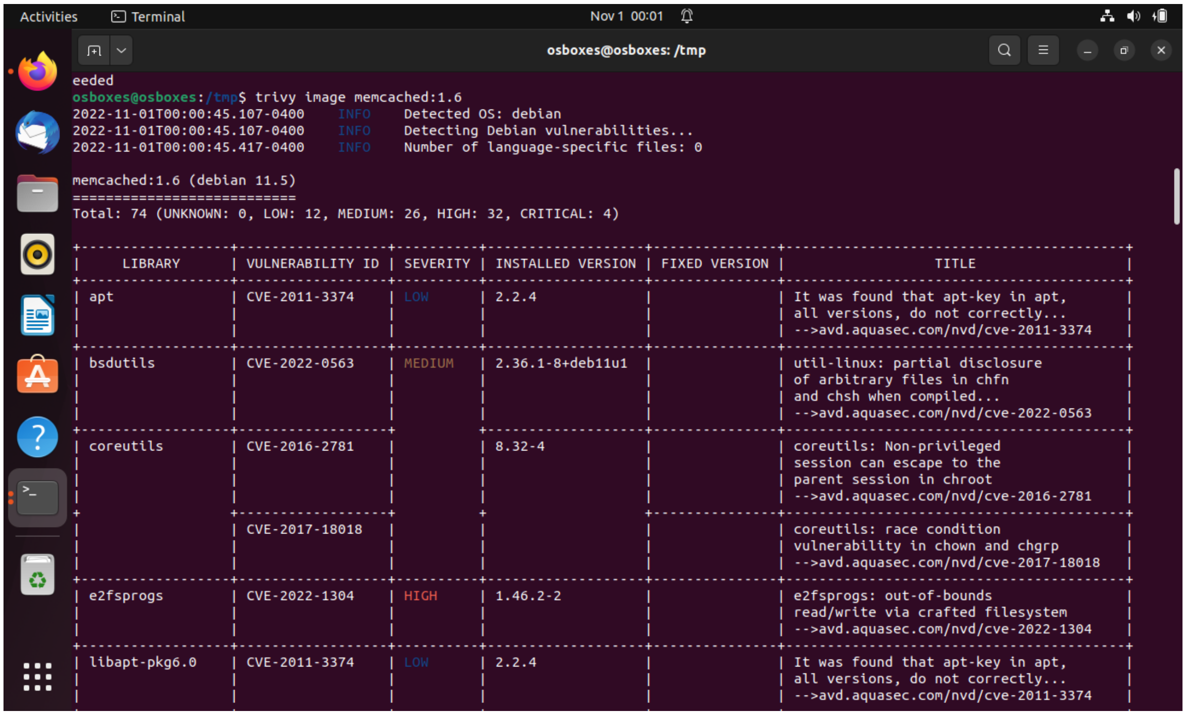
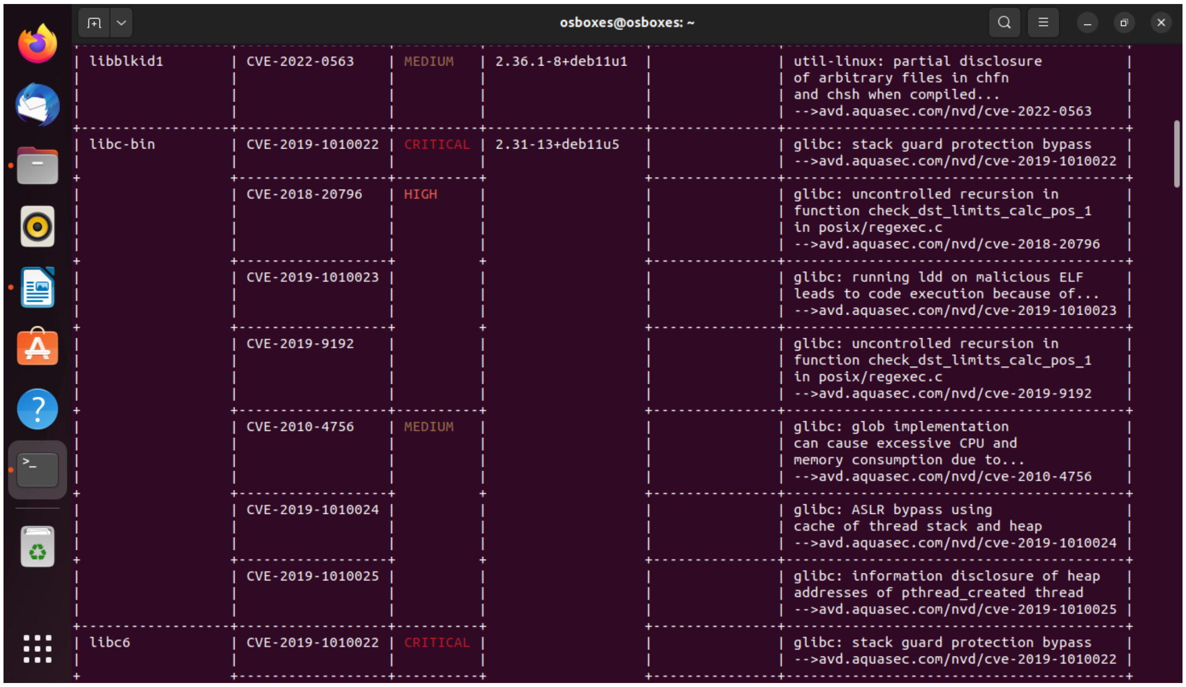
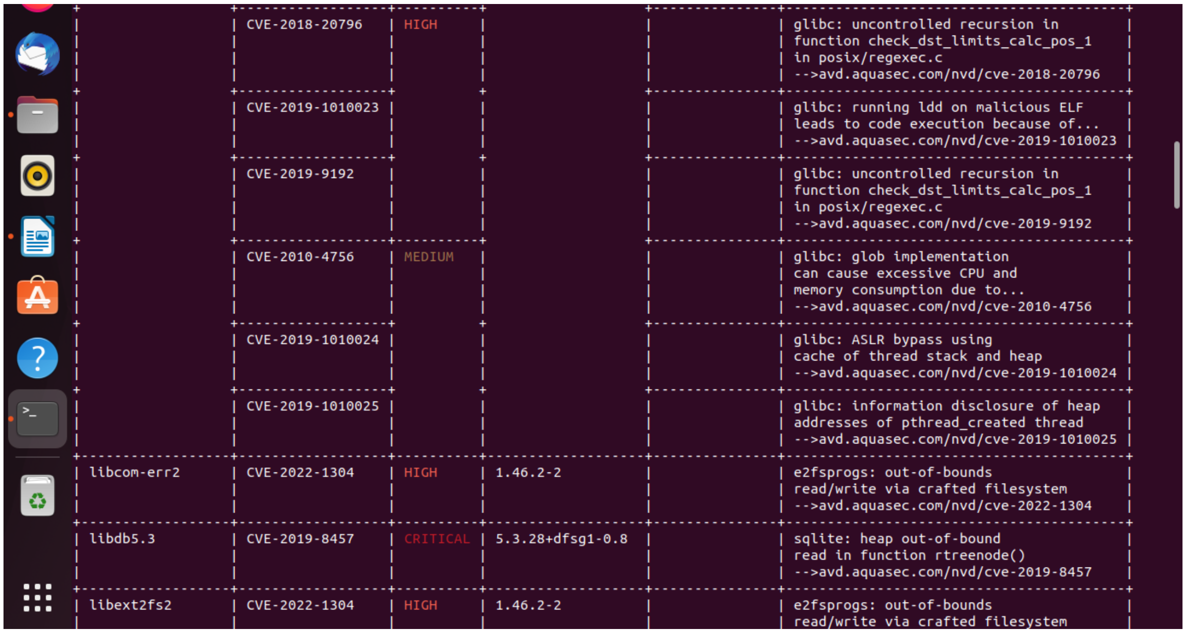
Memcached 1.6



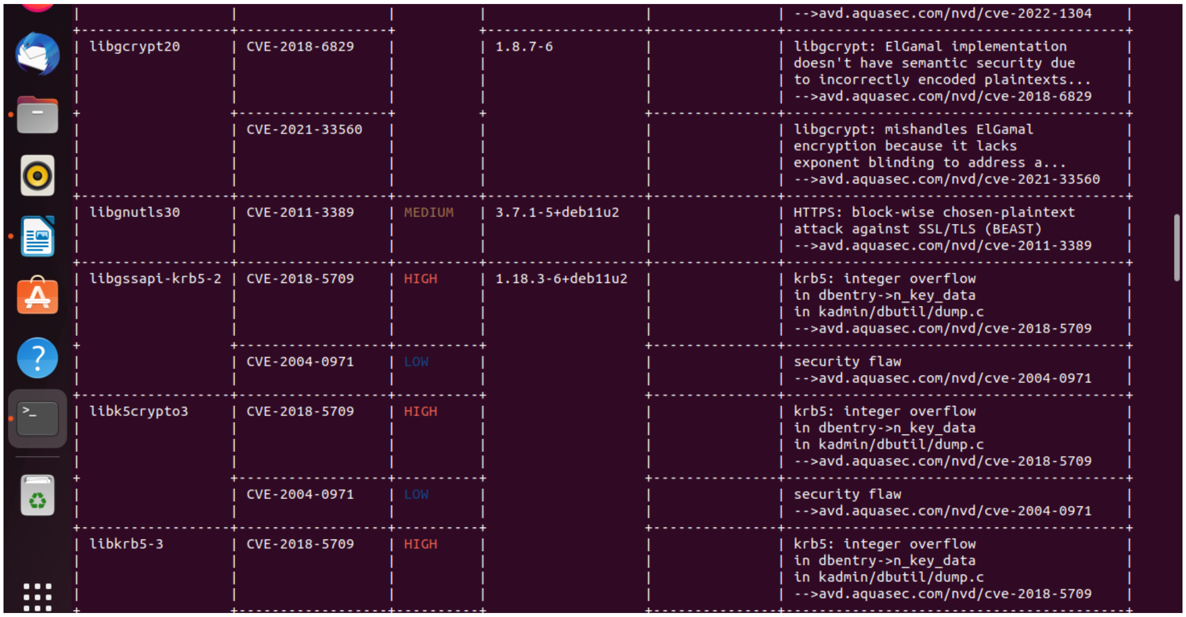
```
eeded
osboxes@osboxes:/tmp$ trivy image memcached:1.6
2022-11-01T00:00:45.107-0400    INFO    Detected OS: debian
2022-11-01T00:00:45.107-0400    INFO    Detecting Debian vulnerabilities...
