```
2022-10-30T02:35:55.0434949Z ##[section]Starting: Ejecutando análisis de
imagen con Trivy
2022-10-30T02:35:55.0443884Z
==============================================================================
=====
2022-10-30T02:35:55.0444249Z Task         : Command line
2022-10-30T02:35:55.0463475Z Description  : Run a command line script
using Bash on Linux and macOS and cmd.exe on Windows
2022-10-30T02:35:55.0463903Z Version      : 2.201.1
2022-10-30T02:35:55.0464162Z Author       : Microsoft Corporation
2022-10-30T02:35:55.0464537Z Help         :
https://docs.microsoft.com/azure/devops/pipelines/tasks/utility/command-
line
2022-10-30T02:35:55.0465026Z
==============================================================================
=====
2022-10-30T02:35:55.1818374Z Generating script.
2022-10-30T02:35:55.1825927Z ========================== Starting Command
Output ===========================
2022-10-30T02:35:55.1848908Z [command]/usr/bin/bash --noprofile --norc
/home/vsts/work/_temp/34bd3eac-b3a0-4522-9a1a-0b5040efbbcc.sh
2022-10-30T02:35:55.2558814Z Reading package lists...
2022-10-30T02:35:55.4493631Z Building dependency tree...
2022-10-30T02:35:55.4516642Z Reading state information...
2022-10-30T02:35:55.6223786Z rpm is already the newest version
(4.14.2.1+dfsg1-1build2).
2022-10-30T02:35:55.7190440Z 0 upgraded, 0 newly installed, 0 to remove
and 20 not upgraded.
2022-10-30T02:35:55.8045576Z --2022-10-30 02:35:55--
https://github.com/aquasecurity/trivy/releases/download/v0.27.1/trivy_0.2
7.1_Linux-64bit.deb
2022-10-30T02:35:55.8088908Z Resolving github.com (github.com)...
20.201.28.151
2022-10-30T02:35:55.8097981Z Connecting to github.com
(github.com)|20.201.28.151|:443... connected.
2022-10-30T02:35:55.9937890Z HTTP request sent, awaiting response... 302
Found
2022-10-30T02:35:55.9941972Z Location:
https://objects.githubusercontent.com/github-production-release-asset-
2e65be/180687624/d22923f2-8a51-4914-b1bf-074ab64f2e51?X-Amz-
Algorithm=AWS4-HMAC-SHA256&X-Amz-
Credential=AKIAIWNJYAX4CSVEH53A%2F20221030%2Fus-east-
1%2Fs3%2Faws4_request&X-Amz-Date=20221030T023555Z&X-Amz-Expires=300&X-
Amz-
Signature=e9e34b5924bb05e4ad2119d9cfae46612f9a787a916565e321d93aaa6018fd2
8&X-Amz-
SignedHeaders=host&actor_id=0&key_id=0&repo_id=180687624&response-
content-disposition=attachment%3B%20filename%3Dtrivy_0.27.1_Linux-
64bit.deb&response-content-type=application%2Foctet-stream [following]
2022-10-30T02:35:55.9945878Z --2022-10-30 02:35:55--
https://objects.githubusercontent.com/github-production-release-asset-
2e65be/180687624/d22923f2-8a51-4914-b1bf-074ab64f2e51?X-Amz-
Algorithm=AWS4-HMAC-SHA256&X-Amz-
Credential=AKIAIWNJYAX4CSVEH53A%2F20221030%2Fus-east-
1%2Fs3%2Faws4_request&X-Amz-Date=20221030T023555Z&X-Amz-Expires=300&X-
Amz-
Signature=e9e34b5924bb05e4ad2119d9cfae46612f9a787a916565e321d93aaa6018fd2
```

```
8&X-Amz-
SignedHeaders=host&actor_id=0&key_id=0&repo_id=180687624&response-
content-disposition=attachment%3B%20filename%3Dtrivy_0.27.1_Linux-
64bit.deb&response-content-type=application%2Foctet-stream
2022-10-30T02:35:56.1297111Z Resolving objects.githubusercontent.com
(objects.githubusercontent.com)... 185.199.109.133, 185.199.110.133,
185.199.111.133, ...
2022-10-30T02:35:56.1317734Z Connecting to objects.githubusercontent.com
(objects.githubusercontent.com)|185.199.109.133|:443... connected.
2022-10-30T02:35:56.8422693Z HTTP request sent, awaiting response... 200
OK
2022-10-30T02:35:56.8423981Z Length: 16498508 (16M) [application/octet-
stream]
2022-10-30T02:35:56.8424658Z Saving to: ‘trivy_0.27.1_Linux-64bit.deb’
2022-10-30T02:35:56.8424868Z
2022-10-30T02:35:57.0713215Z      0K .......... .......... ..........
.......... ..........  0%  217K 74s
2022-10-30T02:35:57.0723298Z     50K .......... .......... ..........
.......... ..........  0% 28.6M 37s
2022-10-30T02:35:57.1975378Z    100K .......... .......... ..........
.......... ..........  0%  400K 38s
2022-10-30T02:35:57.1976148Z    150K .......... .......... ..........
.......... ..........  1%  179M 28s
2022-10-30T02:35:57.3208508Z    200K .......... .......... ..........
.......... ..........  1%  407K 30s
2022-10-30T02:35:57.3209264Z    250K .......... .......... ..........
.......... ..........  1%  176M 25s
2022-10-30T02:35:57.3210252Z    300K .......... .......... ..........
.......... ..........  2%  208M 22s
2022-10-30T02:35:57.4179493Z    350K .......... .......... ..........
.......... ..........  2%  520K 23s
2022-10-30T02:35:57.4180237Z    400K .......... .......... ..........
.......... ..........  2%  179M 20s
2022-10-30T02:35:57.4180794Z    450K .......... .......... ..........
.......... ..........  3%  208M 18s
2022-10-30T02:35:57.4181344Z    500K .......... .......... ..........
.......... ..........  3%  219M 16s
2022-10-30T02:35:57.5323852Z    550K .......... .......... ..........
.......... ..........  3%  442K 18s
2022-10-30T02:35:57.5324548Z    600K .......... .......... ..........
.......... ..........  4%  140M 16s
2022-10-30T02:35:57.5325067Z    650K .......... .......... ..........
.......... ..........  4%  212M 15s
2022-10-30T02:35:57.5325570Z    700K .......... .......... ..........
.......... ..........  4%  215M 14s
2022-10-30T02:35:57.5326117Z    750K .......... .......... ..........
.......... ..........  4%  178M 13s
2022-10-30T02:35:57.5326630Z    800K .......... .......... ..........
.......... ..........  5%  194M 12s
2022-10-30T02:35:57.6468361Z    850K .......... .......... ..........
.......... ..........  5%  443K 14s
2022-10-30T02:35:57.6469083Z    900K .......... .......... ..........
.......... ..........  5%  181M 13s
2022-10-30T02:35:57.6469645Z    950K .......... .......... ..........
.......... ..........  6%  188M 12s
2022-10-30T02:35:57.6470198Z   1000K .......... .......... ..........
.......... ..........  6%  177M 12s
```

```
2022-10-30T02:35:57.6470751Z   1050K .......... .......... ..........
.......... ..........  6%  197M 11s
2022-10-30T02:35:57.6471298Z   1100K .......... .......... ..........
.......... ..........  7%  196M 10s
2022-10-30T02:35:57.6471849Z   1150K .......... .......... ..........
.......... ..........  7%  222M 10s
2022-10-30T02:35:57.7616252Z   1200K .......... .......... ..........
.......... ..........  7%  445K 11s
2022-10-30T02:35:57.7616964Z   1250K .......... .......... ..........
.......... ..........  8%  127M 10s
2022-10-30T02:35:57.7617539Z   1300K .......... .......... ..........
.......... ..........  8%  187M 10s
2022-10-30T02:35:57.7618096Z   1350K .......... .......... ..........
.......... ..........  8%  173M 10s
2022-10-30T02:35:57.7618697Z   1400K .......... .......... ..........
.......... ..........  8%  217M 9s
2022-10-30T02:35:57.7619246Z   1450K .......... .......... ..........
.......... ..........  9%  197M 9s
2022-10-30T02:35:57.7619791Z   1500K .......... .......... ..........
.......... ..........  9%  192M 9s
2022-10-30T02:35:57.7620340Z   1550K .......... .......... ..........
.......... ..........  9%  207M 8s
2022-10-30T02:35:57.7620886Z   1600K .......... .......... ..........
.......... .......... 10%  193M 8s
2022-10-30T02:35:57.7621435Z   1650K .......... .......... ..........
.......... .......... 10%  217M 8s
2022-10-30T02:35:57.8838958Z   1700K .......... .......... ..........
.......... .......... 10%  417K 9s
2022-10-30T02:35:57.8839926Z   1750K .......... .......... ..........
.......... .......... 11%  137M 8s
2022-10-30T02:35:57.8840475Z   1800K .......... .......... ..........
.......... .......... 11%  193M 8s
2022-10-30T02:35:57.8841033Z   1850K .......... .......... ..........
.......... .......... 11%  219M 8s
2022-10-30T02:35:57.8841587Z   1900K .......... .......... ..........
.......... .......... 12%  208M 8s
2022-10-30T02:35:57.8842139Z   1950K .......... .......... ..........
.......... .......... 12%  191M 7s
2022-10-30T02:35:57.8842688Z   2000K .......... .......... ..........
.......... .......... 12%  220M 7s
2022-10-30T02:35:57.8843403Z   2050K .......... .......... ..........
.......... .......... 13%  208M 7s
2022-10-30T02:35:57.8843960Z   2100K .......... .......... ..........
.......... .......... 13%  221M 7s
2022-10-30T02:35:57.8844510Z   2150K .......... .......... ..........
.......... .......... 13%  198M 7s
2022-10-30T02:35:57.8845260Z   2200K .......... .......... ..........
.......... .......... 13%  215M 6s
2022-10-30T02:35:57.8845807Z   2250K .......... .......... ..........
.......... .......... 14%  102M 6s
2022-10-30T02:35:57.9896724Z   2300K .......... .......... ..........
.......... .......... 14%  479K 7s
2022-10-30T02:35:57.9897384Z   2350K .......... .......... ..........
.......... .......... 14%  139M 7s
2022-10-30T02:35:57.9897951Z   2400K .......... .......... ..........
.......... .......... 15%  199M 6s
```

```
2022-10-30T02:35:57.9924966Z   2450K .......... .......... ..........
.......... .......... 15% 97.9M 6s
2022-10-30T02:35:57.9925517Z   2500K .......... .......... ..........
.......... .......... 15%  109M 6s
2022-10-30T02:35:57.9926007Z   2550K .......... .......... ..........
.......... .......... 16%  187M 6s
2022-10-30T02:35:57.9926491Z   2600K .......... .......... ..........
.......... .......... 16%  115M 6s
2022-10-30T02:35:57.9926973Z   2650K .......... .......... ..........
.......... .......... 16%  222M 6s
2022-10-30T02:35:57.9927495Z   2700K .......... .......... ..........
.......... .......... 17%  101M 6s
2022-10-30T02:35:57.9927969Z   2750K .......... .......... ..........
.......... .......... 17%  182M 5s
2022-10-30T02:35:57.9928444Z   2800K .......... .......... ..........
.......... .......... 17%  252M 5s
2022-10-30T02:35:57.9928917Z   2850K .......... .......... ..........
.......... .......... 17%  238M 5s
2022-10-30T02:35:57.9932893Z   2900K .......... .......... ..........
.......... .......... 18%  131M 5s
2022-10-30T02:35:57.9933369Z   2950K .......... .......... ..........
.......... .......... 18%  217M 5s
2022-10-30T02:35:57.9937629Z   3000K .......... .......... ..........
.......... .......... 18%  238M 5s
2022-10-30T02:35:57.9938165Z   3050K .......... .......... ..........
.......... .......... 19%  260M 5s
2022-10-30T02:35:57.9938650Z   3100K .......... .......... ..........
.......... .......... 19%  211M 5s
2022-10-30T02:35:58.1038568Z   3150K .......... .......... ..........
.......... .......... 19%  456K 5s
2022-10-30T02:35:58.1046729Z   3200K .......... .......... ..........
.......... .......... 20%  178M 5s
2022-10-30T02:35:58.1047403Z   3250K .......... .......... ..........
.......... .......... 20%  104M 5s
2022-10-30T02:35:58.1055182Z   3300K .......... .......... ..........
.......... .......... 20%  185M 5s
2022-10-30T02:35:58.1055816Z   3350K .......... .......... ..........
.......... .......... 21%  177M 5s
2022-10-30T02:35:58.1056372Z   3400K .......... .......... ..........
.......... .......... 21%  162M 5s
2022-10-30T02:35:58.1056923Z   3450K .......... .......... ..........
.......... .......... 21%  202M 5s
2022-10-30T02:35:58.1064827Z   3500K .......... .......... ..........
.......... .......... 22%  142M 4s
2022-10-30T02:35:58.1065407Z   3550K .......... .......... ..........
.......... .......... 22%  167M 4s
2022-10-30T02:35:58.1067558Z   3600K .......... .......... ..........
.......... .......... 22%  221M 4s
2022-10-30T02:35:58.1077137Z   3650K .......... .......... ..........
.......... .......... 22%  207M 4s
2022-10-30T02:35:58.1078060Z   3700K .......... .......... ..........
