

# 目次

<b>Trivy を使用して SBOM を作成する</b> .....	1
<b>Trivy のインストール</b> .....	1
<b>root filesystem から SBOM を生成</b> .....	2
<b>SBOM ファイルをスキャンして脆弱性のレポート作成</b> .....	4
<b>参考</b> .....	24



# 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 行分を見てください。

```
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 Fixed Version	Vulnerability Title	Severity	Installed Version
bash	CVE-2022-3715 a heap-buffer-overflow in valid_parameter_transform	LOW	5.1-6ubuntu1
	<a href="https://avd.aquasec.com/nvd/cve-2022-3715">https://avd.aquasec.com/nvd/cve-2022-3715</a>		

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

read\_n() |

| CVE-2016-9917  
| bluez: Heap-based buffer overflow vulnerability in

| <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: BLESAs bluetooth attack	
	<a href="https://avd.aquasec.com/nvd/cve-2020-9770">https://avd.aquasec.com/nvd/cve-2020-9770</a>	
	CVE-2022-3563	
	bluez: NULL pointer dereference in	
	read_50_controller_cap_complete() in tools/mgmt-tester.c	
	<a href="https://avd.aquasec.com/nvd/cve-2022-3563">https://avd.aquasec.com/nvd/cve-2022-3563</a>	
busybox	CVE-2022-28391	1:1.30.1-7ubuntu3
	busybox: remote attackers may execute arbitrary code if	
	netstat is used	
	<a href="https://avd.aquasec.com/nvd/cve-2022-28391">https://avd.aquasec.com/nvd/cve-2022-28391</a>	
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
using	gnupg: denial of service issue (resource consumption)	
	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 .....		
	<a href="https://avd.aquasec.com/nvd/cve-2018-1000215">https://avd.aquasec.com/nvd/cve-2018-1000215</a>		
libglib2.0-0	CVE-2023-24593	LOW	2.72.4-0ubuntu2
	glib: DoS caused by handling a malicious text-form variant		
	<a href="https://avd.aquasec.com/nvd/cve-2023-24593">https://avd.aquasec.com/nvd/cve-2023-24593</a>		
	CVE-2023-25180		
	glib: DoS caused by malicious serialised variant		
	<a href="https://avd.aquasec.com/nvd/cve-2023-25180">https://avd.aquasec.com/nvd/cve-2023-25180</a>		
libglib2.0-data	CVE-2023-24593		
	glib: DoS caused by handling a malicious text-form variant		
	<a href="https://avd.aquasec.com/nvd/cve-2023-24593">https://avd.aquasec.com/nvd/cve-2023-24593</a>		
	CVE-2023-25180		
	glib: DoS caused by malicious serialised variant		
	<a href="https://avd.aquasec.com/nvd/cve-2023-25180">https://avd.aquasec.com/nvd/cve-2023-25180</a>		

libncurses6	CVE-2022-29458	6.3-2
ncurses: segfaulting 00B read		
<a href="https://avd.aquasec.com/nvd/cve-2022-29458">https://avd.aquasec.com/nvd/cve-2022-29458</a>		
libncursesw6		
libpcre3	CVE-2017-11164	
2:8.39-13ubuntu0.22.04.1		pcre: OP_KETRMATCH feature in the match function in
pcre_exec.c		
<a href="https://avd.aquasec.com/nvd/cve-2017-11164">https://avd.aquasec.com/nvd/cve-2017-11164</a>		
libpython3.10-minimal	CVE-2023-24329	MEDIUM
3.10.6-1~22.04.2ubuntu1		urllib.parse url blocklisting bypass
<a href="https://avd.aquasec.com/nvd/cve-2023-24329">https://avd.aquasec.com/nvd/cve-2023-24329</a>		
	CVE-2023-27043	
Parsing errors in email/_parseaddr.py lead to incorrect		
value in email address part...		