2022-11-01T00:00:45.417-0400    INFO    Number of language-specific files: 0

memcached:1.6 (debian 11.5)
===========================
Total: 74 (UNKNOWN: 0, LOW: 12, MEDIUM: 26, HIGH: 32, CRITICAL: 4)

+------------------+------------------+----------+-------------------+---------------+-----------------------------------------+
|     LIBRARY      | VULNERABILITY ID | SEVERITY | INSTALLED VERSION | FIXED VERSION |                  TITLE                  |
+------------------+------------------+----------+-------------------+---------------+-----------------------------------------+
| apt              | CVE-2011-3374    | LOW      | 2.2.4             |               | It was found that apt-key in apt,       |
|                  |                  |          |                   |               | all versions, do not correctly...       |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2011-3374    |
+------------------+------------------+----------+-------------------+---------------+-----------------------------------------+
| bsdutils         | CVE-2022-0563    | MEDIUM   | 2.36.1-8+deb11u1  |               | util-linux: partial disclosure          |
|                  |                  |          |                   |               | of arbitrary files in chfn              |
|                  |                  |          |                   |               | and chsh when compiled...               |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2022-0563    |
+------------------+------------------+          +-------------------+---------------+-----------------------------------------+
| coreutils        | CVE-2016-2781    |          | 8.32-4            |               | coreutils: Non-privileged               |
|                  |                  |          |                   |               | session can escape to the               |
|                  |                  |          |                   |               | parent session in chroot                |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2016-2781    |
+                  +------------------+          +                   +---------------+-----------------------------------------+
|                  | CVE-2017-18018   |          |                   |               | coreutils: race condition               |
|                  |                  |          |                   |               | vulnerability in chown and chgrp        |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2017-18018   |
+------------------+------------------+----------+-------------------+---------------+-----------------------------------------+
| e2fsprogs        | CVE-2022-1304    | HIGH     | 1.46.2-2          |               | e2fsprogs: out-of-bounds                |
|                  |                  |          |                   |               | read/write via crafted filesystem       |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2022-1304    |
+------------------+------------------+----------+-------------------+---------------+-----------------------------------------+
| libapt-pkg6.0    | CVE-2011-3374    | LOW      | 2.2.4             |               | It was found that apt-key in apt,       |
|                  |                  |          |                   |               | all versions, do not correctly...       |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2011-3374    |
```



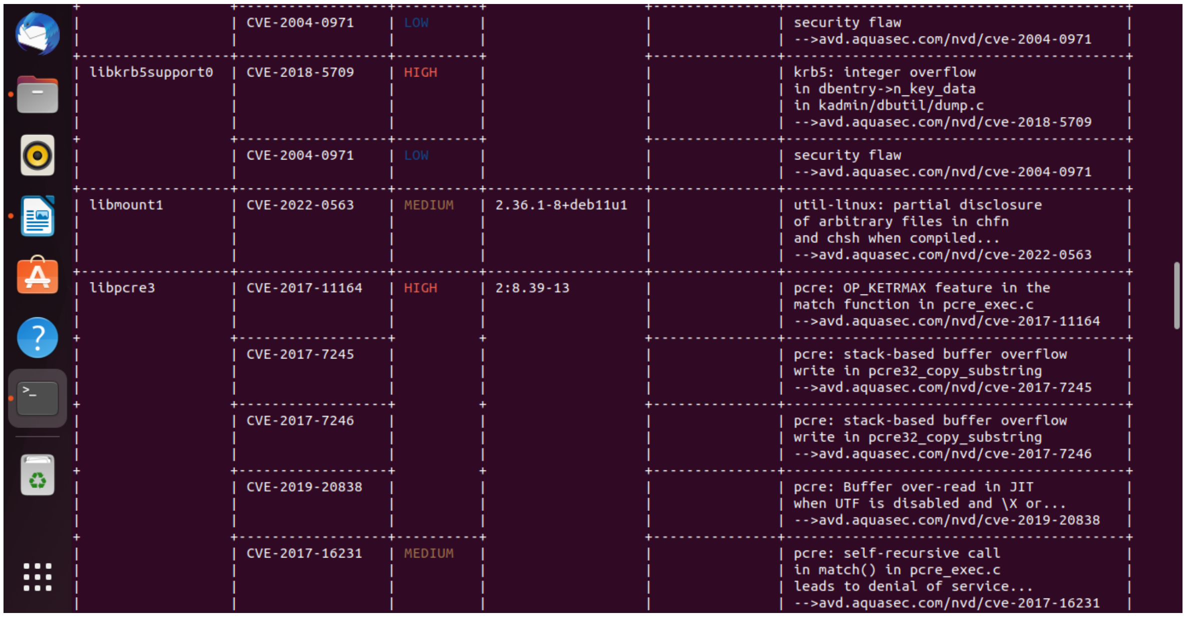
```
| libblkid1        | CVE-2022-0563    | MEDIUM   | 2.36.1-8+deb11u1  |               | util-linux: partial disclosure          |
|                  |                  |          |                   |               | of arbitrary files in chfn              |
|                  |                  |          |                   |               | and chsh when compiled...               |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2022-0563    |
+------------------+------------------+----------+-------------------+---------------+-----------------------------------------+
| libc-bin         | CVE-2019-1010022 | CRITICAL | 2.31-13+deb11u5   |               | glibc: stack guard protection bypass    |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2019-1010022 |
+                  +------------------+----------+                   +---------------+-----------------------------------------+
|                  | CVE-2018-20796   | HIGH     |                   |               | glibc: uncontrolled recursion in        |
|                  |                  |          |                   |               | function check_dst_limits_calc_pos_1    |
|                  |                  |          |                   |               | in posix/regexec.c                      |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2018-20796   |
+                  +------------------+          +                   +---------------+-----------------------------------------+
|                  | CVE-2019-1010023 |          |                   |               | glibc: running ldd on malicious ELF     |
|                  |                  |          |                   |               | leads to code execution because of...   |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2019-1010023 |
+                  +------------------+          +                   +---------------+-----------------------------------------+
|                  | CVE-2019-9192    |          |                   |               | glibc: uncontrolled recursion in        |
|                  |                  |          |                   |               | function check_dst_limits_calc_pos_1    |
|                  |                  |          |                   |               | in posix/regexec.c                      |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2019-9192    |
+                  +------------------+----------+                   +---------------+-----------------------------------------+
|                  | CVE-2010-4756    | MEDIUM   |                   |               | glibc: glob implementation              |
|                  |                  |          |                   |               | can cause excessive CPU and             |
|                  |                  |          |                   |               | memory consumption due to...            |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2010-4756    |