.......... .......... 23%  215M 4s
2022-10-30T02:35:58.1078615Z   3750K .......... .......... ..........
.......... .......... 23%  146M 4s
2022-10-30T02:35:58.1079165Z   3800K .......... .......... ..........
.......... .......... 23%  166M 4s
```

```
2022-10-30T02:35:58.1079713Z   3850K .......... .......... ..........
.......... .......... 24%  207M 4s
2022-10-30T02:35:58.1080263Z   3900K .......... .......... ..........
.......... .......... 24%  222M 4s
2022-10-30T02:35:58.1083039Z   3950K .......... .......... ..........
.......... .......... 24%  130M 4s
2022-10-30T02:35:58.1083734Z   4000K .......... .......... ..........
.......... .......... 25%  189M 4s
2022-10-30T02:35:58.2302651Z   4050K .......... .......... ..........
.......... .......... 25%  411K 4s
2022-10-30T02:35:58.2303341Z   4100K .......... .......... ..........
.......... .......... 25%  145M 4s
2022-10-30T02:35:58.2329523Z   4150K .......... .......... ..........
.......... .......... 26% 75.7M 4s
2022-10-30T02:35:58.2330147Z   4200K .......... .......... ..........
.......... .......... 26%  138M 4s
2022-10-30T02:35:58.2330707Z   4250K .......... .......... ..........
.......... .......... 26%  197M 4s
2022-10-30T02:35:58.2331264Z   4300K .......... .......... ..........
.......... .......... 26%  216M 4s
2022-10-30T02:35:58.2331819Z   4350K .......... .......... ..........
.......... .......... 27%  213M 4s
2022-10-30T02:35:58.2341880Z   4400K .......... .......... ..........
.......... .......... 27%  186M 4s
2022-10-30T02:35:58.2342629Z   4450K .......... .......... ..........
.......... .......... 27%  191M 4s
2022-10-30T02:35:58.2343265Z   4500K .......... .......... ..........
.......... .......... 28%  179M 4s
2022-10-30T02:35:58.2343829Z   4550K .......... .......... ..........
.......... .......... 28%  206M 3s
2022-10-30T02:35:58.2344449Z   4600K .......... .......... ..........
.......... .......... 28% 64.4M 3s
2022-10-30T02:35:58.2345039Z   4650K .......... .......... ..........
.......... .......... 29%  158M 3s
2022-10-30T02:35:58.2345591Z   4700K .......... .......... ..........
.......... .......... 29%  170M 3s
2022-10-30T02:35:58.2351257Z   4750K .......... .......... ..........
.......... .......... 29% 70.9M 3s
2022-10-30T02:35:58.2352192Z   4800K .......... .......... ..........
.......... .......... 30%  143M 3s
2022-10-30T02:35:58.2357263Z   4850K .......... .......... ..........
.......... .......... 30% 84.2M 3s
2022-10-30T02:35:58.2363854Z   4900K .......... .......... ..........
.......... .......... 30%  105M 3s
2022-10-30T02:35:58.2367493Z   4950K .......... .......... ..........
.......... .......... 31% 99.5M 3s
2022-10-30T02:35:58.2372264Z   5000K .......... .......... ..........
.......... .......... 31% 95.2M 3s
2022-10-30T02:35:58.2376283Z   5050K .......... .......... ..........
.......... .......... 31%  113M 3s
2022-10-30T02:35:58.2380922Z   5100K .......... .......... ..........
.......... .......... 31%  105M 3s
2022-10-30T02:35:58.2385158Z   5150K .......... .......... ..........
.......... .......... 32%  116M 3s
2022-10-30T02:35:58.2389554Z   5200K .......... .......... ..........
.......... .......... 32%  102M 3s
```

```
2022-10-30T02:35:58.2394041Z   5250K ..... ..... ..... ..... ..... ..... 32%  121M 3s
2022-10-30T02:35:58.2398044Z   5300K ..... ..... ..... ..... ..... ..... 33%  119M 3s
2022-10-30T02:35:58.2403073Z   5350K ..... ..... ..... ..... ..... ..... 33%  104M 3s
2022-10-30T02:35:58.2408120Z   5400K ..... ..... ..... ..... ..... ..... 33% 86.4M 3s
2022-10-30T02:35:58.2413712Z   5450K ..... ..... ..... ..... ..... ..... 34% 95.2M 3s
2022-10-30T02:35:58.3448698Z   5500K ..... ..... ..... ..... ..... ..... 34%  485K 3s
2022-10-30T02:35:58.3456695Z   5550K ..... ..... ..... ..... ..... ..... 34%  117M 3s
2022-10-30T02:35:58.3457364Z   5600K ..... ..... ..... ..... ..... ..... 35%  147M 3s
2022-10-30T02:35:58.3470441Z   5650K ..... ..... ..... ..... ..... ..... 35%  172M 3s
2022-10-30T02:35:58.3471122Z   5700K ..... ..... ..... ..... ..... ..... 35%  204M 3s
2022-10-30T02:35:58.3471687Z   5750K ..... ..... ..... ..... ..... ..... 35%  171M 3s
2022-10-30T02:35:58.3474180Z   5800K ..... ..... ..... ..... ..... ..... 36%  194M 3s
2022-10-30T02:35:58.3484706Z   5850K ..... ..... ..... ..... ..... ..... 36%  216M 3s
2022-10-30T02:35:58.3485324Z   5900K ..... ..... ..... ..... ..... ..... 36%  135M 3s
2022-10-30T02:35:58.3485882Z   5950K ..... ..... ..... ..... ..... ..... 37%  189M 3s
2022-10-30T02:35:58.3486431Z   6000K ..... ..... ..... ..... ..... ..... 37%  191M 3s
2022-10-30T02:35:58.3486982Z   6050K ..... ..... ..... ..... ..... ..... 37%  227M 2s
2022-10-30T02:35:58.3487747Z   6100K ..... ..... ..... ..... ..... ..... 38%  100M 2s
2022-10-30T02:35:58.3489973Z   6150K ..... ..... ..... ..... ..... ..... 38%  106M 2s
2022-10-30T02:35:58.3491925Z   6200K ..... ..... ..... ..... ..... ..... 38% 72.9M 2s
2022-10-30T02:35:58.3495957Z   6250K ..... ..... ..... ..... ..... ..... 39% 91.6M 2s
2022-10-30T02:35:58.3498957Z   6300K ..... ..... ..... ..... ..... ..... 39%  170M 2s
2022-10-30T02:35:58.3503079Z   6350K ..... ..... ..... ..... ..... ..... 39%  121M 2s
2022-10-30T02:35:58.3506655Z   6400K ..... ..... ..... ..... ..... ..... 40%  129M 2s
2022-10-30T02:35:58.3509232Z   6450K ..... ..... ..... ..... ..... ..... 40%  181M 2s
2022-10-30T02:35:58.3511919Z   6500K ..... ..... ..... ..... ..... ..... 40%  185M 2s
2022-10-30T02:35:58.3514896Z   6550K ..... ..... ..... ..... ..... ..... 40%  187M 2s
2022-10-30T02:35:58.3517578Z   6600K ..... ..... ..... ..... ..... ..... 41%  166M 2s
```

```
2022-10-30T02:35:58.3520226Z   6650K .......... .......... ..........
.......... .......... 41%  171M 2s
2022-10-30T02:35:58.3523404Z   6700K .......... .......... ..........
.......... .......... 41%  178M 2s
2022-10-30T02:35:58.3526792Z   6750K .......... .......... ..........
.......... .......... 42%  169M 2s
2022-10-30T02:35:58.3529321Z   6800K .......... .......... ..........
.......... .......... 42%  179M 2s
2022-10-30T02:35:58.3531708Z   6850K .......... .......... ..........
.......... .......... 42%  164M 2s
2022-10-30T02:35:58.3534979Z   6900K .......... .......... ..........
.......... .......... 43%  178M 2s
2022-10-30T02:35:58.3537485Z   6950K .......... .......... ..........
.......... .......... 43%  173M 2s
2022-10-30T02:35:58.3540785Z   7000K .......... .......... ..........
.......... .......... 43%  177M 2s
2022-10-30T02:35:58.3543250Z   7050K .......... .......... ..........
.......... .......... 44%  154M 2s
2022-10-30T02:35:58.3546644Z   7100K .......... .......... ..........
.......... .......... 44%  178M 2s
2022-10-30T02:35:58.3549060Z   7150K .......... .......... ..........
.......... .......... 44%  176M 2s
2022-10-30T02:35:58.3552331Z   7200K .......... .......... ..........
.......... .......... 44%  172M 2s
2022-10-30T02:35:58.3554803Z   7250K .......... .......... ..........
.......... .......... 45%  163M 2s
2022-10-30T02:35:58.4583889Z   7300K .......... .......... ..........
.......... .......... 45%  487K 2s
2022-10-30T02:35:58.4597543Z   7350K .......... .......... ..........
.......... .......... 45% 64.2M 2s
2022-10-30T02:35:58.4598237Z   7400K .......... .......... ..........
.......... .......... 46%  194M 2s
2022-10-30T02:35:58.4598800Z   7450K .......... .......... ..........
.......... .......... 46%  207M 2s
2022-10-30T02:35:58.4602550Z   7500K .......... .......... ..........
.......... .......... 46%  125M 2s
2022-10-30T02:35:58.4606339Z   7550K .......... .......... ..........
.......... .......... 47% 63.1M 2s
2022-10-30T02:35:58.4611562Z   7600K .......... .......... ..........
.......... .......... 47% 72.9M 2s
2022-10-30T02:35:58.4616656Z   7650K .......... .......... ..........
.......... .......... 47%  129M 2s
2022-10-30T02:35:58.4620436Z   7700K .......... .......... ..........
.......... .......... 48% 93.3M 2s
2022-10-30T02:35:58.4624290Z   7750K .......... .......... ..........
.......... .......... 48%  139M 2s
2022-10-30T02:35:58.4627648Z   7800K .......... .......... ..........
.......... .......... 48%  121M 2s
2022-10-30T02:35:58.4631004Z   7850K .......... .......... ..........
.......... .......... 49%  146M 2s
2022-10-30T02:35:58.4634696Z   7900K .......... .......... ..........
.......... .......... 49%  144M 2s
2022-10-30T02:35:58.4638736Z   7950K .......... .......... ..........
.......... .......... 49%  126M 2s
2022-10-30T02:35:58.4642113Z   8000K .......... .......... ..........
.......... .......... 49%  127M 2s
```

```
2022-10-30T02:35:58.4645598Z   8050K .......... .......... ..........
.......... .......... 50%  147M 2s
2022-10-30T02:35:58.4649027Z   8100K .......... .......... ..........
.......... .......... 50%  141M 2s
2022-10-30T02:35:58.5857230Z   8150K .......... .......... ..........
.......... .......... 50%  416K 2s
2022-10-30T02:35:58.5862342Z   8200K .......... .......... ..........
.......... .......... 51% 51.0M 2s
2022-10-30T02:35:58.5868447Z   8250K .......... .......... ..........
.......... .......... 51% 77.4M 2s
2022-10-30T02:35:58.5874783Z   8300K .......... .......... ..........
.......... .......... 51% 79.8M 2s
2022-10-30T02:35:58.5881327Z   8350K .......... .......... ..........
.......... .......... 52%  116M 2s
2022-10-30T02:35:58.5887238Z   8400K .......... .......... ..........
.......... .......... 52% 56.8M 2s
2022-10-30T02:35:58.5891465Z   8450K .......... .......... ..........
.......... .......... 52%  114M 2s
2022-10-30T02:35:58.5900363Z   8500K .......... .......... ..........
.......... .......... 53% 75.7M 2s
2022-10-30T02:35:58.5904442Z   8550K .......... .......... ..........
.......... .......... 53% 95.5M 2s
2022-10-30T02:35:58.5910368Z   8600K .......... .......... ..........
.......... .......... 53% 76.4M 2s
2022-10-30T02:35:58.5916254Z   8650K .......... .......... ..........
.......... .......... 53% 88.5M 1s
2022-10-30T02:35:58.5920721Z   8700K .......... .......... ..........
.......... .......... 54%  155M 1s
2022-10-30T02:35:58.5924733Z   8750K .......... .......... ..........
.......... .......... 54%  100M 1s
2022-10-30T02:35:58.5930014Z   8800K .......... .......... ..........
.......... .......... 54% 79.5M 1s
2022-10-30T02:35:58.5935369Z   8850K .......... .......... ..........
.......... .......... 55%  171M 1s
2022-10-30T02:35:58.5940316Z   8900K .......... .......... ..........
.......... .......... 55% 90.5M 1s
2022-10-30T02:35:58.5943257Z   8950K .......... .......... ..........
.......... .......... 55%  104M 1s
2022-10-30T02:35:58.5947739Z   9000K .......... .......... ..........
.......... .......... 56% 97.4M 1s
2022-10-30T02:35:58.5950827Z   9050K .......... .......... ..........
.......... .......... 56%  179M 1s
2022-10-30T02:35:58.5956291Z   9100K .......... .......... ..........
.......... .......... 56%  107M 1s
2022-10-30T02:35:58.5959353Z   9150K .......... .......... ..........
.......... .......... 57%  130M 1s
2022-10-30T02:35:58.5962514Z   9200K .......... .......... ..........