<a href="https://avd.aquasec.com/nvd/cve-2023-27043">https://avd.aquasec.com/nvd/cve-2023-27043</a>		

libsqlite3-0	CVE-2022-46908	LOW	3.37.2-2ubuntu0.1
sqlite: safe mode authorizer callback allows disallowed UDFs			
<a href="https://avd.aquasec.com/nvd/cve-2022-46908">https://avd.aquasec.com/nvd/cve-2022-46908</a>			
libssl3	CVE-2023-1255		3.0.2-0ubuntu1.9
Input buffer over-read in AES-XTS implementation on 64 bit ARM			
<a href="https://avd.aquasec.com/nvd/cve-2023-1255">https://avd.aquasec.com/nvd/cve-2023-1255</a>			
libtinfo6	CVE-2022-29458		6.3-2
ncurses: segfaulting 00B read			
<a href="https://avd.aquasec.com/nvd/cve-2022-29458">https://avd.aquasec.com/nvd/cve-2022-29458</a>			
libzstd1	CVE-2022-4899		1.4.8+dfsg-3build1
buffer overrun in util.c			
<a href="https://avd.aquasec.com/nvd/cve-2022-4899">https://avd.aquasec.com/nvd/cve-2022-4899</a>			
locales	CVE-2016-20013		2.35-0ubuntu3.1
sha256crypt and sha512crypt through 0.6 allow attackers to cause a denial of...			
<a href="https://avd.aquasec.com/nvd/cve-2016-20013">https://avd.aquasec.com/nvd/cve-2016-20013</a>			

login	CVE-2023-29383	1:4.8.1-2ubuntu2.1
Improper input validation in shadow-utils package utility		
chfn		
<a href="https://avd.aquasec.com/nvd/cve-2023-29383">https://avd.aquasec.com/nvd/cve-2023-29383</a>		
ncurses-base	CVE-2022-29458	6.3-2
ncurses: segfaulting 00B read		
<a href="https://avd.aquasec.com/nvd/cve-2022-29458">https://avd.aquasec.com/nvd/cve-2022-29458</a>		
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...		
<a href="https://avd.aquasec.com/nvd/cve-2020-14145">https://avd.aquasec.com/nvd/cve-2020-14145</a>		

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

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



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

ssh	CVE-2020-14145	1:8.9p1-3ubuntu0.1
openssh: Observable discrepancy leading to an information		
leak in the algorithm negotiation...		
<a href="https://avd.aquasec.com/nvd/cve-2020-14145">https://avd.aquasec.com/nvd/cve-2020-14145</a>		
or	CVE-2021-41617	
openssh: privilege escalation when AuthorizedKeysCommand		
AuthorizedPrincipalsCommand are configured		
<a href="https://avd.aquasec.com/nvd/cve-2021-41617">https://avd.aquasec.com/nvd/cve-2021-41617</a>		
	CVE-2023-28531	
openssh: smartcard keys to ssh-agent without the intended		
per-hop destination constraints.		
<a href="https://avd.aquasec.com/nvd/cve-2023-28531">https://avd.aquasec.com/nvd/cve-2023-28531</a>		
udhcpd	CVE-2022-28391	1:1.30.1-7ubuntu3
busybox: remote attackers may execute arbitrary code if		
netstat is used		
<a href="https://avd.aquasec.com/nvd/cve-2022-28391">https://avd.aquasec.com/nvd/cve-2022-28391</a>		

vim-common 2:8.2.3995-1ubuntu2.7	CVE-2022-0128	MEDIUM vim: a heap-based 00B read of size 1
		<a href="https://avd.aquasec.com/nvd/cve-2022-0128">https://avd.aquasec.com/nvd/cve-2022-0128</a>
	CVE-2022-0156	vim: use-after-free while treating allocated lines in user functions
		<a href="https://avd.aquasec.com/nvd/cve-2022-0156">https://avd.aquasec.com/nvd/cve-2022-0156</a>
	CVE-2022-0158	vim: heap-based read buffer overflow in compile_get_env()
		<a href="https://avd.aquasec.com/nvd/cve-2022-0158">https://avd.aquasec.com/nvd/cve-2022-0158</a>
	CVE-2022-0393	vim: out-of-bounds read in delete_buff_tail() in getchar.c
		<a href="https://avd.aquasec.com/nvd/cve-2022-0393">https://avd.aquasec.com/nvd/cve-2022-0393</a>
	CVE-2022-0407	vim: heap-based buffer overflow on read in yank_copy_line
		<a href="https://avd.aquasec.com/nvd/cve-2022-0407">https://avd.aquasec.com/nvd/cve-2022-0407</a>
	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		