+                  +------------------+          +                   +---------------+-----------------------------------------+
|                  | CVE-2019-1010024 |          |                   |               | glibc: ASLR bypass using                |
|                  |                  |          |                   |               | cache of thread stack and heap          |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2019-1010024 |
+                  +------------------+          +                   +---------------+-----------------------------------------+
|                  | CVE-2019-1010025 |          |                   |               | glibc: information disclosure of heap   |
|                  |                  |          |                   |               | addresses of pthread_created thread     |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2019-1010025 |
+------------------+------------------+----------+                   +---------------+-----------------------------------------+
| libc6            | CVE-2019-1010022 | CRITICAL |                   |               | glibc: stack guard protection bypass    |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2019-1010022 |
+                  +------------------+----------+                   +---------------+-----------------------------------------+
```



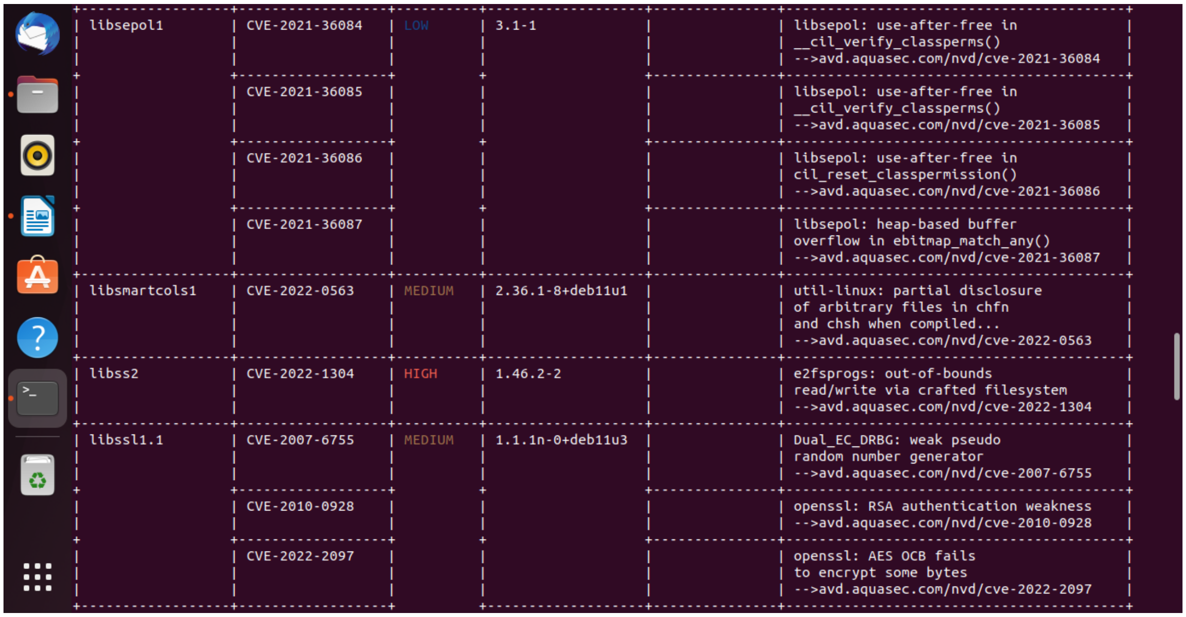
```
+                  +------------------+----------+                   +---------------+-----------------------------------------+
|                  | CVE-2018-20796   | HIGH     |                   |               | glibc: uncontrolled recursion in        |
|                  |                  |          |                   |               | function check_dst_limits_calc_pos_1    |
|                  |                  |          |                   |               | in posix/regexec.c                      |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2018-20796   |
+                  +------------------+          +                   +---------------+-----------------------------------------+
|                  | CVE-2019-1010023 |          |                   |               | glibc: running ldd on malicious ELF     |
|                  |                  |          |                   |               | leads to code execution because of...   |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2019-1010023 |
+                  +------------------+          +                   +---------------+-----------------------------------------+
|                  | CVE-2019-9192    |          |                   |               | glibc: uncontrolled recursion in        |
|                  |                  |          |                   |               | function check_dst_limits_calc_pos_1    |
|                  |                  |          |                   |               | in posix/regexec.c                      |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2019-9192    |
+                  +------------------+----------+                   +---------------+-----------------------------------------+
|                  | CVE-2010-4756    | MEDIUM   |                   |               | glibc: glob implementation              |
|                  |                  |          |                   |               | can cause excessive CPU and             |
|                  |                  |          |                   |               | memory consumption due to...            |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2010-4756    |
+                  +------------------+          +                   +---------------+-----------------------------------------+
|                  | CVE-2019-1010024 |          |                   |               | glibc: ASLR bypass using                |
|                  |                  |          |                   |               | cache of thread stack and heap          |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2019-1010024 |
+                  +------------------+          +                   +---------------+-----------------------------------------+
|                  | CVE-2019-1010025 |          |                   |               | glibc: information disclosure of heap   |
|                  |                  |          |                   |               | addresses of pthread_created thread     |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2019-1010025 |
+------------------+------------------+----------+-------------------+---------------+-----------------------------------------+
| libcom-err2      | CVE-2022-1304    | HIGH     | 1.46.2-2          |               | e2fsprogs: out-of-bounds                |
|                  |                  |          |                   |               | read/write via crafted filesystem       |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2022-1304    |
+------------------+------------------+----------+-------------------+---------------+-----------------------------------------+
| libdb5.3         | CVE-2019-8457    | CRITICAL | 5.3.28+dfsg1-0.8  |               | sqlite: heap out-of-bound               |
|                  |                  |          |                   |               | read in function rtreenode()            |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2019-8457    |
+------------------+------------------+----------+-------------------+---------------+-----------------------------------------+
| libext2fs2       | CVE-2022-1304    | HIGH     | 1.46.2-2          |               | e2fsprogs: out-of-bounds                |
|                  |                  |          |                   |               | read/write via crafted filesystem       |
```



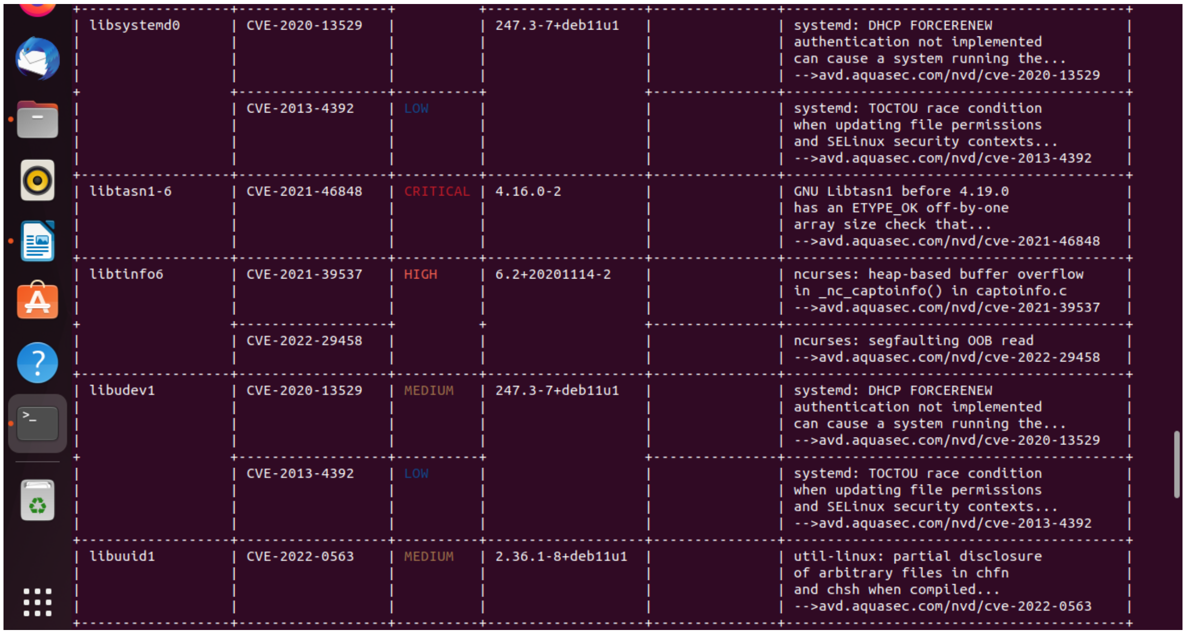
```
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2022-1304    |
+------------------+------------------+          +-------------------+---------------+-----------------------------------------+
| libgcrypt20      | CVE-2018-6829    |          | 1.8.7-6           |               | libgcrypt: ElGamal implementation       |
|                  |                  |          |                   |               | doesn't have semantic security due      |
