目次

Trivy を使用して SBOM を作成する 3
Trivy のインストール 3
root filesystem から SBOM を生成 4
SBOM ファイルをスキャンして脆弱性のレポート作成 6
参考 26

Trivy を使用して SBOM を作成する

Trivy というソフトを使用し、MA-シリーズの root filesystem から SBOM を生成することができます。

Trivy のインストール

Getting Started - Installation に従い、インストールします。

※ 現時点での最新バージョン v0.41.0 をインストールしていますが、適宜読み替えてください。

```
user1@jammy64-dev:~$ wget
https://github.com/aquasecurity/trivy/releases/download/v0.41.0/trivy_0.41.0
_Linux-64bit.deb
--2023-05-09 15:40:08--
https://github.com/aquasecurity/trivy/releases/download/v0.41.0/trivy_0.41.0
_Linux-64bit.deb
Resolving github.com (github.com)... 20.27.177.113
Connecting to github.com (github.com)|20.27.177.113|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location:
https://objects.githubusercontent.com/github-production-release-asset-2e65be
/180687624/8bfa74aa-6249-4531-b5a3-f4a65912a989?X-Amz-Algorithm=AWS4-HMAC-
SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53A%2F20230509%2Fus-
east-1%2Fs3%2Faws4_request&X-Amz-Date=20230509T064009Z&X-Amz-Expires=300&X-
Amz-
Signature=2a38652ab06e5ce4e5ee922379d17a3f961df9e83bf762fbc29032701faeb63a&X
-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=180687624&response-
content-
disposition=attachment%3B%20filename%3Dtrivy_0.41.0_Linux-64bit.deb&response
-content-type=application%2Foctet-stream [following]
--2023-05-09 15:40:09--
https://objects.githubusercontent.com/github-production-release-asset-2e65be
/180687624/8bfa74aa-6249-4531-b5a3-f4a65912a989?X-Amz-Algorithm=AWS4-HMAC-
```

```
SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53A%2F20230509%2Fus-
east-1%2Fs3%2Faws4_request&X-Amz-Date=20230509T064009Z&X-Amz-Expires=300&X-
Amz-
Signature=2a38652ab06e5ce4e5ee922379d17a3f961df9e83bf762fbc29032701faeb63a&X
-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=180687624&response-
content-
disposition=attachment%3B%20filename%3Dtrivy_0.41.0_Linux-64bit.deb&response
-content-type=application%2Foctet-stream
Resolving objects.githubusercontent.com (objects.githubusercontent.com)...
185.199.108.133, 185.199.109.133, 185.199.110.133, ...
Connecting to objects.githubusercontent.com
(objects.githubusercontent.com)|185.199.108.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 53147460 (51M) [application/octet-stream]
Saving to: ‘trivy_0.41.0_Linux-64bit.deb’

trivy_0.41.0_Linux-64bit.deb
100%[=============================================>]  50.68M  19.3MB/s
in 2.6s

2023-05-09 15:40:12 (19.3 MB/s) - ‘trivy_0.41.0_Linux-64bit.deb’ saved
[53147460/53147460]

user1@jammy64-dev:~$
```

```
user1@jammy64-dev:~$ sudo dpkg -i trivy_0.41.0_Linux-64bit.deb
[sudo] password for user1:
Selecting previously unselected package trivy.
(Reading database ... 66017 files and directories currently installed.)
Preparing to unpack trivy_0.41.0_Linux-64bit.deb ...
Unpacking trivy (0.41.0) ...
Setting up trivy (0.41.0) ...
user1@jammy64-dev:~$
```

```
user1@jammy64-dev:~$ trivy --version
Version: 0.41.0
user1@jammy64-dev:~$
```

root filesystem から SBOM を生成

ファームウェアを作成するベースの root filesystem を展開したディレクトリを指定し、SPDX JSON 形式で SBOM ファイルを生成します。

```
root@jammy64-dev:/home/user1/work/MAX3xx# trivy -q rootfs
max3xx_jammy_rootfs/ --format spdx-json|jq . > max3xx_jammy_v6_0_0_sbom.json
root@jammy64-dev:/home/user1/work/MAX3xx# ls -l
```

```
max3xx_jammy_v6_0_0_sbom.json
-rw-r--r-- 1 root root 324755 May  9 15:45 max3xx_jammy_v6_0_0_sbom.json
```

生成された SBOM ファイルの先頭 50 行分を見てみます。

```
root@jammy64-dev:/home/user1/work/MAX3xx# head -50
max3xx_jammy_v6_0_0_sbom.json
{
  "spdxVersion": "SPDX-2.3",
  "dataLicense": "CC0-1.0",
  "SPDXID": "SPDXRef-DOCUMENT",
  "name": "metis",
  "documentNamespace":
"http://aquasecurity.github.io/trivy/filesystem/metis-c32fa95a-4b34-41dd-94a
1-f9b5d4731066",
  "creationInfo": {
    "licenseListVersion": "",
    "creators": [
      "Organization: aquasecurity",
      "Tool: trivy-0.41.0"
    ],
    "created": "2023-05-09T06:45:43Z"
  },
  "packages": [
    {
      "name": "adduser",
      "SPDXID": "SPDXRef-Package-34deaa096ed34b29",
      "versionInfo": "3.118ubuntu5",
      "supplier": "Organization: Ubuntu Developers <ubuntu-devel-
discuss@lists.ubuntu.com>",
      "downloadLocation": "NONE",
      "sourceInfo": "built package from: adduser 3.118ubuntu5",
      "licenseConcluded": "GPL-2.0-only",
      "licenseDeclared": "GPL-2.0-only",
      "copyrightText": "",
      "externalRefs": [
        {
          "referenceCategory": "PACKAGE-MANAGER",
          "referenceType": "purl",
          "referenceLocator":
"pkg:deb/ubuntu/adduser@3.118ubuntu5?arch=all&distro=ubuntu-22.04"
        }
      ],
      "attributionTexts": [
        "PkgID: adduser@3.118ubuntu5"
      ],
      "primaryPackagePurpose": "LIBRARY"
    },
    {
```

```
      "name": "apt",
      "SPDXID": "SPDXRef-Package-d0ca1f264da0ea99",
      "versionInfo": "2.4.9",
      "supplier": "Organization: Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>",
      "downloadLocation": "NONE",
      "sourceInfo": "built package from: apt 2.4.9",
      "licenseConcluded": "GPL-2.0-only",
      "licenseDeclared": "GPL-2.0-only",
      "copyrightText": "",
      "externalRefs": [
        {
          "referenceCategory": "PACKAGE-MANAGER",
root@jammy64-dev:/home/user1/work/MAX3xx#
```