.......... .......... 57%  159M 1s
2022-10-30T02:35:58.5965765Z   9250K .......... .......... ..........
.......... .......... 57%  174M 1s
2022-10-30T02:35:58.5968918Z   9300K .......... .......... ..........
.......... .......... 58%  192M 1s
2022-10-30T02:35:58.5971968Z   9350K .......... .......... ..........
.......... .......... 58%  227M 1s
2022-10-30T02:35:58.5975907Z   9400K .......... .......... ..........
.......... .......... 58%  165M 1s
```

```
2022-10-30T02:35:58.5976428Z   9450K ..... ..... .....
..... ..... 58%  199M 1s
2022-10-30T02:35:58.5979754Z   9500K ..... ..... .....
..... ..... 59%  171M 1s
2022-10-30T02:35:58.5984216Z   9550K ..... ..... .....
..... ..... 59%  261M 1s
2022-10-30T02:35:58.5984739Z   9600K ..... ..... .....
..... ..... 59%  170M 1s
2022-10-30T02:35:58.5988832Z   9650K ..... ..... .....
..... ..... 60%  208M 1s
2022-10-30T02:35:58.5989349Z   9700K ..... ..... .....
..... ..... 60%  199M 1s
2022-10-30T02:35:58.5993433Z   9750K ..... ..... .....
..... ..... 60%  172M 1s
2022-10-30T02:35:58.5993952Z   9800K ..... ..... .....
..... ..... 61%  206M 1s
2022-10-30T02:35:58.5997227Z   9850K ..... ..... .....
..... ..... 61%  165M 1s
2022-10-30T02:35:58.6001130Z   9900K ..... ..... .....
..... ..... 61%  209M 1s
2022-10-30T02:35:58.6001657Z   9950K ..... ..... .....
..... ..... 62%  188M 1s
2022-10-30T02:35:58.6006281Z  10000K ..... ..... .....
..... ..... 62%  169M 1s
2022-10-30T02:35:58.6006815Z  10050K ..... ..... .....
..... ..... 62%  234M 1s
2022-10-30T02:35:58.6010145Z  10100K ..... ..... .....
..... ..... 62%  153M 1s
2022-10-30T02:35:58.6013167Z  10150K ..... ..... .....
..... ..... 63%  237M 1s
2022-10-30T02:35:58.6017066Z  10200K ..... ..... .....
..... ..... 63%  167M 1s
2022-10-30T02:35:58.6017587Z  10250K ..... ..... .....
..... ..... 63%  188M 1s
2022-10-30T02:35:58.6020890Z  10300K ..... ..... .....
..... ..... 64%  172M 1s
2022-10-30T02:35:58.6027936Z  10350K ..... ..... .....
..... ..... 64%  230M 1s
2022-10-30T02:35:58.6028469Z  10400K ..... ..... .....
..... ..... 64%  164M 1s
2022-10-30T02:35:58.6028955Z  10450K ..... ..... .....
..... ..... 65%  193M 1s
2022-10-30T02:35:58.6032997Z  10500K ..... ..... .....
..... ..... 65%  242M 1s
2022-10-30T02:35:58.6033519Z  10550K ..... ..... .....
..... ..... 65%  188M 1s
2022-10-30T02:35:58.6037635Z  10600K ..... ..... .....
..... ..... 66%  159M 1s
2022-10-30T02:35:58.6038156Z  10650K ..... ..... .....
..... ..... 66%  227M 1s
2022-10-30T02:35:58.6045605Z  10700K ..... ..... .....
..... ..... 66%  179M 1s
2022-10-30T02:35:58.6046142Z  10750K ..... ..... .....
..... ..... 67%  246M 1s
2022-10-30T02:35:58.6046628Z  10800K ..... ..... .....
..... ..... 67%  179M 1s
```

```
2022-10-30T02:35:58.6050692Z  10850K .......... .......... ..........
.......... .......... 67%  233M 1s
2022-10-30T02:35:58.6051216Z  10900K .......... .......... ..........
.......... .......... 67%  201M 1s
2022-10-30T02:35:58.6054401Z  10950K .......... .......... ..........
.......... .......... 68%  249M 1s
2022-10-30T02:35:58.7017643Z  11000K .......... .......... ..........
.......... .......... 68%  517K 1s
2022-10-30T02:35:58.7021795Z  11050K .......... .......... ..........
.......... .......... 68% 87.7M 1s
2022-10-30T02:35:58.7028047Z  11100K .......... .......... ..........
.......... .......... 69% 96.2M 1s
2022-10-30T02:35:58.7031349Z  11150K .......... .......... ..........
.......... .......... 69%  112M 1s
2022-10-30T02:35:58.7036522Z  11200K .......... .......... ..........
.......... .......... 69% 86.1M 1s
2022-10-30T02:35:58.7041918Z  11250K .......... .......... ..........
.......... .......... 70% 96.9M 1s
2022-10-30T02:35:58.7044647Z  11300K .......... .......... ..........
.......... .......... 70%  158M 1s
2022-10-30T02:35:58.7050301Z  11350K .......... .......... ..........
.......... .......... 70% 92.1M 1s
2022-10-30T02:35:58.7055139Z  11400K .......... .......... ..........
.......... .......... 71% 95.5M 1s
2022-10-30T02:35:58.7060361Z  11450K .......... .......... ..........
.......... .......... 71%  100M 1s
2022-10-30T02:35:58.7063037Z  11500K .......... .......... ..........
.......... .......... 71%  170M 1s
2022-10-30T02:35:58.7065251Z  11550K .......... .......... ..........
.......... .......... 71%  199M 1s
2022-10-30T02:35:58.7067863Z  11600K .......... .......... ..........
.......... .......... 72%  185M 1s
2022-10-30T02:35:58.7070385Z  11650K .......... .......... ..........
.......... .......... 72%  199M 1s
2022-10-30T02:35:58.7072890Z  11700K .......... .......... ..........
.......... .......... 72%  199M 1s
2022-10-30T02:35:58.7075747Z  11750K .......... .......... ..........
.......... .......... 73%  199M 1s
2022-10-30T02:35:58.7078249Z  11800K .......... .......... ..........
.......... .......... 73%  164M 1s
2022-10-30T02:35:58.7080752Z  11850K .......... .......... ..........
.......... .......... 73%  196M 1s
2022-10-30T02:35:58.7083427Z  11900K .......... .......... ..........
.......... .......... 74%  198M 1s
2022-10-30T02:35:58.7086117Z  11950K .......... .......... ..........
.......... .......... 74%  188M 1s
2022-10-30T02:35:58.7088363Z  12000K .......... .......... ..........
.......... .......... 74%  183M 1s
2022-10-30T02:35:58.7090953Z  12050K .......... .......... ..........
.......... .......... 75%  210M 1s
2022-10-30T02:35:58.7093095Z  12100K .......... .......... ..........
.......... .......... 75%  198M 1s
2022-10-30T02:35:58.7095662Z  12150K .......... .......... ..........
.......... .......... 75%  219M 1s
2022-10-30T02:35:58.7098168Z  12200K .......... .......... ..........
.......... .......... 76%  170M 1s
```

```
2022-10-30T02:35:58.8218415Z  12250K .......... .......... ..........
.......... .......... 76%  448K 1s
2022-10-30T02:35:58.8222240Z  12300K .......... .......... ..........
.......... .......... 76% 83.9M 1s
2022-10-30T02:35:58.8227143Z  12350K .......... .......... ..........
.......... .......... 76% 83.6M 1s
2022-10-30T02:35:58.8233908Z  12400K .......... .......... ..........
.......... .......... 77% 66.3M 1s
2022-10-30T02:35:58.8244056Z  12450K .......... .......... ..........
.......... .......... 77% 62.6M 1s
2022-10-30T02:35:58.8252031Z  12500K .......... .......... ..........
.......... .......... 77% 48.8M 1s
2022-10-30T02:35:58.8259899Z  12550K .......... .......... ..........
.......... .......... 78% 64.6M 1s
2022-10-30T02:35:58.8267065Z  12600K .......... .......... ..........
.......... .......... 78% 61.4M 1s
2022-10-30T02:35:58.8274165Z  12650K .......... .......... ..........
.......... .......... 78% 69.0M 1s
2022-10-30T02:35:58.8392330Z  12700K .......... .......... ..........
.......... .......... 79% 37.3M 1s
2022-10-30T02:35:58.8392878Z  12750K .......... .......... ..........
.......... .......... 79%  243M 1s
2022-10-30T02:35:58.8393377Z  12800K .......... .......... ..........
.......... .......... 79%  205M 1s
2022-10-30T02:35:58.8393867Z  12850K .......... .......... ..........
.......... .......... 80%  248M 0s
2022-10-30T02:35:58.8394349Z  12900K .......... .......... ..........
.......... .......... 80%  118M 0s
2022-10-30T02:35:58.8394875Z  12950K .......... .......... ..........
.......... .......... 80%  236M 0s
2022-10-30T02:35:58.8395355Z  13000K .......... .......... ..........
.......... .......... 80%  225M 0s
2022-10-30T02:35:58.8395833Z  13050K .......... .......... ..........
.......... .......... 81%  269M 0s
2022-10-30T02:35:58.8396310Z  13100K .......... .......... ..........
.......... .......... 81%  234M 0s
2022-10-30T02:35:58.8396786Z  13150K .......... .......... ..........
.......... .......... 81%  127M 0s
2022-10-30T02:35:58.8397251Z  13200K .......... .......... ..........
.......... .......... 82%  222M 0s
2022-10-30T02:35:58.8397728Z  13250K .......... .......... ..........
.......... .......... 82%  259M 0s
2022-10-30T02:35:58.8398207Z  13300K .......... .......... ..........
.......... .......... 82%  259M 0s
2022-10-30T02:35:58.8398687Z  13350K .......... .......... ..........
.......... .......... 83%  226M 0s
2022-10-30T02:35:58.8399165Z  13400K .......... .......... ..........
.......... .......... 83% 42.9M 0s
2022-10-30T02:35:58.8399864Z  13450K .......... .......... ..........
.......... .......... 83%  239M 0s
2022-10-30T02:35:58.8400347Z  13500K .......... .......... ..........
.......... .......... 84%  264M 0s
2022-10-30T02:35:58.8400826Z  13550K .......... .......... ..........
.......... .......... 84%  260M 0s
2022-10-30T02:35:58.8401306Z  13600K .......... .......... ..........
.......... .......... 84%  223M 0s
```

```
2022-10-30T02:35:58.8401786Z  13650K .......... .......... ..........
.......... .......... 85% 91.1M 0s
2022-10-30T02:35:58.8402254Z  13700K .......... .......... ..........
.......... .......... 85%  224M 0s
2022-10-30T02:35:58.8402734Z  13750K .......... .......... ..........
.......... .......... 85%  244M 0s
2022-10-30T02:35:58.8403372Z  13800K .......... .......... ..........
.......... .......... 85%  214M 0s
2022-10-30T02:35:58.8403863Z  13850K .......... .......... ..........
.......... .......... 86%  237M 0s
2022-10-30T02:35:58.8404459Z  13900K .......... .......... ..........
.......... .......... 86%  260M 0s
2022-10-30T02:35:58.8404936Z  13950K .......... .......... ..........
.......... .......... 86%  238M 0s
2022-10-30T02:35:58.8405415Z  14000K .......... .......... ..........
.......... .......... 87%  208M 0s
2022-10-30T02:35:58.8405891Z  14050K .......... .......... ..........
.......... .......... 87%  235M 0s
2022-10-30T02:35:58.8406369Z  14100K .......... .......... ..........
.......... .......... 87%  243M 0s
2022-10-30T02:35:58.8406844Z  14150K .......... .......... ..........
.......... .......... 88%  247M 0s
2022-10-30T02:35:58.8407306Z  14200K .......... .......... ..........
.......... .......... 88%  195M 0s
2022-10-30T02:35:58.8407787Z  14250K .......... .......... ..........
.......... .......... 88%  263M 0s
2022-10-30T02:35:58.8408265Z  14300K .......... .......... ..........
.......... .......... 89%  231M 0s
2022-10-30T02:35:58.8408746Z  14350K .......... .......... ..........
.......... .......... 89%  265M 0s
2022-10-30T02:35:58.8409233Z  14400K .......... .......... ..........
.......... .......... 89%  225M 0s
2022-10-30T02:35:58.8415063Z  14450K .......... .......... ..........
.......... .......... 89% 14.5M 0s
2022-10-30T02:35:58.8415579Z  14500K .......... .......... ..........
.......... .......... 90%  232M 0s
2022-10-30T02:35:58.8416068Z  14550K .......... .......... ..........
.......... .......... 90%  233M 0s
2022-10-30T02:35:58.8416551Z  14600K .......... .......... ..........
.......... .......... 90%  208M 0s
2022-10-30T02:35:58.8424056Z  14650K .......... .......... ..........
.......... .......... 91%  131M 0s
2022-10-30T02:35:58.8424562Z  14700K .......... .......... ..........
.......... .......... 91%  239M 0s
2022-10-30T02:35:58.8425030Z  14750K .......... .......... ..........
.......... .......... 91%  242M 0s
2022-10-30T02:35:58.8428897Z  14800K .......... .......... ..........
.......... .......... 92%  128M 0s
2022-10-30T02:35:58.8429409Z  14850K .......... .......... ..........