|                  |                  |          |                   |               | to incorrectly encoded plaintexts...    |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2018-6829    |
+                  +------------------+          +                   +---------------+-----------------------------------------+
|                  | CVE-2021-33560   |          |                   |               | libgcrypt: mishandles ElGamal           |
|                  |                  |          |                   |               | encryption because it lacks             |
|                  |                  |          |                   |               | exponent blinding to address a...       |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2021-33560   |
+------------------+------------------+----------+-------------------+---------------+-----------------------------------------+
| libgnutls30      | CVE-2011-3389    | MEDIUM   | 3.7.1-5+deb11u2   |               | HTTPS: block-wise chosen-plaintext      |
|                  |                  |          |                   |               | attack against SSL/TLS (BEAST)          |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2011-3389    |
+------------------+------------------+----------+-------------------+---------------+-----------------------------------------+
| libgssapi-krb5-2 | CVE-2018-5709    | HIGH     | 1.18.3-6+deb11u2  |               | krb5: integer overflow                  |
|                  |                  |          |                   |               | in dbentry->n_key_data                  |
|                  |                  |          |                   |               | in kadmin/dbutil/dump.c                 |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2018-5709    |
+                  +------------------+----------+                   +---------------+-----------------------------------------+
|                  | CVE-2004-0971    | LOW      |                   |               | security flaw                           |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2004-0971    |
+------------------+------------------+----------+                   +---------------+-----------------------------------------+
| libk5crypto3     | CVE-2018-5709    | HIGH     |                   |               | krb5: integer overflow                  |
|                  |                  |          |                   |               | in dbentry->n_key_data                  |
|                  |                  |          |                   |               | in kadmin/dbutil/dump.c                 |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2018-5709    |
+                  +------------------+----------+                   +---------------+-----------------------------------------+
|                  | CVE-2004-0971    | LOW      |                   |               | security flaw                           |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2004-0971    |
+------------------+------------------+----------+                   +---------------+-----------------------------------------+
| libkrb5-3        | CVE-2018-5709    | HIGH     |                   |               | krb5: integer overflow                  |
|                  |                  |          |                   |               | in dbentry->n_key_data                  |
|                  |                  |          |                   |               | in kadmin/dbutil/dump.c                 |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2018-5709    |
+------------------+------------------+----------+                   +---------------+-----------------------------------------+
```



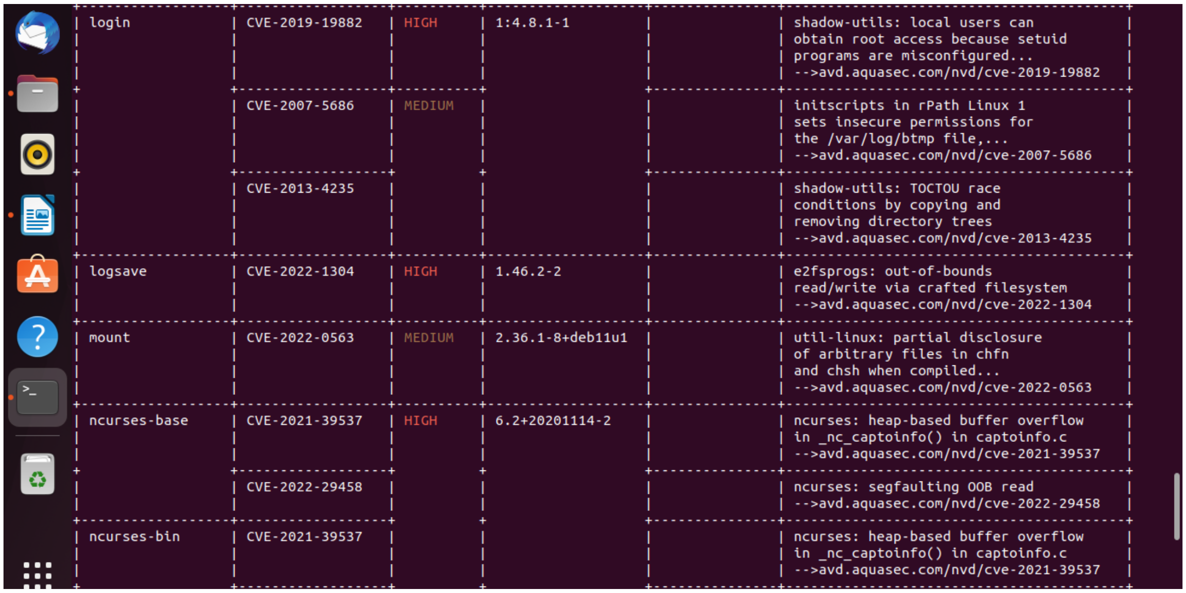
```
+                  +------------------+----------+                   +---------------+----------------------------------------+
|                  | CVE-2004-0971    | LOW      |                   |               | security flaw                          |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2004-0971   |
+------------------+------------------+----------+-------------------+---------------+----------------------------------------+
| libkrb5support0  | CVE-2018-5709    | HIGH     |                   |               | krb5: integer overflow                 |
|                  |                  |          |                   |               | in dbentry->n_key_data                 |
|                  |                  |          |                   |               | in kadmin/dbutil/dump.c                |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2018-5709   |
+                  +------------------+----------+                   +---------------+----------------------------------------+
|                  | CVE-2004-0971    | LOW      |                   |               | security flaw                          |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2004-0971   |
+------------------+------------------+----------+-------------------+---------------+----------------------------------------+
| libmount1        | CVE-2022-0563    | MEDIUM   | 2.36.1-8+deb11u1  |               | util-linux: partial disclosure         |
|                  |                  |          |                   |               | of arbitrary files in chfn             |
|                  |                  |          |                   |               | and chsh when compiled...              |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2022-0563   |
+------------------+------------------+----------+-------------------+---------------+----------------------------------------+
| libpcre3         | CVE-2017-11164   | HIGH     | 2:8.39-13         |               | pcre: OP_KETRMAX feature in the        |
|                  |                  |          |                   |               | match function in pcre_exec.c          |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2017-11164  |
+                  +------------------+          +                   +---------------+----------------------------------------+
|                  | CVE-2017-7245    |          |                   |               | pcre: stack-based buffer overflow      |