インストールされているパッケージの情報から、各パッケージの名前やライセンスなどが抽出されていることがわかります。

SBOM ファイルをスキャンして脆弱性のレポート作成

作成した SBOM ファイルをスキャンし、脆弱性(CVE-xxxx) があるか調査することができます。

```
root@jammy64-dev:/home/user1/work/MAX3xx# trivy -q sbom
max3xx_jammy_v6_0_0_sbom.json
```

```
max3xx_jammy_v6_0_0_sbom.json (ubuntu 22.04)

Total: 96 (UNKNOWN: 0, LOW: 58, MEDIUM: 38, HIGH: 0, CRITICAL: 0)

┌────────────────────────┬───────────────────┬──────────┬──────────────────────
─────┬────────────────┬──────────────────────────────────────────────────────
────────┐
│        Library         │  Vulnerability    │ Severity │    Installed Version
│ Fixed Version │                             Title
│
├────────────────────────┼───────────────────┼──────────┼──────────────────────
─────┼────────────────┼──────────────────────────────────────────────────────
────────┤
│ bash                   │ CVE-2022-3715     │ LOW      │ 5.1-6ubuntu1
│                │ a heap-buffer-overflow in valid_parameter_transform
│
│                        │                   │          │
│                │ https://avd.aquasec.com/nvd/cve-2022-3715
│
├────────────────────────┼───────────────────┼──────────┼──────────────────────
─────┼────────────────┼──────────────────────────────────────────────────────
────────┤
```

```
| bluez                 | CVE-2020-10134   | MEDIUM   | 5.64-0ubuntu1
|               | bluetooth: Method Confusion Pairing Vulnerability in LE
|                       |                  |          |
|                       |                  |          |
|               | Secure Connections and BR/EDR Secure...
|                       |                  |          |
|                       |                  |          |
|               | https://avd.aquasec.com/nvd/cve-2020-10134
|                       |                  |          |
|                       |------------------|----------|
|---------------|-------------------------------------------------------------------------------
---|
|                       | CVE-2016-9797    | LOW      |
|               | bluez: buffer over-read in l2cap_dump()
|                       |                  |          |
|                       |                  |          |
|               | https://avd.aquasec.com/nvd/cve-2016-9797
|                       |                  |          |
|                       |------------------|          |
|---------------|-------------------------------------------------------------------------------
---|
|                       | CVE-2016-9798    |          |
|               | bluez: use-after-free in conf_opt()
|                       |                  |          |
|                       |                  |          |
|               | https://avd.aquasec.com/nvd/cve-2016-9798
|                       |                  |          |
|                       |------------------|          |
|---------------|-------------------------------------------------------------------------------
---|
|                       | CVE-2016-9799    |          |
|               | bluez: buffer overflow in pklg_read_hci()
|                       |                  |          |
|                       |                  |          |
|               | https://avd.aquasec.com/nvd/cve-2016-9799
|                       |                  |          |
|                       |------------------|          |
|---------------|-------------------------------------------------------------------------------
---|
|                       | CVE-2016-9800    |          |
|               | bluez: buffer overflow in pin_code_reply_dump()
|                       |                  |          |
|                       |                  |          |
|               | https://avd.aquasec.com/nvd/cve-2016-9800
|                       |                  |          |
|                       |------------------|          |
|---------------|-------------------------------------------------------------------------------
---|
|                       | CVE-2016-9801    |          |
|               | bluez: buffer overflow in set_ext_ctrl()
|
```

```
|                       |                     |          |
|               | https://avd.aquasec.com/nvd/cve-2016-9801
|
|                       |                     |          |
|---------------|-----------------------------------------------------------------------
---|
|                       | CVE-2016-9802       |          |
|               | bluez: buffer over-read in l2cap_packet()
|
|                       |                     |          |
|               | https://avd.aquasec.com/nvd/cve-2016-9802
|
|                       |                     |          |
|---------------|-----------------------------------------------------------------------
---|
|                       | CVE-2016-9803       |          |
|               | bluez: out-of-bounds read in le_meta_ev_dump()
|
|                       |                     |          |
|               | https://avd.aquasec.com/nvd/cve-2016-9803
|
|                       |                     |          |
|---------------|-----------------------------------------------------------------------
---|
|                       | CVE-2016-9804       |          |
|               | bluez: buffer overflow in commands_dump()
|
|                       |                     |          |
|               | https://avd.aquasec.com/nvd/cve-2016-9804
|
|                       |                     |          |
|---------------|-----------------------------------------------------------------------
---|
|                       | CVE-2016-9917       |          |
|               | bluez: Heap-based buffer overflow vulnerability in
read_n()  |
|                       |                     |          |
|               | https://avd.aquasec.com/nvd/cve-2016-9917
|
|                       |                     |          |
|---------------|-----------------------------------------------------------------------
---|
|                       | CVE-2016-9918       |          |
|               | bluez: Out of bounds stack read in packet_hexdump()
|
|                       |                     |          |
|               | https://avd.aquasec.com/nvd/cve-2016-9918
|
|                       |                     |          |
|---------------|-----------------------------------------------------------------------
---|
```

```
──┤
│                       │ CVE-2020-9770    │          │
│               │ bluez: BLESA bluetooth attack
│                       │                  │          │