.......... .......... 92%  234M 0s
2022-10-30T02:35:58.8435431Z  14900K .......... .......... ..........
.......... .......... 92%  136M 0s
2022-10-30T02:35:58.8435934Z  14950K .......... .......... ..........
.......... .......... 93%  238M 0s
2022-10-30T02:35:58.8437426Z  15000K .......... .......... ..........
.......... .......... 93%  206M 0s
```

```
2022-10-30T02:35:58.8439884Z  15050K .......... .......... ..........
.......... .......... 93%  123M 0s
2022-10-30T02:35:58.8442979Z  15100K .......... .......... ..........
.......... .......... 94%  174M 0s
2022-10-30T02:35:58.8445825Z  15150K .......... .......... ..........
.......... .......... 94%  166M 0s
2022-10-30T02:35:58.8470195Z  15200K .......... .......... ..........
.......... .......... 94% 22.0M 0s
2022-10-30T02:35:58.8476505Z  15250K .......... .......... ..........
.......... .......... 94%  176M 0s
2022-10-30T02:35:58.8477059Z  15300K .......... .......... ..........
.......... .......... 95%  145M 0s
2022-10-30T02:35:58.8477555Z  15350K .......... .......... ..........
.......... .......... 95%  255M 0s
2022-10-30T02:35:58.8479925Z  15400K .......... .......... ..........
.......... .......... 95%  123M 0s
2022-10-30T02:35:58.8489069Z  15450K .......... .......... ..........
.......... .......... 96%  123M 0s
2022-10-30T02:35:58.8489582Z  15500K .......... .......... ..........
.......... .......... 96%  212M 0s
2022-10-30T02:35:58.8496168Z  15550K .......... .......... ..........
.......... .......... 96% 52.5M 0s
2022-10-30T02:35:58.8498547Z  15600K .......... .......... ..........
.......... .......... 97%  157M 0s
2022-10-30T02:35:58.8503765Z  15650K .......... .......... ..........
.......... .......... 97% 97.8M 0s
2022-10-30T02:35:58.8507841Z  15700K .......... .......... ..........
.......... .......... 97%  171M 0s
2022-10-30T02:35:58.8510917Z  15750K .......... .......... ..........
.......... .......... 98%  104M 0s
2022-10-30T02:35:58.8513774Z  15800K .......... .......... ..........
.......... .......... 98%  168M 0s
2022-10-30T02:35:58.8516242Z  15850K .......... .......... ..........
.......... .......... 98%  201M 0s
2022-10-30T02:35:58.8518807Z  15900K .......... .......... ..........
.......... .......... 98%  212M 0s
2022-10-30T02:35:58.8520863Z  15950K .......... .......... ..........
.......... .......... 99%  203M 0s
2022-10-30T02:35:58.8523715Z  16000K .......... .......... ..........
.......... .......... 99%  183M 0s
2022-10-30T02:35:58.8526277Z  16050K .......... .......... ..........
.......... .......... 99%  189M 0s
2022-10-30T02:35:58.8528360Z  16100K .......... .
100%  217M=2.0s
2022-10-30T02:35:58.8528588Z
2022-10-30T02:35:58.8529762Z 2022-10-30 02:35:58 (7.82 MB/s) -
‘trivy_0.27.1_Linux-64bit.deb’ saved [16498508/16498508]
2022-10-30T02:35:58.8530052Z
2022-10-30T02:35:58.8914725Z Selecting previously unselected package
trivy.
2022-10-30T02:35:59.3766958Z (Reading database ... 242027 files and
directories currently installed.)
2022-10-30T02:35:59.3888595Z Preparing to unpack trivy_0.27.1_Linux-
64bit.deb ...
2022-10-30T02:35:59.3918154Z Unpacking trivy (0.27.1) ...
2022-10-30T02:35:59.7184016Z Setting up trivy (0.27.1) ...
```

```
2022-10-30T02:35:59.8697026Z 2022-10-30T02:35:59.868Z [34mINFO [0m  Need
to update DB
2022-10-30T02:35:59.8698575Z 2022-10-30T02:35:59.868Z [34mINFO [0m  DB
Repository: ghcr.io/aquasecurity/trivy-db
2022-10-30T02:35:59.8699915Z 2022-10-30T02:35:59.868Z [34mINFO [0m
       Downloading DB...
2022-10-30T02:36:09.6315805Z 34.66 MiB / 34.66 MiB [----------------------
--------------------------------------->] 100.00% ? p/s ?34.66 MiB / 34.66
MiB [------------------------------------------------------------>]
100.00% ? p/s ?34.66 MiB / 34.66 MiB [-----------------------------------
------------------------>] 100.00% ? p/s ?34.66 MiB / 34.66 MiB [--------
-------------------------------------------------->] 100.00% ? p/s
?34.66 MiB / 34.66 MiB [-------------------------------------------------
---------->] 100.00% ? p/s ?34.66 MiB / 34.66 MiB [----------------------
--------------------------------------->] 100.00% ? p/s ?34.66 MiB / 34.66
MiB [------------------------------------------------------------>]
100.00% ? p/s ?34.66 MiB / 34.66 MiB [-----------------------------------
--------------] 100.00% 28.64 MiB p/s 1.4s2022-10-30T02:36:09.630Z
        [34mINFO [0m  Detected OS: alpine
2022-10-30T02:36:09.6318673Z 2022-10-30T02:36:09.630Z [34mINFO [0m
       Detecting Alpine vulnerabilities...
2022-10-30T02:36:09.6348345Z 2022-10-30T02:36:09.634Z [34mINFO [0m
       Number of language-specific files: 1
2022-10-30T02:36:09.6349590Z 2022-10-30T02:36:09.634Z [34mINFO [0m
       Detecting jar vulnerabilities...
2022-10-30T02:36:09.6395327Z 2022-10-30T02:36:09.639Z [33mWARN [0m  This
OS version is no longer supported by the distribution: alpine 3.9.4
2022-10-30T02:36:09.6396808Z 2022-10-30T02:36:09.639Z [33mWARN [0m  The
vulnerability detection may be insufficient because security updates are
not provided
2022-10-30T02:36:09.6951083Z
2022-10-30T02:36:09.6956017Z ***/spring-boot-kubernetes:latest (alpine
3.9.4)
2022-10-30T02:36:09.6987755Z
==========================================================
2022-10-30T02:36:09.6988328Z Total: 274 (UNKNOWN: 0, LOW: 140, MEDIUM:
98, HIGH: 32, CRITICAL: 4)
2022-10-30T02:36:09.6988590Z
2022-10-30T02:36:09.6989691Z +-------------------+-----------------+----
------+-------------------+---------------+------------------------------
------------+
2022-10-30T02:36:09.6990420Z |      LIBRARY      | VULNERABILITY ID |
SEVERITY | INSTALLED VERSION | FIXED VERSION |                  TITLE
|
2022-10-30T02:36:09.6991383Z +-------------------+-----------------+----
------+-------------------+---------------+------------------------------
------------+
2022-10-30T02:36:09.6992386Z | freetype          | CVE-2020-15999   |
MEDIUM   | 2.9.1-r2          | 2.9.1-r3      | freetype: Heap-based
buffer              |
2022-10-30T02:36:09.6992991Z |                   |                  |
|                   |               | overflow due to integer
|
2022-10-30T02:36:09.6993518Z |                   |                  |
|                   |               | truncation in Load_SBit_Png
|
```

```
2022-10-30T02:36:09.6994562Z |                   |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2020-
15999    |
2022-10-30T02:36:09.6995471Z +-------------------+------------------+----
------+-------------------+--------------+-----------------------------
------------+
2022-10-30T02:36:09.6996470Z | krb5-libs         | CVE-2020-28196   |
HIGH     | 1.15.5-r0         | 1.15.5-r1     | krb5: unbounded recursion
via an         |
2022-10-30T02:36:09.6997315Z |                   |                  |
|                   |              | ASN.1-encoded Kerberos message
|
2022-10-30T02:36:09.6997849Z |                   |                  |
|                   |              | in lib/krb5/asn.1/asn1_encode.c
|
2022-10-30T02:36:09.6998346Z |                   |                  |
|                   |              | may lead...
|
2022-10-30T02:36:09.6999110Z |                   |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2020-
28196    |
2022-10-30T02:36:09.7000020Z +-------------------+------------------+----
------+-------------------+--------------+-----------------------------
------------+
2022-10-30T02:36:09.7000999Z | libbz2            | CVE-2019-12900   |
CRITICAL | 1.0.6-r6          | 1.0.6-r7      | bzip2: out-of-bounds write
|
2022-10-30T02:36:09.7001600Z |                   |                  |
|                   |              | in function BZ2_decompress
|
2022-10-30T02:36:09.7002371Z |                   |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2019-
12900    |
2022-10-30T02:36:09.7003534Z +-------------------+------------------+----
------+-------------------+--------------+-----------------------------
------------+
2022-10-30T02:36:09.7004577Z | libcom_err        | CVE-2019-5094    |
MEDIUM   | 1.44.5-r0         | 1.44.5-r1     | e2fsprogs: Crafted ext4
partition        |
2022-10-30T02:36:09.7005437Z |                   |                  |
|                   |              | leads to out-of-bounds write
|
2022-10-30T02:36:09.7006664Z |                   |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2019-
5094     |
2022-10-30T02:36:09.7007511Z +                   +------------------+
+                   +--------------+-----------------------------------
------+
2022-10-30T02:36:09.7008378Z |                   | CVE-2019-5188    |
|                   | 1.44.5-r2     | e2fsprogs: Out-of-bounds
|
2022-10-30T02:36:09.7008937Z |                   |                  |
|                   |              | write in e2fsck/rehash.c
|
2022-10-30T02:36:09.7009708Z |                   |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2019-
5188     |
```

```
2022-10-30T02:36:09.7010770Z +------------------+-----------------+----
------+------------------+---------------+------------------------------
------------+
2022-10-30T02:36:09.7011727Z | libcrypto1.1     | CVE-2020-1967    |
HIGH     | 1.1.1b-r1        | 1.1.1g-r0     | openssl: Segmentation
|
2022-10-30T02:36:09.7012327Z |                  |                  |
|                  |              | fault in SSL_check_chain
|
2022-10-30T02:36:09.7012832Z |                  |                  |
|                  |              | causes denial of service
|
2022-10-30T02:36:09.7013601Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2020-
1967     |
2022-10-30T02:36:09.7014447Z +                  +------------------+
+                  +--------------+----------------------------------
------+
2022-10-30T02:36:09.7015418Z |                  | CVE-2021-23840   |
|                  | 1.1.1j-r0    | openssl: integer
|
2022-10-30T02:36:09.7015965Z |                  |                  |
|                  |              | overflow in CipherUpdate
|
2022-10-30T02:36:09.7016730Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2021-
23840    |
2022-10-30T02:36:09.7017571Z +                  +------------------+
+                  +--------------+----------------------------------
------+
2022-10-30T02:36:09.7018442Z |                  | CVE-2021-3450    |
|                  | 1.1.1k-r0    | openssl: CA certificate check
|
2022-10-30T02:36:09.7019022Z |                  |                  |
|                  |              | bypass with X509_V_FLAG_X509_STRICT
|
2022-10-30T02:36:09.7019811Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2021-
3450     |
2022-10-30T02:36:09.7020665Z +                  +------------------+----
------+                  +--------------+------------------------------
------------+
2022-10-30T02:36:09.7021557Z |                  | CVE-2019-1547    |
MEDIUM   |                  | 1.1.1d-r0    | openssl: side-channel weak
|
2022-10-30T02:36:09.7022123Z |                  |                  |
|                  |              | encryption vulnerability
|
2022-10-30T02:36:09.7022889Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2019-
1547     |
2022-10-30T02:36:09.7023734Z +                  +------------------+
+                  +              +----------------------------------
------+
2022-10-30T02:36:09.7024435Z |                  | CVE-2019-1549    |
|                  |              | openssl: information
|
```

```
2022-10-30T02:36:09.7024900Z |                   |                  |
|                   |               | disclosure in fork()
|
2022-10-30T02:36:09.7025561Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2019-
1549     |
2022-10-30T02:36:09.7026298Z +                   +------------------+
+                   +---------------+-----------------------------------
------+
2022-10-30T02:36:09.7027067Z |                   | CVE-2019-1551    |
|                   | 1.1.1d-r2     | openssl: Integer overflow in RSAZ
|
2022-10-30T02:36:09.7027571Z |                   |                  |
|                   |               | modular exponentiation on x86_64
|
2022-10-30T02:36:09.7028249Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2019-
1551     |
2022-10-30T02:36:09.7029072Z +                   +------------------+
+                   +---------------+-----------------------------------
------+
2022-10-30T02:36:09.7029827Z |                   | CVE-2020-1971    |
|                   | 1.1.1i-r0     | openssl: EDIPARTYNAME
|
2022-10-30T02:36:09.7030514Z |                   |                  |
|                   |               | NULL pointer de-reference
|
2022-10-30T02:36:09.7031188Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
1971     |
2022-10-30T02:36:09.7031916Z +                   +------------------+
+                   +---------------+-----------------------------------
------+
2022-10-30T02:36:09.7032679Z |                   | CVE-2021-23841   |
|                   | 1.1.1j-r0     | openssl: NULL pointer dereference
|
2022-10-30T02:36:09.7033183Z |                   |                  |
|                   |               | in X509_issuer_and_serial_hash()
|
2022-10-30T02:36:09.7033948Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2021-
23841    |
2022-10-30T02:36:09.7034677Z +                   +------------------+
+                   +---------------+-----------------------------------
------+
2022-10-30T02:36:09.7035441Z |                   | CVE-2021-3449    |
|                   | 1.1.1k-r0     | openssl: NULL pointer dereference
|
2022-10-30T02:36:09.7035929Z |                   |                  |
|                   |               | in signature_algorithms processing
|
2022-10-30T02:36:09.7036613Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2021-
3449     |
2022-10-30T02:36:09.7037354Z +                   +------------------+----
------+                  +---------------+------------------------------
------------+
```

```
2022-10-30T02:36:09.7038128Z |                    | CVE-2019-1563    | LOW
|                    | 1.1.1d-r0     | openssl: information
|
2022-10-30T02:36:09.7038625Z |                    |                  |
|                    |               | disclosure in PKCS7_dataDecode
|
2022-10-30T02:36:09.7039079Z |                    |                  |
|                    |               | and CMS_decrypt_set1_pkey
|
2022-10-30T02:36:09.7039747Z |                    |                  |
|                    |               | -->avd.aquasec.com/nvd/cve-2019-
1563     |
2022-10-30T02:36:09.7040474Z +                    +------------------+
+                   +---------------+-----------------------------------
------+
2022-10-30T02:36:09.7041232Z |                    | CVE-2021-23839   |
|                    | 1.1.1j-r0     | openssl: incorrect SSLv2
|
2022-10-30T02:36:09.7041714Z |                    |                  |
|                    |               | rollback protection
|
2022-10-30T02:36:09.7042392Z |                    |                  |
|                    |               | -->avd.aquasec.com/nvd/cve-2021-
23839    |
2022-10-30T02:36:09.7043293Z +--------------------+------------------+----
------+--------------------+---------------+------------------------------
------------+
2022-10-30T02:36:09.7044168Z | libjpeg-turbo      | CVE-2019-2201    |
HIGH     | 1.5.3-r4           | 1.5.3-r6      | libjpeg-turbo: several
integer           |
2022-10-30T02:36:09.7044693Z |                    |                  |
|                    |               | overflows and subsequent
|
2022-10-30T02:36:09.7045134Z |                    |                  |
|                    |               | segfaults when attempting to
|
2022-10-30T02:36:09.7045588Z |                    |                  |
|                    |               | compress/decompress gigapixel...