|                  |                  |          |                   |               | write in pcre32_copy_substring         |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2017-7245   |
+                  +------------------+          +                   +---------------+----------------------------------------+
|                  | CVE-2017-7246    |          |                   |               | pcre: stack-based buffer overflow      |
|                  |                  |          |                   |               | write in pcre32_copy_substring         |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2017-7246   |
+                  +------------------+          +                   +---------------+----------------------------------------+
|                  | CVE-2019-20838   |          |                   |               | pcre: Buffer over-read in JIT          |
|                  |                  |          |                   |               | when UTF is disabled and \X or...      |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2019-20838  |
+                  +------------------+----------+                   +---------------+----------------------------------------+
|                  | CVE-2017-16231   | MEDIUM   |                   |               | pcre: self-recursive call              |
|                  |                  |          |                   |               | in match() in pcre_exec.c              |
|                  |                  |          |                   |               | leads to denial of service...          |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2017-16231  |
```



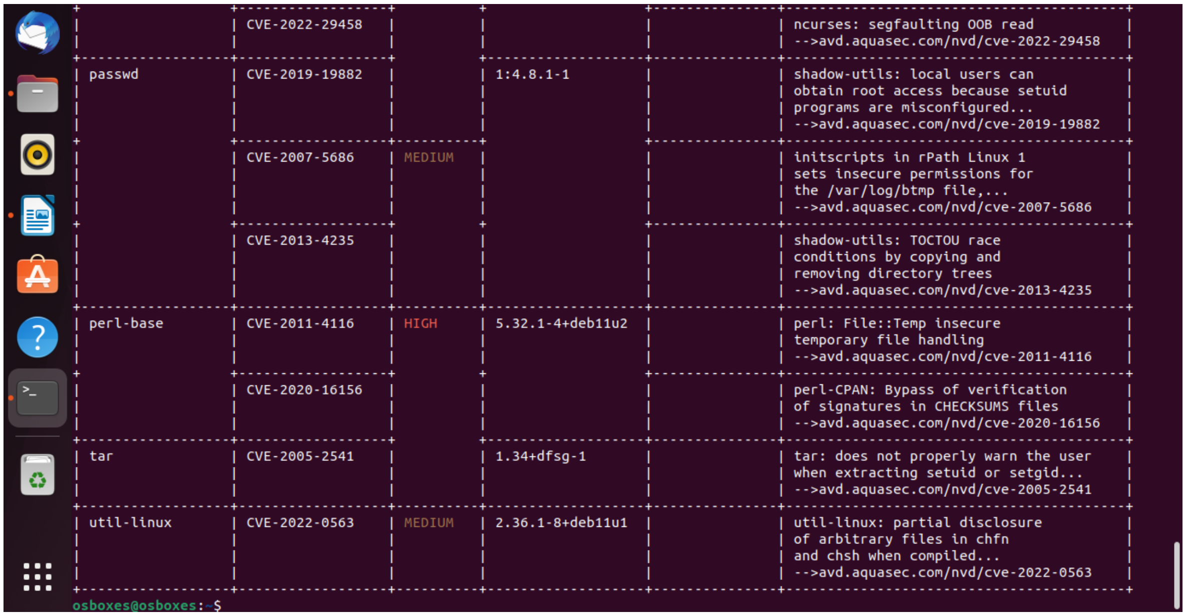
```
+------------------+------------------+----------+-------------------+---------------+----------------------------------------+
| libsepol1        | CVE-2021-36084   | LOW      | 3.1-1             |               | libsepol: use-after-free in            |
|                  |                  |          |                   |               | __cil_verify_classperms()              |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2021-36084  |
+                  +------------------+          +                   +---------------+----------------------------------------+
|                  | CVE-2021-36085   |          |                   |               | libsepol: use-after-free in            |
|                  |                  |          |                   |               | __cil_verify_classperms()              |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2021-36085  |
+                  +------------------+          +                   +---------------+----------------------------------------+
|                  | CVE-2021-36086   |          |                   |               | libsepol: use-after-free in            |
|                  |                  |          |                   |               | cil_reset_classpermission()            |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2021-36086  |
+                  +------------------+          +                   +---------------+----------------------------------------+
|                  | CVE-2021-36087   |          |                   |               | libsepol: heap-based buffer            |
|                  |                  |          |                   |               | overflow in ebitmap_match_any()        |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2021-36087  |
+------------------+------------------+----------+-------------------+---------------+----------------------------------------+
| libsmartcols1    | CVE-2022-0563    | MEDIUM   | 2.36.1-8+deb11u1  |               | util-linux: partial disclosure         |
|                  |                  |          |                   |               | of arbitrary files in chfn             |
|                  |                  |          |                   |               | and chsh when compiled...              |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2022-0563   |
+------------------+------------------+----------+-------------------+---------------+----------------------------------------+
| libss2           | CVE-2022-1304    | HIGH     | 1.46.2-2          |               | e2fsprogs: out-of-bounds               |
|                  |                  |          |                   |               | read/write via crafted filesystem      |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2022-1304   |
+------------------+------------------+----------+-------------------+---------------+----------------------------------------+
| libssl1.1        | CVE-2007-6755    | MEDIUM   | 1.1.1n-0+deb11u3  |               | Dual_EC_DRBG: weak pseudo              |
|                  |                  |          |                   |               | random number generator                |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2007-6755   |
+                  +------------------+          +                   +---------------+----------------------------------------+
|                  | CVE-2010-0928    |          |                   |               | openssl: RSA authentication weakness   |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2010-0928   |
+                  +------------------+          +                   +---------------+----------------------------------------+
|                  | CVE-2022-2097    |          |                   |               | openssl: AES OCB fails                 |
|                  |                  |          |                   |               | to encrypt some bytes                  |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2022-2097   |
+------------------+------------------+          +-------------------+---------------+----------------------------------------+
```



```
+-------------------+------------------+          +-------------------+---------------+------------------------------------------+
| libsystemd0       | CVE-2020-13529   |          | 247.3-7+deb11u1   |               | systemd: DHCP FORCERENEW                 |
|                   |                  |          |                   |               | authentication not implemented           |
|                   |                  |          |                   |               | can cause a system running the...        |