│               │ https://avd.aquasec.com/nvd/cve-2020-9770
│                       ├──────────────────┤          │
├──────────────┼──────────────────────────────────────────────────────────────────────────────
──┤
│                       │ CVE-2022-3563    │          │
│               │ bluez: NULL pointer dereference in
│                       │                  │          │
│               │ read_50_controller_cap_complete() in tools/mgmt-tester.c
│                       │                  │          │
│               │ https://avd.aquasec.com/nvd/cve-2022-3563
│                       ├──────────────────┤
├──────────────┼──────────────────┼──────────────────────────────────────────────────────────────
──────────────┤
│ busybox               │ CVE-2022-28391   │          │ 1:1.30.1-7ubuntu3
│               │ busybox: remote attackers may execute arbitrary code if
│                       │                  │          │
│               │ netstat is used
│                       │                  │          │
│               │ https://avd.aquasec.com/nvd/cve-2022-28391
│                       │                  │          │
├──────────────┼──────────────────┼──────────┼──────────┤
│ busybox-initramfs     │                  │          │
│               │
│                       │                  │          │
│               │
│                       │                  │          │
│               │
│                       │                  │          │
│               │
│                       │                  │          │
├──────────────┼──────────────────┼──────────┼──────────┤
│ coreutils             │ CVE-2016-2781    │          │ 8.32-4.1ubuntu1
│               │ coreutils: Non-privileged session can escape to the parent
│                       │                  │          │
│               │ session in chroot
```

```
│                         │                   │          │
│                 │ https://avd.aquasec.com/nvd/cve-2016-2781
│
├─────────────────────────┼───────────────────┤
├─────────────────────────┼───────────────────┼──────────────────────────────────
──────────────────────────────┤
│ gpgv                    │ CVE-2022-3219     │          │ 2.2.27-3ubuntu2.1
│                 │ gnupg: denial of service issue (resource consumption)
using  │
│                         │                   │          │
│                 │ compressed packets
│
│                         │                   │          │
│                 │ https://avd.aquasec.com/nvd/cve-2022-3219
│
├─────────────────────────┼───────────────────┼──────────┼──────────────────────
──────┼──────────────────┼──────────────────────────────────────────────────────
──────────┤
│ libapparmor1            │ CVE-2016-1585     │ MEDIUM   │ 3.0.4-2ubuntu2.2
│                 │ In all versions of AppArmor mount rules are accidentally
│
│                         │                   │          │
│                 │ widened when ...
│
│                         │                   │          │
│                 │ https://avd.aquasec.com/nvd/cve-2016-1585
│
├─────────────────────────┼───────────────────┼──────────┼──────────────────────
──────┼──────────────────┼──────────────────────────────────────────────────────
──────────┤
│ libc-bin                │ CVE-2016-20013    │ LOW      │ 2.35-0ubuntu3.1
│                 │ sha256crypt and sha512crypt through 0.6 allow attackers to
│
│                         │                   │          │
│                 │ cause a denial of...
│
│                         │                   │          │
│                 │ https://avd.aquasec.com/nvd/cve-2016-20013
│
├─────────────────────────┤                   │          │
├─────────────────┤
│
│ libc6                   │                   │          │
│                 │
│
│                         │                   │          │
│                 │
│
│                         │                   │          │
```

```
│                │
│
├────────────────────────┼──────────────────────┼──────────┼──────────────────────
──────┼──────────────────┼──────────────────────────────────────────────────────
──────┤
│ libcjson1              │ CVE-2018-1000215 │ MEDIUM   │ 1.7.15-1
│                │ Dave Gamble cJSON version 1.7.6 and earlier contains a
│
│                        │                  │          │
│                │ CWE-772 vulnera ......
│
│                        │                  │          │
│                │ https://avd.aquasec.com/nvd/cve-2018-1000215
│
├────────────────────────┼──────────────────────┼──────────┼──────────────────────
──────┼──────────────────┼──────────────────────────────────────────────────────
──────┤
│ libglib2.0-0           │ CVE-2023-24593   │ LOW      │ 2.72.4-0ubuntu2
│                │ glib: DoS caused by handling a malicious text-form variant
│
│                        │                  │          │
│                │ https://avd.aquasec.com/nvd/cve-2023-24593
│
│                        ├──────────────────┤          │
├────────────────┼──────────────────────────────────────────────────────────────
──┤
│                        │ CVE-2023-25180   │          │
│                │ glib: DoS caused by malicious serialised variant
│
│                        │                  │          │
│                │ https://avd.aquasec.com/nvd/cve-2023-25180
│
├────────────────────────┼──────────────────┤          │
├────────────────┼──────────────────────────────────────────────────────────────
──┤
│ libglib2.0-data        │ CVE-2023-24593   │          │
│                │ glib: DoS caused by handling a malicious text-form variant
│
│                        │                  │          │
│                │ https://avd.aquasec.com/nvd/cve-2023-24593
│
│                        ├──────────────────┤          │
├────────────────┼──────────────────────────────────────────────────────────────
──┤
│                        │ CVE-2023-25180   │          │
│                │ glib: DoS caused by malicious serialised variant
│
│                        │                  │          │
│                │ https://avd.aquasec.com/nvd/cve-2023-25180
│
├────────────────────────┼──────────────────┼──────────┼──────────────────────
```

```
┌──────────────────────────┬──────────────────┬──────────┬──────────────────────────────────────────
──────────────────────────┐
│ libncurses6              │ CVE-2022-29458   │          │ 6.3-2
│                 │ ncurses: segfaulting OOB read
│
│                          │                  │          │