|
2022-10-30T02:36:09.7046371Z |                    |                  |
|                    |               | -->avd.aquasec.com/nvd/cve-2019-
2201     |
2022-10-30T02:36:09.7047108Z +                    +------------------+----
------+                   +---------------+------------------------------
------------+
2022-10-30T02:36:09.7047879Z |                    | CVE-2018-14498   |
MEDIUM   |                    | 1.5.3-r5      | libjpeg-turbo: heap-based
buffer         |
2022-10-30T02:36:09.7048600Z |                    |                  |
|                    |               | over-read via crafted 8-bit BMP
|
2022-10-30T02:36:09.7049063Z |                    |                  |
|                    |               | in get_8bit_row in rdbmp.c...
|
2022-10-30T02:36:09.7049747Z |                    |                  |
|                    |               | -->avd.aquasec.com/nvd/cve-2018-
14498    |
```

```
2022-10-30T02:36:09.7050619Z +------------------+-----------------+----
------+-------------------+---------------+------------------------------
------------+
2022-10-30T02:36:09.7051457Z | libssl1.1        | CVE-2020-1967    |
HIGH     | 1.1.1b-r1         | 1.1.1g-r0     | openssl: Segmentation
|
2022-10-30T02:36:09.7051967Z |                  |                  |
|                   |               | fault in SSL_check_chain
|
2022-10-30T02:36:09.7052404Z |                  |                  |
|                   |               | causes denial of service
|
2022-10-30T02:36:09.7053069Z |                  |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
1967     |
2022-10-30T02:36:09.7053796Z +                  +------------------+
+                   +---------------+----------------------------------
------+
2022-10-30T02:36:09.7054542Z |                  | CVE-2021-23840   |
|                   | 1.1.1j-r0     | openssl: integer
|
2022-10-30T02:36:09.7055014Z |                  |                  |
|                   |               | overflow in CipherUpdate
|
2022-10-30T02:36:09.7055680Z |                  |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2021-
23840    |
2022-10-30T02:36:09.7056413Z +                  +------------------+
+                   +---------------+----------------------------------
------+
2022-10-30T02:36:09.7057175Z |                  | CVE-2021-3450    |
|                   | 1.1.1k-r0     | openssl: CA certificate check
|
2022-10-30T02:36:09.7057675Z |                  |                  |
|                   |               | bypass with X509_V_FLAG_X509_STRICT
|
2022-10-30T02:36:09.7058356Z |                  |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2021-
3450     |
2022-10-30T02:36:09.7059089Z +                  +------------------+----
------+                   +---------------+------------------------------
------------+
2022-10-30T02:36:09.7059872Z |                  | CVE-2019-1547    |
MEDIUM   |                   | 1.1.1d-r0     | openssl: side-channel weak
|
2022-10-30T02:36:09.7060367Z |                  |                  |
|                   |               | encryption vulnerability
|
2022-10-30T02:36:09.7061036Z |                  |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2019-
1547     |
2022-10-30T02:36:09.7061754Z +                  +------------------+
+                   +               +----------------------------------
------+
2022-10-30T02:36:09.7062473Z |                  | CVE-2019-1549    |
|                   |               | openssl: information
|
```

```
2022-10-30T02:36:09.7062996Z |                   |                  |
|                   |               | disclosure in fork()
|
2022-10-30T02:36:09.7063671Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2019-
1549     |
2022-10-30T02:36:09.7064398Z +                   +------------------+
+                   +---------------+-----------------------------------
------+
2022-10-30T02:36:09.7065162Z |                   | CVE-2019-1551    |
|                   | 1.1.1d-r2     | openssl: Integer overflow in RSAZ
|
2022-10-30T02:36:09.7065660Z |                   |                  |
|                   |               | modular exponentiation on x86_64
|
2022-10-30T02:36:09.7066335Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2019-
1551     |
2022-10-30T02:36:09.7077265Z +                   +------------------+
+                   +---------------+-----------------------------------
------+
2022-10-30T02:36:09.7078400Z |                   | CVE-2020-1971    |
|                   | 1.1.1i-r0     | openssl: EDIPARTYNAME
|
2022-10-30T02:36:09.7079185Z |                   |                  |
|                   |               | NULL pointer de-reference
|
2022-10-30T02:36:09.7079866Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
1971     |
2022-10-30T02:36:09.7080598Z +                   +------------------+
+                   +---------------+-----------------------------------
------+
2022-10-30T02:36:09.7081353Z |                   | CVE-2021-23841   |
|                   | 1.1.1j-r0     | openssl: NULL pointer dereference
|
2022-10-30T02:36:09.7081867Z |                   |                  |
|                   |               | in X509_issuer_and_serial_hash()
|
2022-10-30T02:36:09.7082571Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2021-
23841    |
2022-10-30T02:36:09.7083428Z +                   +------------------+
+                   +---------------+-----------------------------------
------+
2022-10-30T02:36:09.7084204Z |                   | CVE-2021-3449    |
|                   | 1.1.1k-r0     | openssl: NULL pointer dereference
|
2022-10-30T02:36:09.7084714Z |                   |                  |
|                   |               | in signature_algorithms processing
|
2022-10-30T02:36:09.7085412Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2021-
3449     |
2022-10-30T02:36:09.7086153Z +                   +------------------+----
------+                  +---------------+------------------------------
------------+
```

```
2022-10-30T02:36:09.7120914Z |                    | CVE-2019-1563    | LOW
|                    | 1.1.1d-r0     | openssl: information
|
2022-10-30T02:36:09.7121500Z |                    |                  |
|                    |               | disclosure in PKCS7_dataDecode
|
2022-10-30T02:36:09.7121964Z |                    |                  |
|                    |               | and CMS_decrypt_set1_pkey
|
2022-10-30T02:36:09.7122657Z |                    |                  |
|                    |               | -->avd.aquasec.com/nvd/cve-2019-
1563     |
2022-10-30T02:36:09.7123545Z +                    +------------------+
+                   +---------------+-----------------------------------
------+
2022-10-30T02:36:09.7124321Z |                    | CVE-2021-23839   |
|                    | 1.1.1j-r0     | openssl: incorrect SSLv2
|
2022-10-30T02:36:09.7124799Z |                    |                  |
|                    |               | rollback protection
|
2022-10-30T02:36:09.7125656Z |                    |                  |
|                    |               | -->avd.aquasec.com/nvd/cve-2021-
23839    |
2022-10-30T02:36:09.7126443Z +--------------------+------------------+----
------+--------------------+---------------+------------------------------
------------+
2022-10-30T02:36:09.7127285Z | libtasn1           | CVE-2018-1000654 |
MEDIUM   | 4.13-r0            | 4.14-r0       | libtasn1: Infinite loop in
|
2022-10-30T02:36:09.7127817Z |                    |                  |
|                    |               | _asn1_expand_object_id(ptree)
|
2022-10-30T02:36:09.7128270Z |                    |                  |
|                    |               | leads to memory exhaustion
|
2022-10-30T02:36:09.7128945Z |                    |                  |
|                    |               | -->avd.aquasec.com/nvd/cve-2018-
1000654  |
2022-10-30T02:36:09.7129738Z +--------------------+------------------+----
------+--------------------+---------------+------------------------------
------------+
2022-10-30T02:36:09.7130703Z | libx11             | CVE-2020-14363   |
HIGH     | 1.6.7-r0           | 1.6.12-r0     | libX11: integer overflow
leads           |
2022-10-30T02:36:09.7131232Z |                    |                  |
|                    |               | to double free in locale handling
|
2022-10-30T02:36:09.7131909Z |                    |                  |
|                    |               | -->avd.aquasec.com/nvd/cve-2020-
14363    |
2022-10-30T02:36:09.7132647Z +                    +------------------+----
------+                  +---------------+------------------------------
------------+
2022-10-30T02:36:09.7133424Z |                    | CVE-2020-14344   |
MEDIUM   |                    | 1.6.10-r0     | libX11: Heap overflow in
|
```

```
2022-10-30T02:36:09.7133913Z |                    |                  |
|                    |               | the X input method client
|
2022-10-30T02:36:09.7134586Z |                    |                  |
|                    |               | -->avd.aquasec.com/nvd/cve-2020-
14344    |
2022-10-30T02:36:09.7135367Z +--------------------+------------------+----
------+--------------------+---------------+------------------------------
------------+
2022-10-30T02:36:09.7136217Z | musl               | CVE-2019-14697   |
CRITICAL | 1.1.20-r4          | 1.1.20-r5     | musl libc through 1.1.23
|
2022-10-30T02:36:09.7136947Z |                    |                  |
|                    |               | has an x87 floating-point
|
2022-10-30T02:36:09.7137396Z |                    |                  |
|                    |               | stack adjustment im ......
|
2022-10-30T02:36:09.7138065Z |                    |                  |
|                    |               | -->avd.aquasec.com/nvd/cve-2019-
14697    |
2022-10-30T02:36:09.7138799Z +                    +------------------+----
------+                  +---------------+------------------------------
------------+
2022-10-30T02:36:09.7139585Z |                    | CVE-2020-28928   |
MEDIUM   |                    | 1.1.20-r6     | In musl libc through
1.2.1,               |
2022-10-30T02:36:09.7140081Z |                    |                  |
|                    |               | wcsnrtombs mishandles
|
2022-10-30T02:36:09.7146574Z |                    |                  |
|                    |               | particular combinati ...
|
2022-10-30T02:36:09.7147453Z |                    |                  |
|                    |               | -->avd.aquasec.com/nvd/cve-2020-
28928    |
2022-10-30T02:36:09.7148246Z +--------------------+------------------+----
------+                  +---------------+------------------------------
------------+
2022-10-30T02:36:09.7149089Z | musl-utils         | CVE-2019-14697   |
CRITICAL |                    | 1.1.20-r5     | musl libc through 1.1.23
|
2022-10-30T02:36:09.7150014Z |                    |                  |
|                    |               | has an x87 floating-point
|
2022-10-30T02:36:09.7150467Z |                    |                  |
|                    |               | stack adjustment im ......
|
2022-10-30T02:36:09.7151139Z |                    |                  |
|                    |               | -->avd.aquasec.com/nvd/cve-2019-
14697    |
2022-10-30T02:36:09.7151889Z +                    +------------------+----
------+                  +---------------+------------------------------
------------+
2022-10-30T02:36:09.7152672Z |                    | CVE-2020-28928   |
MEDIUM   |                    | 1.1.20-r6     | In musl libc through
1.2.1,               |
```

```
2022-10-30T02:36:09.7153167Z |                   |                  |
|                   |               | wcsnrtombs mishandles
|
2022-10-30T02:36:09.7153697Z |                   |                  |
|                   |               | particular combinati ...