|                   |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2020-13529    |
+                   +------------------+----------+                   +---------------+------------------------------------------+
|                   | CVE-2013-4392    | LOW      |                   |               | systemd: TOCTOU race condition           |
|                   |                  |          |                   |               | when updating file permissions           |
|                   |                  |          |                   |               | and SELinux security contexts...         |
|                   |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2013-4392     |
+-------------------+------------------+----------+-------------------+---------------+------------------------------------------+
| libtasn1-6        | CVE-2021-46848   | CRITICAL | 4.16.0-2          |               | GNU Libtasn1 before 4.19.0               |
|                   |                  |          |                   |               | has an ETYPE_OK off-by-one               |
|                   |                  |          |                   |               | array size check that...                 |
|                   |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2021-46848    |
+-------------------+------------------+----------+-------------------+---------------+------------------------------------------+
| libtinfo6         | CVE-2021-39537   | HIGH     | 6.2+20201114-2    |               | ncurses: heap-based buffer overflow      |
|                   |                  |          |                   |               | in _nc_captoinfo() in captoinfo.c        |
|                   |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2021-39537    |
+                   +------------------+          +                   +---------------+------------------------------------------+
|                   | CVE-2022-29458   |          |                   |               | ncurses: segfaulting OOB read            |
|                   |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2022-29458    |
+-------------------+------------------+----------+-------------------+---------------+------------------------------------------+
| libudev1          | CVE-2020-13529   | MEDIUM   | 247.3-7+deb11u1   |               | systemd: DHCP FORCERENEW                 |
|                   |                  |          |                   |               | authentication not implemented           |
|                   |                  |          |                   |               | can cause a system running the...        |
|                   |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2020-13529    |
+                   +------------------+----------+                   +---------------+------------------------------------------+
|                   | CVE-2013-4392    | LOW      |                   |               | systemd: TOCTOU race condition           |
|                   |                  |          |                   |               | when updating file permissions           |
|                   |                  |          |                   |               | and SELinux security contexts...         |
|                   |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2013-4392     |
+-------------------+------------------+----------+-------------------+---------------+------------------------------------------+
| libuuid1          | CVE-2022-0563    | MEDIUM   | 2.36.1-8+deb11u1  |               | util-linux: partial disclosure           |
|                   |                  |          |                   |               | of arbitrary files in chfn               |
|                   |                  |          |                   |               | and chsh when compiled...                |
|                   |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2022-0563     |
+-------------------+------------------+----------+-------------------+---------------+------------------------------------------+
```



```
+-------------------+------------------+----------+-------------------+---------------+------------------------------------------+
| login             | CVE-2019-19882   | HIGH     | 1:4.8.1-1         |               | shadow-utils: local users can            |
|                   |                  |          |                   |               | obtain root access because setuid        |
|                   |                  |          |                   |               | programs are misconfigured...            |
|                   |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2019-19882    |
+                   +------------------+----------+                   +---------------+------------------------------------------+
|                   | CVE-2007-5686    | MEDIUM   |                   |               | initscripts in rPath Linux 1             |
|                   |                  |          |                   |               | sets insecure permissions for            |
|                   |                  |          |                   |               | the /var/log/btmp file,...               |
|                   |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2007-5686     |
+                   +------------------+          +                   +---------------+------------------------------------------+
|                   | CVE-2013-4235    |          |                   |               | shadow-utils: TOCTOU race                |
|                   |                  |          |                   |               | conditions by copying and                |
|                   |                  |          |                   |               | removing directory trees                 |
|                   |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2013-4235     |
+-------------------+------------------+----------+-------------------+---------------+------------------------------------------+
| logsave           | CVE-2022-1304    | HIGH     | 1.46.2-2          |               | e2fsprogs: out-of-bounds                 |
|                   |                  |          |                   |               | read/write via crafted filesystem        |