│                 │ https://avd.aquasec.com/nvd/cve-2022-29458
│
├──────────────────────────┤                  │          │
├─────────────────┤
│
│ libncursesw6             │                  │          │
│                 │
│
│                          │                  │          │
│                 │
│
├──────────────────────────┼──────────────────┤
├──────────────────────────┼──────────────────┼──────────────────────────────────────────
──────────────────────────┘
│ libpcre3                 │ CVE-2017-11164   │          │
2:8.39-13ubuntu0.22.04.1 │                  │ pcre: OP_KETRMAX feature in the
match function in            │
│                          │                  │          │
│                 │ pcre_exec.c
│
│                          │                  │          │
│                 │ https://avd.aquasec.com/nvd/cve-2017-11164
│
├──────────────────────────┼──────────────────┼──────────┼──────────────────────────────────────────
──────┼──────────────────┼──────────────────────────────────────────────────────────────────────
──────┐
│ libpython3.10-minimal │ CVE-2023-24329   │ MEDIUM   │
3.10.6-1~22.04.2ubuntu1  │                  │ urllib.parse url blocklisting
bypass                          │
│                          │                  │          │
│                 │ https://avd.aquasec.com/nvd/cve-2023-24329
│
│                          ├──────────────────┤          │
├─────────────────┼──────────────────────────────────────────────────────────────────────────
──┤
│                          │ CVE-2023-27043   │          │
│                 │ Parsing errors in email/_parseaddr.py lead to incorrect
│
│                          │                  │          │
│                 │ value in email address part...
│
│                          │                  │          │
│                 │ https://avd.aquasec.com/nvd/cve-2023-27043
│
```

```
├──────────────────────────┼──────────────────┼──────────┼──────────────────────────
──────┼──────────────────┼──────────────────────────────────────────────────────────
──────┤
│ libsqlite3-0             │ CVE-2022-46908   │ LOW      │ 3.37.2-2ubuntu0.1
│                  │ sqlite: safe mode authorizer callback allows disallowed
UDFs │
│                          │                  │          │
│                  │ https://avd.aquasec.com/nvd/cve-2022-46908
│
├──────────────────────────┼──────────────────┤
├──────────────────────────┼──────────────────┼──────────────────────────────────
──────────────────────────┤
│ libssl3                  │ CVE-2023-1255    │          │ 3.0.2-0ubuntu1.9
│                  │ Input buffer over-read in AES-XTS implementation on 64 bit
│
│                          │                  │          │
│                  │ ARM
│
│                          │                  │          │
│                  │ https://avd.aquasec.com/nvd/cve-2023-1255
│
├──────────────────────────┼──────────────────┤
├──────────────────────────┼──────────────────┼──────────────────────────────────
──────────────────────────┤
│ libtinfo6                │ CVE-2022-29458   │          │ 6.3-2
│                  │ ncurses: segfaulting OOB read
│
│                          │                  │          │
│                  │ https://avd.aquasec.com/nvd/cve-2022-29458
│
├──────────────────────────┼──────────────────┤
├──────────────────────────┼──────────────────┼──────────────────────────────────
──────────────────────────┤
│ libzstd1                 │ CVE-2022-4899    │          │ 1.4.8+dfsg-3build1
│                  │ buffer overrun in util.c
│
│                          │                  │          │
│                  │ https://avd.aquasec.com/nvd/cve-2022-4899
│
├──────────────────────────┼──────────────────┤
├──────────────────────────┼──────────────────┼──────────────────────────────────
──────────────────────────┤
│ locales                  │ CVE-2016-20013   │          │ 2.35-0ubuntu3.1
│                  │ sha256crypt and sha512crypt through 0.6 allow attackers to
│
│                          │                  │          │
│                  │ cause a denial of...
│
│                          │                  │          │
│                  │ https://avd.aquasec.com/nvd/cve-2016-20013
│
```

```
├──────────────────────┼──────────────────┼──────────┼──────────────────────────────────────────────
──────────────────────┤
│ login                │ CVE-2023-29383   │          │ 1:4.8.1-2ubuntu2.1
│                      │ Improper input validation in shadow-utils package utility
│                      │                  │          │
│                      │ chfn
│                      │                  │          │
│                      │ https://avd.aquasec.com/nvd/cve-2023-29383
│                      │                  │          │
├──────────────────────┼──────────────────┼──────────┼──────────────────────────────────────────────
──────────────────────┤
│ ncurses-base         │ CVE-2022-29458   │          │ 6.3-2
│                      │ ncurses: segfaulting OOB read
│                      │                  │          │
│                      │ https://avd.aquasec.com/nvd/cve-2022-29458
│                      │                  │          │
├──────────────────────┤                  │          │
├──────────────────────┤
│ ncurses-bin          │                  │          │
│                      │
│                      │                  │          │
│                      │
│                      │                  │          │
├──────────────────────┤                  │          │
├──────────────────────┤
│ ncurses-term         │                  │          │
│                      │
│                      │                  │          │
│                      │
│                      │                  │          │
├──────────────────────┼──────────────────┼──────────┼──────────────────────────────────────────────
──────────────────────┤
│ openssh-client       │ CVE-2020-14145   │          │ 1:8.9p1-3ubuntu0.1
│                      │ openssh: Observable discrepancy leading to an information
│                      │                  │          │
│                      │ leak in the algorithm negotiation...
│                      │                  │          │
│                      │ https://avd.aquasec.com/nvd/cve-2020-14145
```

```
│                       ├──────────────────────┤          │
├──────────────┼──────────────────────────────────────────────────────────────
──┤
│                       │ CVE-2021-41617       │          │
