                │          │        │                   │                 │ https://avd.aquasec.com/nvd/cve-2025-58183                    │
│         ├────────────────┤          │        │                   │                 ├───────────────────────────────────────────────────────────────┤
│         │ CVE-2025-58186 │          │        │                   │                 │ Despite HTTP headers having a default limit of 1MB, the       │
│         │                │          │        │                   │                 │ number of...                                                  │
│         │                │          │        │                   │                 │ https://avd.aquasec.com/nvd/cve-2025-58186                    │
│         ├────────────────┤          │        │                   ├─────────────────┼───────────────────────────────────────────────────────────────┤
│         │ CVE-2025-58187 │          │        │                   │ 1.24.9, 1.25.3  │ Due to the design of the name constraint checking algorithm,  │
│         │                │          │        │                   │                 │ the proce...                                                  │
│         │                │          │        │                   │                 │ https://avd.aquasec.com/nvd/cve-2025-58187                    │
│         ├────────────────┤          │        │                   ├─────────────────┼───────────────────────────────────────────────────────────────┤
│         │ CVE-2025-61729 │          │        │                   │ 1.24.11, 1.25.5 │ crypto/x509: Excessive resource consumption when printing     │
│         │                │          │        │                   │                 │ error string for host certificate validation...               │
│         │                │          │        │                   │                 │ https://avd.aquasec.com/nvd/cve-2025-61729                    │
│         ├────────────────┼──────────┤        │                   ├─────────────────┼───────────────────────────────────────────────────────────────┤
│         │ CVE-2025-47912 │ MEDIUM   │        │                   │ 1.24.8, 1.25.2  │ net/url: Insufficient validation of bracketed IPv6 hostnames  │
│         │                │          │        │                   │                 │ in net/url                                                    │
│         │                │          │        │                   │                 │ https://avd.aquasec.com/nvd/cve-2025-47912                    │
│         ├────────────────┤          │        │                   │                 ├───────────────────────────────────────────────────────────────┤
│         │ CVE-2025-58185 │          │        │                   │                 │ encoding/asn1: Parsing DER payload can cause memory           │
│         │                │          │        │                   │                 │ exhaustion in encoding/asn1                                   │
│         │                │          │        │                   │                 │ https://avd.aquasec.com/nvd/cve-2025-58185                    │
│         ├────────────────┤          │        │                   │                 ├───────────────────────────────────────────────────────────────┤
│         │ CVE-2025-58188 │          │        │                   │                 │ crypto/x509: golang: Panic when validating certificates with  │
│         │                │          │        │                   │                 │ DSA public keys in crypto/x509...                             │
│         │                │          │        │                   │                 │ https://avd.aquasec.com/nvd/cve-2025-58188                    │
│         ├────────────────┤          │        │                   │                 ├───────────────────────────────────────────────────────────────┤
│         │ CVE-2025-58189 │          │        │                   │                 │ crypto/tls: go crypto/tls ALPN negotiation error contains     │
```

RAM 0.96 GB CPU 0.00% Disk: 2.75 GB used (limit 1006.85 GB)



```
│         │                │          │        │                   │                 │ https://avd.aquasec.com/nvd/cve-2025-61729                    │
│         ├────────────────┼──────────┤        │                   ├─────────────────┼───────────────────────────────────────────────────────────────┤
│         │ CVE-2025-47912 │ MEDIUM   │        │                   │ 1.24.8, 1.25.2  │ net/url: Insufficient validation of bracketed IPv6 hostnames  │
│         │                │          │        │                   │                 │ in net/url                                                    │
│         │                │          │        │                   │                 │ https://avd.aquasec.com/nvd/cve-2025-47912                    │
│         ├────────────────┤          │        │                   │                 ├───────────────────────────────────────────────────────────────┤
│         │ CVE-2025-58185 │          │        │                   │                 │ encoding/asn1: Parsing DER payload can cause memory           │
│         │                │          │        │                   │                 │ exhaustion in encoding/asn1                                   │
│         │                │          │        │                   │                 │ https://avd.aquasec.com/nvd/cve-2025-58185                    │
│         ├────────────────┤          │        │                   │                 ├───────────────────────────────────────────────────────────────┤
│         │ CVE-2025-58188 │          │        │                   │                 │ crypto/x509: golang: Panic when validating certificates with  │
│         │                │          │        │                   │                 │ DSA public keys in crypto/x509...                             │
│         │                │          │        │                   │                 │ https://avd.aquasec.com/nvd/cve-2025-58188                    │
│         ├────────────────┤          │        │                   │                 ├───────────────────────────────────────────────────────────────┤
│         │ CVE-2025-58189 │          │        │                   │                 │ crypto/tls: go crypto/tls ALPN negotiation error contains     │
│         │                │          │        │                   │                 │ attacker controlled information                               │
│         │                │          │        │                   │                 │ https://avd.aquasec.com/nvd/cve-2025-58189                    │
│         ├────────────────┤          │        │                   │                 ├───────────────────────────────────────────────────────────────┤
│         │ CVE-2025-61723 │          │        │                   │                 │ encoding/pem: Quadratic complexity when parsing some invalid  │
│         │                │          │        │                   │                 │ inputs in encoding/pem                                        │
│         │                │          │        │                   │                 │ https://avd.aquasec.com/nvd/cve-2025-61723                    │
│         ├────────────────┤          │        │                   │                 ├───────────────────────────────────────────────────────────────┤
│         │ CVE-2025-61724 │          │        │                   │                 │ net/textproto: Excessive CPU consumption in                   │
│         │                │          │        │                   │                 │ Reader.ReadResponse in net/textproto                          │
│         │                │          │        │                   │                 │ https://avd.aquasec.com/nvd/cve-2025-61724                    │
│         ├────────────────┤          │        │                   │                 ├───────────────────────────────────────────────────────────────┤
│         │ CVE-2025-61725 │          │        │                   │                 │ net/mail: Excessive CPU consumption in ParseAddress in        │
│         │                │          │        │                   │                 │ net/mail                                                      │
│         │                │          │        │                   │                 │ https://avd.aquasec.com/nvd/cve-2025-61725                    │
│         ├────────────────┤          │        │                   ├─────────────────┼───────────────────────────────────────────────────────────────┤
│         │ CVE-2025-61727 │          │        │                   │ 1.24.11, 1.25.5 │ An excluded subdomain constraint in a certificate chain does  │
│         │                │          │        │                   │                 │ not restr ......                                              │
│         │                │          │        │                   │                 │ https://avd.aquasec.com/nvd/cve-2025-61727                    │
└─────────┴────────────────┴──────────┴────────┴───────────────────┴─────────────────┴───────────────────────────────────────────────────────────────┘
```