|                   |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2022-1304     |
+-------------------+------------------+----------+-------------------+---------------+------------------------------------------+
| mount             | CVE-2022-0563    | MEDIUM   | 2.36.1-8+deb11u1  |               | util-linux: partial disclosure           |
|                   |                  |          |                   |               | of arbitrary files in chfn               |
|                   |                  |          |                   |               | and chsh when compiled...                |
|                   |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2022-0563     |
+-------------------+------------------+----------+-------------------+---------------+------------------------------------------+
| ncurses-base      | CVE-2021-39537   | HIGH     | 6.2+20201114-2    |               | ncurses: heap-based buffer overflow      |
|                   |                  |          |                   |               | in _nc_captoinfo() in captoinfo.c        |
|                   |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2021-39537    |
+                   +------------------+          +                   +---------------+------------------------------------------+
|                   | CVE-2022-29458   |          |                   |               | ncurses: segfaulting OOB read            |
|                   |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2022-29458    |
+-------------------+------------------+          +                   +---------------+------------------------------------------+
| ncurses-bin       | CVE-2021-39537   |          |                   |               | ncurses: heap-based buffer overflow      |
|                   |                  |          |                   |               | in _nc_captoinfo() in captoinfo.c        |
|                   |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2021-39537    |
+-------------------+------------------+          +                   +---------------+------------------------------------------+
```



```
+                  +------------------+          +                   +---------------+------------------------------------------+
|                  | CVE-2022-29458   |          |                   |               | ncurses: segfaulting OOB read            |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2022-29458    |
+------------------+------------------+          +-------------------+---------------+------------------------------------------+
| passwd           | CVE-2019-19882   |          | 1:4.8.1-1         |               | shadow-utils: local users can            |
|                  |                  |          |                   |               | obtain root access because setuid        |
|                  |                  |          |                   |               | programs are misconfigured...            |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2019-19882    |
+                  +------------------+----------+                   +---------------+------------------------------------------+
|                  | CVE-2007-5686    | MEDIUM   |                   |               | initscripts in rPath Linux 1             |
|                  |                  |          |                   |               | sets insecure permissions for            |
|                  |                  |          |                   |               | the /var/log/btmp file,...               |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2007-5686     |
+                  +------------------+          +                   +---------------+------------------------------------------+
|                  | CVE-2013-4235    |          |                   |               | shadow-utils: TOCTOU race                |
|                  |                  |          |                   |               | conditions by copying and                |
|                  |                  |          |                   |               | removing directory trees                 |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2013-4235     |
+------------------+------------------+----------+-------------------+---------------+------------------------------------------+
| perl-base        | CVE-2011-4116    | HIGH     | 5.32.1-4+deb11u2  |               | perl: File::Temp insecure                |
|                  |                  |          |                   |               | temporary file handling                  |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2011-4116     |
+                  +------------------+          +                   +---------------+------------------------------------------+
|                  | CVE-2020-16156   |          |                   |               | perl-CPAN: Bypass of verification        |
|                  |                  |          |                   |               | of signatures in CHECKSUMS files         |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2020-16156    |
+------------------+------------------+          +-------------------+---------------+------------------------------------------+
| tar              | CVE-2005-2541    |          | 1.34+dfsg-1       |               | tar: does not properly warn the user     |
|                  |                  |          |                   |               | when extracting setuid or setgid...      |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2005-2541     |
+------------------+------------------+----------+-------------------+---------------+------------------------------------------+
| util-linux       | CVE-2022-0563    | MEDIUM   | 2.36.1-8+deb11u1  |               | util-linux: partial disclosure           |
|                  |                  |          |                   |               | of arbitrary files in chfn               |
|                  |                  |          |                   |               | and chsh when compiled...                |
|                  |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2022-0563     |
+------------------+------------------+----------+-------------------+---------------+------------------------------------------+
osboxes@osboxes:~$
```