│              │ openssh: privilege escalation when AuthorizedKeysCommand
or  │
│                       │                      │          │
│              │ AuthorizedPrincipalsCommand are configured
│
│                       │                      │          │
│              │ https://avd.aquasec.com/nvd/cve-2021-41617
│
│                       ├──────────────────────┤          │
├──────────────┼──────────────────────────────────────────────────────────────
──┤
│                       │ CVE-2023-28531       │          │
│              │ openssh: smartcard keys to ssh-agent without the intended
│
│                       │                      │          │
│              │ per-hop destination constraints.
│
│                       │                      │          │
│              │ https://avd.aquasec.com/nvd/cve-2023-28531
│
├──────────────────────┼──────────────────────┤          │
├──────────────┼──────────────────────────────────────────────────────────────
──┤
│ openssh-server       │ CVE-2020-14145       │          │
│              │ openssh: Observable discrepancy leading to an information
│
│                       │                      │          │
│              │ leak in the algorithm negotiation...
│
│                       │                      │          │
│              │ https://avd.aquasec.com/nvd/cve-2020-14145
│
│                       ├──────────────────────┤          │
├──────────────┼──────────────────────────────────────────────────────────────
──┤
│                       │ CVE-2021-41617       │          │
│              │ openssh: privilege escalation when AuthorizedKeysCommand
or  │
│                       │                      │          │
│              │ AuthorizedPrincipalsCommand are configured
│
│                       │                      │          │
│              │ https://avd.aquasec.com/nvd/cve-2021-41617
│
│                       ├──────────────────────┤          │
├──────────────┼──────────────────────────────────────────────────────────────
──┤
```

```
──┤
│                      │ CVE-2023-28531   │          │
│               │ openssh: smartcard keys to ssh-agent without the intended
│
│                      │                  │          │
│               │ per-hop destination constraints.
│
│                      │                  │          │
│               │ https://avd.aquasec.com/nvd/cve-2023-28531
│
├──────────────────────┼──────────────────┤          │
├──────────────┼──────────────────────────────────────────────────────────────
──┤
│ openssh-sftp-server  │ CVE-2020-14145   │          │
│               │ openssh: Observable discrepancy leading to an information
│
│                      │                  │          │
│               │ leak in the algorithm negotiation...
│
│                      │                  │          │
│               │ https://avd.aquasec.com/nvd/cve-2020-14145
│
│                      ├──────────────────┤          │
├──────────────┼──────────────────────────────────────────────────────────────
──┤
│                      │ CVE-2021-41617   │          │
│               │ openssh: privilege escalation when AuthorizedKeysCommand
or  │
│                      │                  │          │
│               │ AuthorizedPrincipalsCommand are configured
│
│                      │                  │          │
│               │ https://avd.aquasec.com/nvd/cve-2021-41617
│
│                      ├──────────────────┤          │
├──────────────┼──────────────────────────────────────────────────────────────
──┤
│                      │ CVE-2023-28531   │          │
│               │ openssh: smartcard keys to ssh-agent without the intended
│
│                      │                  │          │
│               │ per-hop destination constraints.
│
│                      │                  │          │
│               │ https://avd.aquasec.com/nvd/cve-2023-28531
│
├──────────────────────┼──────────────────┤
├──────────────────────┼──────────────────┼──────────────────────────────────
──────────────────────┤
│ openssl              │ CVE-2023-1255    │          │ 3.0.2-0ubuntu1.9
```

```
│                │ Input buffer over-read in AES-XTS implementation on 64 bit
│
│                       │                  │          │
│                │ ARM
│
│                       │                  │          │
│                │ https://avd.aquasec.com/nvd/cve-2023-1255
│
├───────────────────────┼──────────────────┤
├──────────────────────────┼──────────────────────────────────────────────────────
─────────────────────────────┤
│ passwd                │ CVE-2023-29383   │          │ 1:4.8.1-2ubuntu2.1
│                │ Improper input validation in shadow-utils package utility
│
│                       │                  │          │
│                │ chfn
│
│                       │                  │          │
│                │ https://avd.aquasec.com/nvd/cve-2023-29383
│
├───────────────────────┼──────────────────┼──────────┼──────────────────────────
─────┼───────────────┼────────────────────────────────────────────────────────
────────┤
│ python3.10-minimal    │ CVE-2023-24329   │ MEDIUM   │
3.10.6-1~22.04.2ubuntu1  │               │ urllib.parse url blocklisting
bypass                                │
│                       │                  │          │
│                │ https://avd.aquasec.com/nvd/cve-2023-24329
│
│                       ├──────────────────┤          │
├────────────────┼────────────────────────────────────────────────────────────────
───┤
│                       │ CVE-2023-27043   │          │
│                │ Parsing errors in email/_parseaddr.py lead to incorrect
│
│                       │                  │          │
│                │ value in email address part...
│
│                       │                  │          │
│                │ https://avd.aquasec.com/nvd/cve-2023-27043
│
├───────────────────────┼──────────────────┼──────────┼──────────────────────────
─────┼───────────────┼────────────────────────────────────────────────────────
────────┤
│ sqlite3               │ CVE-2022-46908   │ LOW      │ 3.37.2-2ubuntu0.1
│                │ sqlite: safe mode authorizer callback allows disallowed
UDFs │
│                       │                  │          │
│                │ https://avd.aquasec.com/nvd/cve-2022-46908
│
├───────────────────────┼──────────────────┤
```

```
┌──────────────────────────┬──────────────────┬──────────┬──────────────────────────────────────────────