|
2022-10-30T02:36:09.7154378Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
28928    |
2022-10-30T02:36:09.7155166Z +-------------------+------------------+----
------+-------------------+--------------+-----------------------------
------------+
2022-10-30T02:36:09.7156033Z | openjdk8          | CVE-2020-14583   |
HIGH     | 8.212.04-r0       | 8.272.10-r0   | OpenJDK: Bypass of
boundary checks       |
2022-10-30T02:36:09.7156554Z |                   |                  |
|                   |               | in nio.Buffer via concurrent
|
2022-10-30T02:36:09.7157012Z |                   |                  |
|                   |               | access (Libraries, 8238920)...
|
2022-10-30T02:36:09.7157705Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
14583    |
2022-10-30T02:36:09.7158434Z +                   +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7160308Z |                   | CVE-2020-14593   |
|                   |               | OpenJDK: Incomplete bounds checks
in     |
2022-10-30T02:36:09.7160815Z |                   |                  |
|                   |               | Affine Transformations (2D,
8240119)     |
2022-10-30T02:36:09.7161524Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
14593    |
2022-10-30T02:36:09.7162254Z +                   +------------------+
+                   +---------------+-----------------------------------
------+
2022-10-30T02:36:09.7163024Z |                   | CVE-2020-2604    |
|                   | 8.242.08-r0   | OpenJDK: Serialization filter
|
2022-10-30T02:36:09.7163638Z |                   |                  |
|                   |               | changes via jdk.serialFilter
|
2022-10-30T02:36:09.7164084Z |                   |                  |
|                   |               | property modification
|
2022-10-30T02:36:09.7164522Z |                   |                  |
|                   |               | (Serialization, 8231422)
|
2022-10-30T02:36:09.7165198Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
2604     |
2022-10-30T02:36:09.7165926Z +                   +------------------+
+                   +---------------+-----------------------------------
------+
```

```
2022-10-30T02:36:09.7166694Z |                   | CVE-2020-2803    |
|                   | 8.252.09-r0   | OpenJDK: Incorrect bounds checks
|
2022-10-30T02:36:09.7167361Z |                   |                  |
|                   |               | in NIO Buffers (Libraries, 8234841)
|
2022-10-30T02:36:09.7168057Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
2803     |
2022-10-30T02:36:09.7168751Z +                   +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7169488Z |                   | CVE-2020-2805    |
|                   |               | OpenJDK: Incorrect type checks
|
2022-10-30T02:36:09.7169967Z |                   |                  |
|                   |               | in MethodType.readObject()
|
2022-10-30T02:36:09.7170412Z |                   |                  |
|                   |               | (Libraries, 8235274)
|
2022-10-30T02:36:09.7171082Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
2805     |
2022-10-30T02:36:09.7171915Z +                   +------------------+----
------+                   +---------------+------------------------------
------------+
2022-10-30T02:36:09.7172706Z |                   | CVE-2019-2745    |
MEDIUM   |                   | 8.222.10-r0   | OpenJDK: Side-channel
attack             |
2022-10-30T02:36:09.7173212Z |                   |                  |
|                   |               | risks in Elliptic Curve (EC)
|
2022-10-30T02:36:09.7173672Z |                   |                  |
|                   |               | cryptography (Security, 8208698)
|
2022-10-30T02:36:09.7174351Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2019-
2745     |
2022-10-30T02:36:09.7175066Z +                   +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7175800Z |                   | CVE-2019-2762    |
|                   |               | OpenJDK: Insufficient checks
|
2022-10-30T02:36:09.7176274Z |                   |                  |
|                   |               | of suppressed exceptions in
|
2022-10-30T02:36:09.7176730Z |                   |                  |
|                   |               | deserialization (Utilities,
8212328)     |
2022-10-30T02:36:09.7177416Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2019-
2762     |
2022-10-30T02:36:09.7178129Z +                   +------------------+
+                   +               +-----------------------------------
------+
```

```
2022-10-30T02:36:09.7178884Z |                  | CVE-2019-2769    |
|                  |              | OpenJDK: Unbounded memory
|
2022-10-30T02:36:09.7179355Z |                  |                  |
|                  |              | allocation during deserialization
|
2022-10-30T02:36:09.7179824Z |                  |                  |
|                  |              | in Collections (Utilities, 8213432)
|
2022-10-30T02:36:09.7180514Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2019-
2769     |
2022-10-30T02:36:09.7181229Z +                  +------------------+
+                  +              +-----------------------------------
------+
2022-10-30T02:36:09.7181959Z |                  | CVE-2019-2816    |
|                  |              | OpenJDK: Missing URL format
|
2022-10-30T02:36:09.7182441Z |                  |                  |
|                  |              | validation (Networking, 8221518)
|
2022-10-30T02:36:09.7183119Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2019-
2816     |
2022-10-30T02:36:09.7183929Z +                  +------------------+
+                  +--------------+-----------------------------------
------+
2022-10-30T02:36:09.7184694Z |                  | CVE-2019-2949    |
|                  | 8.232.09-r0  | OpenJDK: Improper handling
|
2022-10-30T02:36:09.7185187Z |                  |                  |
|                  |              | of Kerberos proxy credentials
|
2022-10-30T02:36:09.7185631Z |                  |                  |
|                  |              | (Kerberos, 8220302)
|
2022-10-30T02:36:09.7186293Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2019-
2949     |
2022-10-30T02:36:09.7187011Z +                  +------------------+
+                  +              +-----------------------------------
------+
2022-10-30T02:36:09.7187799Z |                  | CVE-2019-2958    |
|                  |              | OpenJDK: Incorrect
|
2022-10-30T02:36:09.7188257Z |                  |                  |
|                  |              | escaping of command line
|
2022-10-30T02:36:09.7188693Z |                  |                  |
|                  |              | arguments in ProcessImpl
|
2022-10-30T02:36:09.7189130Z |                  |                  |
|                  |              | on Windows (Libraries,...
|
2022-10-30T02:36:09.7250369Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2019-
2958     |
```

```
2022-10-30T02:36:09.7251186Z +                  +------------------+
+                  +              +-----------------------------------
------+
2022-10-30T02:36:09.7251937Z |                  | CVE-2019-2975    |
|                  |              | OpenJDK: Unexpected exception
thrown     |
2022-10-30T02:36:09.7252469Z |                  |                  |
|                  |              | during regular expression
processing     |
2022-10-30T02:36:09.7252943Z |                  |                  |
|                  |              | in Nashorn (Scripting, 8223518)...
|
2022-10-30T02:36:09.7253640Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2019-
2975     |
2022-10-30T02:36:09.7254353Z +                  +------------------+
+                  +              +-----------------------------------
------+
2022-10-30T02:36:09.7255090Z |                  | CVE-2019-2989    |
|                  |              | OpenJDK: Incorrect handling of HTTP
|
2022-10-30T02:36:09.7255589Z |                  |                  |
|                  |              | proxy responses in
HttpURLConnection     |
2022-10-30T02:36:09.7256049Z |                  |                  |
|                  |              | (Networking, 8225298)
|
2022-10-30T02:36:09.7256718Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2019-
2989     |
2022-10-30T02:36:09.7257429Z +                  +------------------+
+                  +              +-----------------------------------
------+
2022-10-30T02:36:09.7258153Z |                  | CVE-2019-2999    |
|                  |              | OpenJDK: Insufficient filtering
|
2022-10-30T02:36:09.7258629Z |                  |                  |
|                  |              | of HTML event attributes in
|
2022-10-30T02:36:09.7259070Z |                  |                  |
|                  |              | Javadoc (Javadoc, 8226765)
|
2022-10-30T02:36:09.7259918Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2019-
2999     |
2022-10-30T02:36:09.7260652Z +                  +------------------+
+                  +--------------+-----------------------------------
------+
2022-10-30T02:36:09.7261399Z |                  | CVE-2019-7317    |
|                  | 8.222.10-r0  | libpng: use-after-free in
|
2022-10-30T02:36:09.7261878Z |                  |                  |
|                  |              | png_image_free in png.c
|
2022-10-30T02:36:09.7262544Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2019-
7317     |
```

```
2022-10-30T02:36:09.7263278Z +                  +------------------+
+                  +---------------+-----------------------------------
------+
2022-10-30T02:36:09.7264051Z |                  | CVE-2020-14556   |
|                  | 8.272.10-r0   | OpenJDK: Incorrect handling
|
2022-10-30T02:36:09.7264645Z |                  |                  |
|                  |               | of access control context in
|
2022-10-30T02:36:09.7265103Z |                  |                  |
|                  |               | ForkJoinPool (Libraries, 8237117)
|
2022-10-30T02:36:09.7265793Z |                  |                  |
|                  |               | -->avd.aquasec.com/nvd/cve-2020-
14556    |
2022-10-30T02:36:09.7266508Z +                  +------------------+
+                  +               +-----------------------------------
------+
2022-10-30T02:36:09.7267245Z |                  | CVE-2020-14621   |
|                  |               | OpenJDK: XML validation
manipulation     |
2022-10-30T02:36:09.7267738Z |                  |                  |
|                  |               | due to incomplete application of
|
2022-10-30T02:36:09.7268418Z |                  |                  |
|                  |               | the use-grammar-pool-only
feature...     |
2022-10-30T02:36:09.7269111Z |                  |                  |
|                  |               | -->avd.aquasec.com/nvd/cve-2020-
14621    |
2022-10-30T02:36:09.7269823Z +                  +------------------+
+                  +               +-----------------------------------
------+
2022-10-30T02:36:09.7270547Z |                  | CVE-2020-14792   |
|                  |               | OpenJDK: Integer overflow
|
2022-10-30T02:36:09.7271223Z |                  |                  |
|                  |               | leading to out-of-bounds
|
2022-10-30T02:36:09.7271671Z |                  |                  |
|                  |               | access (Hotspot, 8241114)
|
2022-10-30T02:36:09.7272325Z |                  |                  |
|                  |               | -->avd.aquasec.com/nvd/cve-2020-
14792    |
2022-10-30T02:36:09.7273052Z +                  +------------------+
+                  +               +-----------------------------------
------+
2022-10-30T02:36:09.7273790Z |                  | CVE-2020-14803   |
|                  |               | OpenJDK: Race condition in NIO
Buffer    |
2022-10-30T02:36:09.7274295Z |                  |                  |
|                  |               | boundary checks (Libraries,
8244136)     |
2022-10-30T02:36:09.7274983Z |                  |                  |
|                  |               | -->avd.aquasec.com/nvd/cve-2020-
14803    |
```

```
2022-10-30T02:36:09.7275715Z +                   +------------------+
+                   +---------------+-----------------------------------
------+
2022-10-30T02:36:09.7276469Z |                   | CVE-2020-2593    |
|                   | 8.242.08-r0   | OpenJDK: Incorrect
|
2022-10-30T02:36:09.7277030Z |                   |                  |
|                   |               | isBuiltinStreamHandler check
|
2022-10-30T02:36:09.7277479Z |                   |                  |
|                   |               | causing URL normalization
|
2022-10-30T02:36:09.7277926Z |                   |                  |
|                   |               | issues (Networking, 8228548)
|
2022-10-30T02:36:09.7278656Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
2593     |
2022-10-30T02:36:09.7279374Z +                   +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7280094Z |                   | CVE-2020-2601    |
|                   |               | OpenJDK: Use of unsafe
|
2022-10-30T02:36:09.7280779Z |                   |                  |
|                   |               | RSA-MD5 checksum in Kerberos
|
2022-10-30T02:36:09.7281309Z |                   |                  |
|                   |               | TGS (Security, 8229951)
|
2022-10-30T02:36:09.7281988Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
2601     |
2022-10-30T02:36:09.7282719Z +                   +------------------+
+                   +---------------+-----------------------------------
------+
2022-10-30T02:36:09.7283618Z |                   | CVE-2020-2781    |
|                   | 8.252.09-r0   | OpenJDK: Re-use of single
|
2022-10-30T02:36:09.7284102Z |                   |                  |
|                   |               | TLS session for new
|
2022-10-30T02:36:09.7284547Z |                   |                  |
|                   |               | connections (JSSE, 8234408)
|
2022-10-30T02:36:09.7285238Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
2781     |
2022-10-30T02:36:09.7286038Z +                   +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7286769Z |                   | CVE-2020-2800    |
|                   |               | OpenJDK: CRLF injection into HTTP
|
2022-10-30T02:36:09.7287259Z |                   |                  |
|                   |               | headers in HttpServer (Lightweight
|
```

```
2022-10-30T02:36:09.7310441Z |                   |                  |
|                   |               | HTTP Server, 8234825)...