		<a href="https://avd.aquasec.com/nvd/cve-2022-0696">https://avd.aquasec.com/nvd/cve-2022-0696</a>		
		CVE-2022-1886		
	vim:	heap-based buffer overflow in function utf_head_off		
		<a href="https://avd.aquasec.com/nvd/cve-2022-1886">https://avd.aquasec.com/nvd/cve-2022-1886</a>		
vim-tiny		CVE-2022-0128	MEDIUM	
	vim:	a heap-based 00B read of size 1		
		<a href="https://avd.aquasec.com/nvd/cve-2022-0128">https://avd.aquasec.com/nvd/cve-2022-0128</a>		
		CVE-2022-0156		
	vim:	use-after-free while treating allocated lines in user functions		
		<a href="https://avd.aquasec.com/nvd/cve-2022-0156">https://avd.aquasec.com/nvd/cve-2022-0156</a>		
		CVE-2022-0158		
	vim:	heap-based read buffer overflow in compile_get_env()		
		<a href="https://avd.aquasec.com/nvd/cve-2022-0158">https://avd.aquasec.com/nvd/cve-2022-0158</a>		

```
| 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 |
```

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

xxd 2:8.2.3995-1ubuntu2.7 size 1	CVE-2022-0128	vim: a heap-based 00B read of size 1
	<a href="https://avd.aquasec.com/nvd/cve-2022-0128">https://avd.aquasec.com/nvd/cve-2022-0128</a>	
	CVE-2022-0156	vim: use-after-free while treating allocated lines in user functions
	<a href="https://avd.aquasec.com/nvd/cve-2022-0156">https://avd.aquasec.com/nvd/cve-2022-0156</a>	
	CVE-2022-0158	vim: heap-based read buffer overflow in compile_get_env()
	<a href="https://avd.aquasec.com/nvd/cve-2022-0158">https://avd.aquasec.com/nvd/cve-2022-0158</a>	
	CVE-2022-0393	vim: out-of-bounds read in delete_buff_tail() in getchar.c
	<a href="https://avd.aquasec.com/nvd/cve-2022-0393">https://avd.aquasec.com/nvd/cve-2022-0393</a>	
	CVE-2022-0407	vim: heap-based buffer overflow on read in yank_copy_line
	<a href="https://avd.aquasec.com/nvd/cve-2022-0407">https://avd.aquasec.com/nvd/cve-2022-0407</a>	



	CVE-2022-2182	
parse_cmd_address()	vim: heap-based buffer overflow through	
	in function utf_ptr2char	
	<a href="https://avd.aquasec.com/nvd/cve-2022-2182">https://avd.aquasec.com/nvd/cve-2022-2182</a>	
	CVE-2022-2343	
	vim: heap-based buffer overflow in ins_compl_add() in	
	insexpand.c	
	<a href="https://avd.aquasec.com/nvd/cve-2022-2343">https://avd.aquasec.com/nvd/cve-2022-2343</a>	
	CVE-2022-2862	
	vim: heap use-after-free in generate_PCALL() at	
	src/vim9instr.c	
	<a href="https://avd.aquasec.com/nvd/cve-2022-2862">https://avd.aquasec.com/nvd/cve-2022-2862</a>	
	CVE-2022-2889	
	vim: use-after-free in find_var_also_in_script() in	
	evalvars.c	
	<a href="https://avd.aquasec.com/nvd/cve-2022-2889">https://avd.aquasec.com/nvd/cve-2022-2889</a>	
	CVE-2022-2982	
	vim: use after free in qf_fill_buffer() at src/quickfix.c	

		<a href="https://avd.aquasec.com/nvd/cve-2022-2982">https://avd.aquasec.com/nvd/cve-2022-2982</a>	
	CVE-2022-0696	LOW	
	vim: NULL Pointer Dereference in vim prior to 8.2		
		<a href="https://avd.aquasec.com/nvd/cve-2022-0696">https://avd.aquasec.com/nvd/cve-2022-0696</a>	
	CVE-2022-1886		
	vim: heap-based buffer overflow in function utf_head_off		
		<a href="https://avd.aquasec.com/nvd/cve-2022-1886">https://avd.aquasec.com/nvd/cve-2022-1886</a>	
zstd	CVE-2022-4899		1.4.8+dfsg-3build1
	buffer overrun in util.c		
		<a href="https://avd.aquasec.com/nvd/cve-2022-4899">https://avd.aquasec.com/nvd/cve-2022-4899</a>	

## 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](#)

From:

<https://ma-tech.centurysys.jp/> - MA-X/MA-S/MA-E/IP-K Developers' Wiki

Permanent link:

[https://ma-tech.centurysys.jp/doku.php?id=ma\\_series\\_tips:create\\_sbom:start](https://ma-tech.centurysys.jp/doku.php?id=ma_series_tips:create_sbom:start)

Last update: 2023/05/10 09:25