──────────────────────────┐
│ ssh                      │ CVE-2020-14145   │          │ 1:8.9p1-3ubuntu0.1
│                          │ openssh: Observable discrepancy leading to an information
│
│                          │                  │          │
│                          │ leak in the algorithm negotiation...
│
│                          │                  │          │
│                          │ https://avd.aquasec.com/nvd/cve-2020-14145
│
│                          ├──────────────────┤          │
├──────────────────────────┼──────────────────────────────────────────────────────────────────────────
──┤
│                          │ CVE-2021-41617   │          │
│                          │ openssh: privilege escalation when AuthorizedKeysCommand
or  │
│                          │                  │          │
│                          │ AuthorizedPrincipalsCommand are configured
│
│                          │                  │          │
│                          │ https://avd.aquasec.com/nvd/cve-2021-41617
│
│                          ├──────────────────┤          │
├──────────────────────────┼──────────────────────────────────────────────────────────────────────────
──┤
│                          │ CVE-2023-28531   │          │
│                          │ openssh: smartcard keys to ssh-agent without the intended
│
│                          │                  │          │
│                          │ per-hop destination constraints.
│
│                          │                  │          │
│                          │ https://avd.aquasec.com/nvd/cve-2023-28531
│
├──────────────────────────┼──────────────────┼──────────┤
├──────────────────────────┼──────────────────┼──────────┼──────────────────────────────────────────────
──────────────────────────┘
│ udhcpc                   │ CVE-2022-28391   │          │ 1:1.30.1-7ubuntu3
│                          │ busybox: remote attackers may execute arbitrary code if
│
│                          │                  │          │
│                          │ netstat is used
│
│                          │                  │          │
│                          │ https://avd.aquasec.com/nvd/cve-2022-28391
│
├──────────────────────────┼──────────────────┼──────────┼──────────┬──────────────────────────────────
──────────────────────────┐
└──────────────────────────┴──────────────────┴──────────┴──────────┴──────────────────────────────────
──────────────────────────┘
```

```
| vim-common             | CVE-2022-0128    | MEDIUM   |
2:8.2.3995-1ubuntu2.7    |                  | vim: a heap-based OOB read of
size 1                          |
|                        |                  |          |
|                | https://avd.aquasec.com/nvd/cve-2022-0128
|
|                        |                  |          |
|------------------------|------------------------------------------------------------
----|
|                        | CVE-2022-0156    |          |
|                | vim: use-after-free while treating allocated lines in user
|
|                        |                  |          |
|                | functions
|
|                        |                  |          |
|                | https://avd.aquasec.com/nvd/cve-2022-0156
|
|                        |                  |          |
|------------------------|------------------------------------------------------------
----|
|                        | CVE-2022-0158    |          |
|                | vim: heap-based read buffer overflow in compile_get_env()
|
|                        |                  |          |
|                | https://avd.aquasec.com/nvd/cve-2022-0158
|
|                        |                  |          |
|------------------------|------------------------------------------------------------
----|
|                        | CVE-2022-0393    |          |
|                | vim: out-of-bounds read in delete_buff_tail() in getchar.c
|
|                        |                  |          |
|                | https://avd.aquasec.com/nvd/cve-2022-0393
|
|                        |                  |          |
|------------------------|------------------------------------------------------------
----|
|                        | CVE-2022-0407    |          |
|                | vim: heap-based buffer overflow on read in yank_copy_line
|
|                        |                  |          |
|                | https://avd.aquasec.com/nvd/cve-2022-0407
|
|                        |                  |          |
|------------------------|------------------------------------------------------------
----|
|                        | CVE-2022-2182    |          |
|                | vim: heap-based buffer overflow through
parse_cmd_address()  |
```

```
│                       │                    │          │
│                 │ in function utf_ptr2char
│                       │                    │          │
│                 │ https://avd.aquasec.com/nvd/cve-2022-2182
│                       ├────────────────────┤          │
├─────────────────┼─────────────────────────────────────────────────────────
──┤
│                       │ CVE-2022-2343      │          │
│                 │ vim: heap-based buffer overflow in ins_compl_add() in
│                       │                    │          │
│                 │ insexpand.c
│                       │                    │          │
│                 │ https://avd.aquasec.com/nvd/cve-2022-2343
│                       ├────────────────────┤          │
├─────────────────┼─────────────────────────────────────────────────────────
──┤
│                       │ CVE-2022-2862      │          │
│                 │ vim: heap use-after-free in generate_PCALL() at
│                       │                    │          │
│                 │ src/vim9instr.c
│                       │                    │          │
│                 │ https://avd.aquasec.com/nvd/cve-2022-2862
│                       ├────────────────────┤          │
├─────────────────┼─────────────────────────────────────────────────────────
──┤
│                       │ CVE-2022-2889      │          │
│                 │ vim: use-after-free in find_var_also_in_script() in
│                       │                    │          │
│                 │ evalvars.c
│                       │                    │          │
│                 │ https://avd.aquasec.com/nvd/cve-2022-2889
│                       ├────────────────────┤          │
├─────────────────┼─────────────────────────────────────────────────────────