|
2022-10-30T02:36:09.7311423Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
2800     |
2022-10-30T02:36:09.7312188Z +                   +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7312920Z |                   | CVE-2020-2830    |
|                   |               | OpenJDK: Regular expression DoS
|
2022-10-30T02:36:09.7313411Z |                   |                  |
|                   |               | in Scanner (Concurrency, 8236201)
|
2022-10-30T02:36:09.7314097Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
2830     |
2022-10-30T02:36:09.7314839Z +                   +------------------+----
------+                   +---------------+------------------------------
------------+
2022-10-30T02:36:09.7315638Z |                   | CVE-2019-2766    | LOW
|                   | 8.222.10-r0   | OpenJDK: Insufficient permission
|
2022-10-30T02:36:09.7316143Z |                   |                  |
|                   |               | checks for file:// URLs on
|
2022-10-30T02:36:09.7316761Z |                   |                  |
|                   |               | Windows (Networking, 8213431)
|
2022-10-30T02:36:09.7317450Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2019-
2766     |
2022-10-30T02:36:09.7318167Z +                   +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7318886Z |                   | CVE-2019-2786    |
|                   |               | OpenJDK: Insufficient
|
2022-10-30T02:36:09.7319358Z |                   |                  |
|                   |               | restriction of privileges in
|
2022-10-30T02:36:09.7319820Z |                   |                  |
|                   |               | AccessController (Security,
8216381)     |
2022-10-30T02:36:09.7320610Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2019-
2786     |
2022-10-30T02:36:09.7321327Z +                   +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7322069Z |                   | CVE-2019-2842    |
|                   |               | OpenJDK: Missing array bounds check
|
2022-10-30T02:36:09.7322563Z |                   |                  |
|                   |               | in crypto providers (JCE, 8223511)
|
```

```
2022-10-30T02:36:09.7326087Z |                   |                   |
|                   |               | -->avd.aquasec.com/nvd/cve-2019-
2842     |
2022-10-30T02:36:09.7332898Z +                   +-------------------+
+                   +---------------+-------------------------------------
------+
2022-10-30T02:36:09.7335452Z |                   | CVE-2019-2894     |
|                   | 8.232.09-r0   | OpenJDK: Side-channel
|
2022-10-30T02:36:09.7337497Z |                   |                   |
|                   |               | vulnerability in the ECDSA
|
2022-10-30T02:36:09.7342277Z |                   |                   |
|                   |               | implementation (Security, 8228825)
|
2022-10-30T02:36:09.7346126Z |                   |                   |
|                   |               | -->avd.aquasec.com/nvd/cve-2019-
2894     |
2022-10-30T02:36:09.7349950Z +                   +-------------------+
+                   +               +-------------------------------------
------+
2022-10-30T02:36:09.7355149Z |                   | CVE-2019-2933     |
|                   |               | OpenJDK: FilePermission checks
|
2022-10-30T02:36:09.7357140Z |                   |                   |
|                   |               | not preformed correctly on
|
2022-10-30T02:36:09.7360514Z |                   |                   |
|                   |               | Windows (Libraries, 8213429)
|
2022-10-30T02:36:09.7364395Z |                   |                   |
|                   |               | -->avd.aquasec.com/nvd/cve-2019-
2933     |
2022-10-30T02:36:09.7368201Z +                   +-------------------+
+                   +               +-------------------------------------
------+
2022-10-30T02:36:09.7373459Z |                   | CVE-2019-2945     |
|                   |               | OpenJDK: Missing restrictions
|
2022-10-30T02:36:09.7376825Z |                   |                   |
|                   |               | on use of custom SocketImpl
|
2022-10-30T02:36:09.7378842Z |                   |                   |
|                   |               | (Networking, 8218573)
|
2022-10-30T02:36:09.7384309Z |                   |                   |
|                   |               | -->avd.aquasec.com/nvd/cve-2019-
2945     |
2022-10-30T02:36:09.7389562Z +                   +-------------------+
+                   +               +-------------------------------------
------+
2022-10-30T02:36:09.7391396Z |                   | CVE-2019-2962     |
|                   |               | OpenJDK: NULL pointer dereference
|
2022-10-30T02:36:09.7395108Z |                   |                   |
|                   |               | in DrawGlyphList (2D, 8222690)
|
```

```
2022-10-30T02:36:09.7395929Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2019-
2962     |
2022-10-30T02:36:09.7396660Z +                  +------------------+
+                  +              +-----------------------------------
------+
2022-10-30T02:36:09.7397393Z |                  | CVE-2019-2964    |
|                  |              | OpenJDK: Unexpected exception
|
2022-10-30T02:36:09.7400714Z |                  |                  |
|                  |              | thrown by Pattern processing
|
2022-10-30T02:36:09.7401225Z |                  |                  |
|                  |              | crafted regular expression
|
2022-10-30T02:36:09.7401675Z |                  |                  |
|                  |              | (Concurrency, 8222684)...
|
2022-10-30T02:36:09.7402434Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2019-
2964     |
2022-10-30T02:36:09.7403276Z +                  +------------------+
+                  +              +-----------------------------------
------+
2022-10-30T02:36:09.7404025Z |                  | CVE-2019-2973    |
|                  |              | OpenJDK: Unexpected exception
thrown     |
2022-10-30T02:36:09.7404539Z |                  |                  |
|                  |              | by XPathParser processing crafted
|
2022-10-30T02:36:09.7405013Z |                  |                  |
|                  |              | XPath expression (JAXP, 8223505)...
|
2022-10-30T02:36:09.7405704Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2019-
2973     |
2022-10-30T02:36:09.7406427Z +                  +------------------+
+                  +              +-----------------------------------
------+
2022-10-30T02:36:09.7407154Z |                  | CVE-2019-2978    |
|                  |              | OpenJDK: Incorrect handling
|
2022-10-30T02:36:09.7407631Z |                  |                  |
|                  |              | of nested jar: URLs in Jar
|
2022-10-30T02:36:09.7408084Z |                  |                  |
|                  |              | URL handler (Networking,...
|
2022-10-30T02:36:09.7408764Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2019-
2978     |
2022-10-30T02:36:09.7409463Z +                  +------------------+
+                  +              +-----------------------------------
------+
2022-10-30T02:36:09.7410193Z |                  | CVE-2019-2981    |
|                  |              | OpenJDK: Unexpected exception
|
```

```
2022-10-30T02:36:09.7410680Z |                  |                  |
|                   |              | thrown by XPath processing crafted
|
2022-10-30T02:36:09.7411146Z |                  |                  |
|                   |              | XPath expression (JAXP, 8224532)...
|
2022-10-30T02:36:09.7411834Z |                  |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2019-
2981     |
2022-10-30T02:36:09.7412708Z +                  +------------------+
+                   +              +-----------------------------------
------+
2022-10-30T02:36:09.7413454Z |                  | CVE-2019-2983    |
|                   |              | OpenJDK: Unexpected exception
thrown     |
2022-10-30T02:36:09.7413951Z |                  |                  |
|                   |              | during Font object deserialization
|
2022-10-30T02:36:09.7414404Z |                  |                  |
|                   |              | (Serialization, 8224915)
|
2022-10-30T02:36:09.7415075Z |                  |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2019-
2983     |
2022-10-30T02:36:09.7415788Z +                  +------------------+
+                   +              +-----------------------------------
------+
2022-10-30T02:36:09.7416612Z |                  | CVE-2019-2987    |
|                   |              | OpenJDK: Missing glyph bitmap
|
2022-10-30T02:36:09.7417085Z |                  |                  |
|                   |              | image dimension check in
|
2022-10-30T02:36:09.7417534Z |                  |                  |
|                   |              | FreetypeFontScaler (2D, 8225286)
|
2022-10-30T02:36:09.7418216Z |                  |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2019-
2987     |
2022-10-30T02:36:09.7418933Z +                  +------------------+
+                   +              +-----------------------------------
------+
2022-10-30T02:36:09.7419674Z |                  | CVE-2019-2988    |
|                   |              | OpenJDK: Integer overflow in bounds
|
2022-10-30T02:36:09.7420161Z |                  |                  |
|                   |              | check in SunGraphics2D (2D,
8225292)     |
2022-10-30T02:36:09.7420853Z |                  |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2019-
2988     |
2022-10-30T02:36:09.7421568Z +                  +------------------+
+                   +              +-----------------------------------
------+
2022-10-30T02:36:09.7422292Z |                  | CVE-2019-2992    |
|                   |              | OpenJDK: Excessive memory
|
```

```
2022-10-30T02:36:09.7422776Z |                    |                  |
|                    |               | allocation in CMap when reading
|
2022-10-30T02:36:09.7423231Z |                    |                  |
|                    |               | TrueType font (2D, 8225597)...
|
2022-10-30T02:36:09.7423911Z |                    |                  |
|                    |               | -->avd.aquasec.com/nvd/cve-2019-
2992     |
2022-10-30T02:36:09.7424650Z +                    +------------------+
+                    +---------------+-----------------------------------
------+
2022-10-30T02:36:09.7425418Z |                    | CVE-2020-14577   |
|                    | 8.272.10-r0   | OpenJDK: HostnameChecker does
|
2022-10-30T02:36:09.7425919Z |                    |                  |
|                    |               | not ensure X.509 certificate
|
2022-10-30T02:36:09.7426370Z |                    |                  |
|                    |               | names are in normalized form...
|
2022-10-30T02:36:09.7427046Z |                    |                  |
|                    |               | -->avd.aquasec.com/nvd/cve-2020-
14577    |
2022-10-30T02:36:09.7427762Z +                    +------------------+
+                    +               +-----------------------------------
------+
2022-10-30T02:36:09.7428580Z |                    | CVE-2020-14578   |
|                    |               | OpenJDK: Unexpected exception
|
2022-10-30T02:36:09.7429068Z |                    |                  |
|                    |               | raised by DerInputStream
|
2022-10-30T02:36:09.7429505Z |                    |                  |
|                    |               | (Libraries, 8237731)
|
2022-10-30T02:36:09.7430168Z |                    |                  |
|                    |               | -->avd.aquasec.com/nvd/cve-2020-
14578    |
2022-10-30T02:36:09.7430867Z +                    +------------------+
+                    +               +-----------------------------------
------+
2022-10-30T02:36:09.7431598Z |                    | CVE-2020-14579   |
|                    |               | OpenJDK: Unexpected exception
|
2022-10-30T02:36:09.7432079Z |                    |                  |
|                    |               | raised by DerValue.equals()
|
2022-10-30T02:36:09.7432609Z |                    |                  |
|                    |               | (Libraries, 8237736)
|
2022-10-30T02:36:09.7433291Z |                    |                  |
|                    |               | -->avd.aquasec.com/nvd/cve-2020-
14579    |
2022-10-30T02:36:09.7434007Z +                    +------------------+
+                    +               +-----------------------------------
------+
```

```
2022-10-30T02:36:09.7434740Z |                  | CVE-2020-14581   |
|                   |              | OpenJDK: Information disclosure
|
2022-10-30T02:36:09.7435230Z |                  |                  |
|                   |              | in color management (2D, 8238002)
|
2022-10-30T02:36:09.7435914Z |                  |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2020-
14581    |
2022-10-30T02:36:09.7436638Z +                  +------------------+
+                   +              +-----------------------------------
------+
2022-10-30T02:36:09.7437358Z |                  | CVE-2020-14779   |
|                   |              | OpenJDK: High memory usage
|
2022-10-30T02:36:09.7437836Z |                  |                  |
|                   |              | during deserialization of Proxy
|
2022-10-30T02:36:09.7438291Z |                  |                  |
|                   |              | class with many interfaces...
|
2022-10-30T02:36:09.7438961Z |                  |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2020-
14779    |
2022-10-30T02:36:09.7439676Z +                  +------------------+
+                   +              +-----------------------------------
------+
2022-10-30T02:36:09.7440399Z |                  | CVE-2020-14781   |
|                   |              | OpenJDK: Credentials sent
|
2022-10-30T02:36:09.7440871Z |                  |                  |
|                   |              | over unencrypted LDAP
|
2022-10-30T02:36:09.7441293Z |                  |                  |
|                   |              | connection (JNDI, 8237990)
|
2022-10-30T02:36:09.7441966Z |                  |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2020-
14781    |
2022-10-30T02:36:09.7442684Z +                  +------------------+
+                   +              +-----------------------------------
------+
2022-10-30T02:36:09.7443532Z |                  | CVE-2020-14782   |
|                   |              | OpenJDK: Certificate blacklist
|
2022-10-30T02:36:09.7444024Z |                  |                  |
|                   |              | bypass via alternate certificate
|
2022-10-30T02:36:09.7444573Z |                  |                  |
|                   |              | encodings (Libraries, 8237995)
|
2022-10-30T02:36:09.7445262Z |                  |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2020-
14782    |
2022-10-30T02:36:09.7445981Z +                  +------------------+
+                   +              +-----------------------------------
------+
```

```
2022-10-30T02:36:09.7446709Z |                   | CVE-2020-14796   |
|                   |               | OpenJDK: Missing permission
|
2022-10-30T02:36:09.7447181Z |                   |                  |
|                   |               | check in path to URI
|
2022-10-30T02:36:09.7447634Z |                   |                  |
|                   |               | conversion (Libraries, 8242680)
|
2022-10-30T02:36:09.7448320Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
14796    |
2022-10-30T02:36:09.7449121Z +                   +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7449845Z |                   | CVE-2020-14797   |
|                   |               | OpenJDK: Incomplete check for
|
2022-10-30T02:36:09.7450331Z |                   |                  |
|                   |               | invalid characters in URI to
|
2022-10-30T02:36:09.7450781Z |                   |                  |
|                   |               | path conversion (Libraries,...