──┤
│                       │ CVE-2022-2982      │          │
│                 │ vim: use after free in qf_fill_buffer() at src/quickfix.c
│                       │                    │          │
│                 │ https://avd.aquasec.com/nvd/cve-2022-2982
```

```
│                       ├──────────────────────┼──────────┤
├──────────────────┼──────────────────────────────────────────────────────────
──┤
│                       │ CVE-2022-0696        │ LOW      │
│                  │ vim: NULL Pointer Dereference in vim prior to 8.2
│                       │                      │          │
│                  │ https://avd.aquasec.com/nvd/cve-2022-0696
│                       ├──────────────────────┤          │
├──────────────────┼──────────────────────────────────────────────────────────
──┤
│                       │ CVE-2022-1886        │          │
│                  │ vim: heap-based buffer overflow in function utf_head_off
│                       │                      │          │
│                  │ https://avd.aquasec.com/nvd/cve-2022-1886
│                       │                      │          │
├──────────────────┼──────────────────────┼──────────┤
├──────────────────┼──────────────────────────────────────────────────────────
──┤
│ vim-tiny              │ CVE-2022-0128        │ MEDIUM   │
│                  │ vim: a heap-based OOB read of size 1
│                       │                      │          │
│                  │ https://avd.aquasec.com/nvd/cve-2022-0128
│                       ├──────────────────────┤          │
├──────────────────┼──────────────────────────────────────────────────────────
──┤
│                       │ CVE-2022-0156        │          │
│                  │ vim: use-after-free while treating allocated lines in user
│                       │                      │          │
│                  │ functions
│                       │                      │          │
│                  │ https://avd.aquasec.com/nvd/cve-2022-0156
│                       ├──────────────────────┤          │
├──────────────────┼──────────────────────────────────────────────────────────
──┤
│                       │ CVE-2022-0158        │          │
│                  │ vim: heap-based read buffer overflow in compile_get_env()
│                       │                      │          │
│                  │ https://avd.aquasec.com/nvd/cve-2022-0158
│                       ├──────────────────────┤          │
├──────────────────┼──────────────────────────────────────────────────────────
```

```
──┤
│                    │ CVE-2022-0393    │          │
│               │ vim: out-of-bounds read in delete_buff_tail() in getchar.c
│
│                    │                  │          │
│               │ https://avd.aquasec.com/nvd/cve-2022-0393
│
│                    ├──────────────────┤          │
├──────────────┼──────────────────────────────────────────────────────────────
──┤
│                    │ CVE-2022-0407    │          │
│               │ vim: heap-based buffer overflow on read in yank_copy_line
│
│                    │                  │          │
│               │ https://avd.aquasec.com/nvd/cve-2022-0407
│
│                    ├──────────────────┤          │
├──────────────┼──────────────────────────────────────────────────────────────
──┤
│                    │ CVE-2022-2182    │          │
│               │ vim: heap-based buffer overflow through
parse_cmd_address()  │
│                    │                  │          │
│               │ in function utf_ptr2char
│
│                    │                  │          │
│               │ https://avd.aquasec.com/nvd/cve-2022-2182
│
│                    ├──────────────────┤          │
├──────────────┼──────────────────────────────────────────────────────────────
──┤
│                    │ CVE-2022-2343    │          │
│               │ vim: heap-based buffer overflow in ins_compl_add() in
│
│                    │                  │          │
│               │ insexpand.c
│
│                    │                  │          │
│               │ https://avd.aquasec.com/nvd/cve-2022-2343
│
│                    ├──────────────────┤          │
├──────────────┼──────────────────────────────────────────────────────────────
──┤
│                    │ CVE-2022-2862    │          │
│               │ vim: heap use-after-free in generate_PCALL() at
│
│                    │                  │          │
│               │ src/vim9instr.c
│
│                    │                  │          │
```

```
│                │ https://avd.aquasec.com/nvd/cve-2022-2862
│
│                       ├──────────────────┤          │
├────────────────┼──────────────────────────────────────────────────────────────
──┤
│                       │ CVE-2022-2889    │          │
│                │ vim: use-after-free in find_var_also_in_script() in
│
│                       │                  │          │
│                │ evalvars.c
│
│                       │                  │          │
│                │ https://avd.aquasec.com/nvd/cve-2022-2889
│
│                       ├──────────────────┤          │
├────────────────┼──────────────────────────────────────────────────────────────
──┤
│                       │ CVE-2022-2982    │          │
│                │ vim: use after free in qf_fill_buffer() at src/quickfix.c
│
│                       │                  │          │
│                │ https://avd.aquasec.com/nvd/cve-2022-2982
│
│                       ├──────────────────┼──────────┤
├────────────────┼──────────────────────────────────────────────────────────────
──┤
│                       │ CVE-2022-0696    │ LOW      │
│                │ vim: NULL Pointer Dereference in vim prior to 8.2
│
│                       │                  │          │
│                │ https://avd.aquasec.com/nvd/cve-2022-0696
│
│                       ├──────────────────┤          │
├────────────────┼──────────────────────────────────────────────────────────────
──┤
│                       │ CVE-2022-1886    │          │
│                │ vim: heap-based buffer overflow in function utf_head_off
│
│                       │                  │          │
│                │ https://avd.aquasec.com/nvd/cve-2022-1886
│
├────────────────────────┼──────────────────┼──────────┼──────────────────────
──┼──────────────────┼──────────────────────────────────────────────────────────
──┤
│ wget                   │ CVE-2021-31879   │ MEDIUM   │ 1.21.2-2ubuntu1
│                │ wget: authorization header disclosure on redirect
│
│                       │                  │          │
│                │ https://avd.aquasec.com/nvd/cve-2021-31879
│
├────────────────────────┼──────────────────┤
```

```
├──────────────────────────┼──────────────────┼──────────────────────────────────────────────────────────────
──────────────────────────┤
│ xxd                      │ CVE-2022-0128    │                  │
2:8.2.3995-1ubuntu2.7    │                  │ vim: a heap-based OOB read of
size 1                          │
│                          │                  │                  │
│                  │ https://avd.aquasec.com/nvd/cve-2022-0128
│
│                          ├──────────────────┤                  │
├──────────────────┼──────────────────────────────────────────────────────────────────────────────────────
──┤
│                          │ CVE-2022-0156    │                  │
│                  │ vim: use-after-free while treating allocated lines in user
│
│                          │                  │                  │
│                  │ functions
│
│                          │                  │                  │
│                  │ https://avd.aquasec.com/nvd/cve-2022-0156
│
│                          ├──────────────────┤                  │
├──────────────────┼──────────────────────────────────────────────────────────────────────────────────────
──┤
│                          │ CVE-2022-0158    │                  │
│                  │ vim: heap-based read buffer overflow in compile_get_env()
│
│                          │                  │                  │
│                  │ https://avd.aquasec.com/nvd/cve-2022-0158
│
│                          ├──────────────────┤                  │
├──────────────────┼──────────────────────────────────────────────────────────────────────────────────────
──┤
│                          │ CVE-2022-0393    │                  │
│                  │ vim: out-of-bounds read in delete_buff_tail() in getchar.c
│
│                          │                  │                  │
│                  │ https://avd.aquasec.com/nvd/cve-2022-0393
│
│                          ├──────────────────┤                  │
├──────────────────┼──────────────────────────────────────────────────────────────────────────────────────
──┤
│                          │ CVE-2022-0407    │                  │
│                  │ vim: heap-based buffer overflow on read in yank_copy_line
│
│                          │                  │                  │
│                  │ https://avd.aquasec.com/nvd/cve-2022-0407
│
│                          ├──────────────────┤                  │
├──────────────────┼──────────────────────────────────────────────────────────────────────────────────────
──┤
```

```
│                       │ CVE-2022-2182    │          │
│               │ vim: heap-based buffer overflow through
parse_cmd_address()  │
│                       │                  │          │
│               │ in function utf_ptr2char
│
│                       │                  │          │
│               │ https://avd.aquasec.com/nvd/cve-2022-2182
│
│                       ├──────────────────┤          │
├───────────────┼──────────────────────────────────────────────────────────────
──┤
│                       │ CVE-2022-2343    │          │
│               │ vim: heap-based buffer overflow in ins_compl_add() in
│
│                       │                  │          │
│               │ insexpand.c
│
│                       │                  │          │
│               │ https://avd.aquasec.com/nvd/cve-2022-2343
│
│                       ├──────────────────┤          │
├───────────────┼──────────────────────────────────────────────────────────────
──┤
│                       │ CVE-2022-2862    │          │
│               │ vim: heap use-after-free in generate_PCALL() at
│
│                       │                  │          │
│               │ src/vim9instr.c
│
│                       │                  │          │
│               │ https://avd.aquasec.com/nvd/cve-2022-2862
│
│                       ├──────────────────┤          │
├───────────────┼──────────────────────────────────────────────────────────────
──┤
│                       │ CVE-2022-2889    │          │
│               │ vim: use-after-free in find_var_also_in_script() in
│
│                       │                  │          │
│               │ evalvars.c
│
│                       │                  │          │
│               │ https://avd.aquasec.com/nvd/cve-2022-2889
│
│                       ├──────────────────┤          │
├───────────────┼──────────────────────────────────────────────────────────────
──┤
│                       │ CVE-2022-2982    │          │
│               │ vim: use after free in qf_fill_buffer() at src/quickfix.c
│
```

```
│                        │                   │           │
│               │ https://avd.aquasec.com/nvd/cve-2022-2982
│
│                        ├───────────────────┼───────────┤
├───────────────┼────────────────────────────────────────────────────────────────────────────
───┤
│                        │ CVE-2022-0696     │ LOW       │
│               │ vim: NULL Pointer Dereference in vim prior to 8.2
│
│                        │                   │           │
│               │ https://avd.aquasec.com/nvd/cve-2022-0696
│
│                        ├───────────────────┤           │
├───────────────┼────────────────────────────────────────────────────────────────────────────
───┤
│                        │ CVE-2022-1886     │           │
│               │ vim: heap-based buffer overflow in function utf_head_off
│
│                        │                   │           │
│               │ https://avd.aquasec.com/nvd/cve-2022-1886
│
├────────────────────────┼───────────────────┤
├───────────────────────────┼────────────────┼───────────────────────────────────────────────
──────────────────────────────┤
│ zstd                   │ CVE-2022-4899     │           │ 1.4.8+dfsg-3build1
│               │ buffer overrun in util.c
│
│                        │                   │           │
│               │ https://avd.aquasec.com/nvd/cve-2022-4899
│
└────────────────────────┴───────────────────┴───────────┴───────────────────────────────────
─────┴────────────────┴──────────────────────────────────────────────────────────────────────
────────┘
```

参考

SBOM などに関する参考になる情報を載せたサイトです。

- 開発に使える脆弱性スキャンツール - NTT Communications Engineers' Blog