|
2022-10-30T02:36:09.7451462Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
14797    |
2022-10-30T02:36:09.7452173Z +                   +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7452908Z |                   | CVE-2020-14798   |
|                   |               | OpenJDK: Missing maximum length
check in |
2022-10-30T02:36:09.7453414Z |                   |                  |
|                   |               |
WindowsNativeDispatcher.asNativeBuffer() |
2022-10-30T02:36:09.7453876Z |                   |                  |
|                   |               | (Libraries, 8242695)
|
2022-10-30T02:36:09.7454544Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
14798    |
2022-10-30T02:36:09.7455279Z +                   +------------------+
+                   +---------------+-----------------------------------
------+
2022-10-30T02:36:09.7456043Z |                   | CVE-2020-2583    |
|                   | 8.242.08-r0   | OpenJDK: Incorrect exception
|
2022-10-30T02:36:09.7456557Z |                   |                  |
|                   |               | processing during deserialization
|
2022-10-30T02:36:09.7457005Z |                   |                  |
|                   |               | in BeanContextSupport
|
2022-10-30T02:36:09.7457440Z |                   |                  |
|                   |               | (Serialization, 8224909)
|
```

```
2022-10-30T02:36:09.7458112Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
2583     |
2022-10-30T02:36:09.7458822Z +                   +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7459545Z |                   | CVE-2020-2590    |
|                   |               | OpenJDK: Improper checks of
|
2022-10-30T02:36:09.7460017Z |                   |                  |
|                   |               | SASL message properties in
|
2022-10-30T02:36:09.7460565Z |                   |                  |
|                   |               | GssKrb5Base (Security, 8226352)
|
2022-10-30T02:36:09.7461258Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
2590     |
2022-10-30T02:36:09.7462192Z +                   +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7462930Z |                   | CVE-2020-2654    |
|                   |               | OpenJDK: Excessive memory usage
|
2022-10-30T02:36:09.7463393Z |                   |                  |
|                   |               | in OID processing in X.509
|
2022-10-30T02:36:09.7463851Z |                   |                  |
|                   |               | certificate parsing (Libraries,...
|
2022-10-30T02:36:09.7464660Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
2654     |
2022-10-30T02:36:09.7465377Z +                   +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7466117Z |                   | CVE-2020-2659    |
|                   |               | OpenJDK: Incomplete enforcement
|
2022-10-30T02:36:09.7466602Z |                   |                  |
|                   |               | of maxDatagramSockets limit
|
2022-10-30T02:36:09.7467041Z |                   |                  |
|                   |               | in DatagramChannelImpl
|
2022-10-30T02:36:09.7467472Z |                   |                  |
|                   |               | (Networking, 8231795)
|
2022-10-30T02:36:09.7468146Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
2659     |
2022-10-30T02:36:09.7468887Z +                   +------------------+
+                   +---------------+-----------------------------------
------+
2022-10-30T02:36:09.7469650Z |                   | CVE-2020-2754    |
|                   | 8.252.09-r0   | OpenJDK: Misplaced regular
|
```

```
2022-10-30T02:36:09.7470143Z |                  |                  |
|                   |              | expression syntax error check in
|
2022-10-30T02:36:09.7470610Z |                  |                  |
|                   |              | RegExpScanner (Scripting, 8223898)
|
2022-10-30T02:36:09.7471295Z |                  |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2020-
2754     |
2022-10-30T02:36:09.7472005Z +                  +------------------+
+                   +              +-----------------------------------
------+
2022-10-30T02:36:09.7472745Z |                  | CVE-2020-2755    |
|                   |              | OpenJDK: Incorrect handling of
|
2022-10-30T02:36:09.7473222Z |                  |                  |
|                   |              | empty string nodes in regular
|
2022-10-30T02:36:09.7473663Z |                  |                  |
|                   |              | expression Parser (Scripting,...
|
2022-10-30T02:36:09.7474352Z |                  |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2020-
2755     |
2022-10-30T02:36:09.7475064Z +                  +------------------+
+                   +              +-----------------------------------
------+
2022-10-30T02:36:09.7475795Z |                  | CVE-2020-2756    |
|                   |              | OpenJDK: Incorrect handling
|
2022-10-30T02:36:09.7476360Z |                  |                  |
|                   |              | of references to uninitialized
|
2022-10-30T02:36:09.7476806Z |                  |                  |
|                   |              | class descriptors during
|
2022-10-30T02:36:09.7477257Z |                  |                  |
|                   |              | deserialization (Serialization,...
|
2022-10-30T02:36:09.7477958Z |                  |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2020-
2756     |
2022-10-30T02:36:09.7478707Z +                  +------------------+
+                   +              +-----------------------------------
------+
2022-10-30T02:36:09.7479438Z |                  | CVE-2020-2757    |
|                   |              | OpenJDK: Uncaught
InstantiationError     |
2022-10-30T02:36:09.7479931Z |                  |                  |
|                   |              | exception in ObjectStreamClass
|
2022-10-30T02:36:09.7480472Z |                  |                  |
|                   |              | (Serialization, 8224549)
|
2022-10-30T02:36:09.7481154Z |                  |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2020-
2757     |
```

```
2022-10-30T02:36:09.7481867Z +                  +------------------+
+                  +              +-----------------------------------
------+
2022-10-30T02:36:09.7482601Z |                  | CVE-2020-2773    |
|                  |              | OpenJDK: Unexpected exceptions
|
2022-10-30T02:36:09.7483078Z |                  |                  |
|                  |              | raised by DOMKeyInfoFactory
|
2022-10-30T02:36:09.7484450Z |                  |                  |
|                  |              | and DOMXMLSignatureFactory
|
2022-10-30T02:36:09.7484889Z |                  |                  |
|                  |              | (Security, 8231415)
|
2022-10-30T02:36:09.7485581Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2020-
2773     |
2022-10-30T02:36:09.7486347Z +------------------+------------------+----
------+                  +--------------+--------------------------------
------------+
2022-10-30T02:36:09.7487184Z | openjdk8-jre     | CVE-2020-14583   |
HIGH     |                  | 8.272.10-r0   | OpenJDK: Bypass of
boundary checks       |
2022-10-30T02:36:09.7487717Z |                  |                  |
|                  |              | in nio.Buffer via concurrent
|
2022-10-30T02:36:09.7488174Z |                  |                  |
|                  |              | access (Libraries, 8238920)...
|
2022-10-30T02:36:09.7488863Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2020-
14583    |
2022-10-30T02:36:09.7489582Z +                  +------------------+
+                  +              +-----------------------------------
------+
2022-10-30T02:36:09.7490324Z |                  | CVE-2020-14593   |
|                  |              | OpenJDK: Incomplete bounds checks
in     |
2022-10-30T02:36:09.7490826Z |                  |                  |
|                  |              | Affine Transformations (2D,
8240119)     |
2022-10-30T02:36:09.7491517Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2020-
14593    |
2022-10-30T02:36:09.7492252Z +                  +------------------+
+                  +--------------+-----------------------------------
------+
2022-10-30T02:36:09.7493014Z |                  | CVE-2020-2604    |
|                  | 8.242.08-r0   | OpenJDK: Serialization filter
|
2022-10-30T02:36:09.7493609Z |                  |                  |
|                  |              | changes via jdk.serialFilter
|
2022-10-30T02:36:09.7494051Z |                  |                  |
|                  |              | property modification
|
```

```
2022-10-30T02:36:09.7494486Z |                    |                  |
|                    |               | (Serialization, 8231422)
|
2022-10-30T02:36:09.7495163Z |                    |                  |
|                    |               | -->avd.aquasec.com/nvd/cve-2020-
2604     |
2022-10-30T02:36:09.7495879Z +                    +------------------+
+                    +---------------+-----------------------------------
------+
2022-10-30T02:36:09.7496648Z |                    | CVE-2020-2803    |
|                    | 8.252.09-r0   | OpenJDK: Incorrect bounds checks
|
2022-10-30T02:36:09.7497248Z |                    |                  |
|                    |               | in NIO Buffers (Libraries, 8234841)
|
2022-10-30T02:36:09.7497944Z |                    |                  |
|                    |               | -->avd.aquasec.com/nvd/cve-2020-
2803     |
2022-10-30T02:36:09.7498662Z +                    +------------------+
+                    +               +-----------------------------------
------+
2022-10-30T02:36:09.7499399Z |                    | CVE-2020-2805    |
|                    |               | OpenJDK: Incorrect type checks
|
2022-10-30T02:36:09.7499881Z |                    |                  |
|                    |               | in MethodType.readObject()
|
2022-10-30T02:36:09.7500318Z |                    |                  |
|                    |               | (Libraries, 8235274)
|
2022-10-30T02:36:09.7500986Z |                    |                  |
|                    |               | -->avd.aquasec.com/nvd/cve-2020-
2805     |
2022-10-30T02:36:09.7501734Z +                    +------------------+----
------+                   +---------------+-------------------------------
------------+
2022-10-30T02:36:09.7502520Z |                    | CVE-2019-2745    |
MEDIUM   |                   | 8.222.10-r0   | OpenJDK: Side-channel
attack             |
2022-10-30T02:36:09.7503024Z |                    |                  |
|                    |               | risks in Elliptic Curve (EC)
|
2022-10-30T02:36:09.7503473Z |                    |                  |
|                    |               | cryptography (Security, 8208698)
|
2022-10-30T02:36:09.7504155Z |                    |                  |
|                    |               | -->avd.aquasec.com/nvd/cve-2019-
2745     |
2022-10-30T02:36:09.7504870Z +                    +------------------+
+                    +               +-----------------------------------
------+
2022-10-30T02:36:09.7505604Z |                    | CVE-2019-2762    |
|                    |               | OpenJDK: Insufficient checks
|
2022-10-30T02:36:09.7506080Z |                    |                  |
|                    |               | of suppressed exceptions in
|
```

```
2022-10-30T02:36:09.7506521Z |                   |                  |
|                   |               | deserialization (Utilities,
8212328)     |
2022-10-30T02:36:09.7507206Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2019-
2762     |
2022-10-30T02:36:09.7507918Z +                   +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7508646Z |                   | CVE-2019-2769    |
|                   |               | OpenJDK: Unbounded memory
|
2022-10-30T02:36:09.7509203Z |                   |                  |
|                   |               | allocation during deserialization
|
2022-10-30T02:36:09.7509676Z |                   |                  |
|                   |               | in Collections (Utilities, 8213432)
|
2022-10-30T02:36:09.7510370Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2019-
2769     |
2022-10-30T02:36:09.7511090Z +                   +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7511821Z |                   | CVE-2019-2816    |
|                   |               | OpenJDK: Missing URL format
|
2022-10-30T02:36:09.7512304Z |                   |                  |
|                   |               | validation (Networking, 8221518)
|
2022-10-30T02:36:09.7512982Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2019-
2816     |
2022-10-30T02:36:09.7513795Z +                   +------------------+
+                   +---------------+-----------------------------------
------+
2022-10-30T02:36:09.7514570Z |                   | CVE-2019-2949    |
|                   | 8.232.09-r0   | OpenJDK: Improper handling
|
2022-10-30T02:36:09.7515064Z |                   |                  |
|                   |               | of Kerberos proxy credentials
|
2022-10-30T02:36:09.7515505Z |                   |                  |
|                   |               | (Kerberos, 8220302)
|
2022-10-30T02:36:09.7516171Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2019-
2949     |
2022-10-30T02:36:09.7516884Z +                   +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7517591Z |                   | CVE-2019-2958    |
|                   |               | OpenJDK: Incorrect
|
2022-10-30T02:36:09.7518053Z |                   |                  |
|                   |               | escaping of command line
|
```

```
2022-10-30T02:36:09.7518489Z |                  |                  |
|                  |              | arguments in ProcessImpl
|
2022-10-30T02:36:09.7518931Z |                  |                  |
|                  |              | on Windows (Libraries,...
|
2022-10-30T02:36:09.7519608Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2019-
2958     |
2022-10-30T02:36:09.7520328Z +                  +------------------+
+                  +              +-----------------------------------
------+
2022-10-30T02:36:09.7521066Z |                  | CVE-2019-2975    |
|                  |              | OpenJDK: Unexpected exception
thrown     |
2022-10-30T02:36:09.7521578Z |                  |                  |
|                  |              | during regular expression
processing     |
2022-10-30T02:36:09.7522054Z |                  |                  |
|                  |              | in Nashorn (Scripting, 8223518)...
|
2022-10-30T02:36:09.7522735Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2019-
2975     |
2022-10-30T02:36:09.7523594Z +                  +------------------+
+                  +              +-----------------------------------
------+
2022-10-30T02:36:09.7524341Z |                  | CVE-2019-2989    |
|                  |              | OpenJDK: Incorrect handling of HTTP
|
2022-10-30T02:36:09.7524832Z |                  |                  |
|                  |              | proxy responses in
HttpURLConnection     |
2022-10-30T02:36:09.7525393Z |                  |                  |
|                  |              | (Networking, 8225298)
|
2022-10-30T02:36:09.7526067Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2019-
2989     |
2022-10-30T02:36:09.7526784Z +                  +------------------+
+                  +              +-----------------------------------
------+
2022-10-30T02:36:09.7527513Z |                  | CVE-2019-2999    |
|                  |              | OpenJDK: Insufficient filtering
|
2022-10-30T02:36:09.7527977Z |                  |                  |
|                  |              | of HTML event attributes in
|
2022-10-30T02:36:09.7528422Z |                  |                  |
|                  |              | Javadoc (Javadoc, 8226765)
|
2022-10-30T02:36:09.7529101Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2019-
2999     |
2022-10-30T02:36:09.7529916Z +                  +------------------+
+                  +--------------+-----------------------------------
------+
```

```
2022-10-30T02:36:09.7530685Z |                   | CVE-2019-7317    |
|                   | 8.222.10-r0   | libpng: use-after-free in
|
2022-10-30T02:36:09.7531173Z |                   |                  |
|                   |               | png_image_free in png.c
|
2022-10-30T02:36:09.7531837Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2019-
7317     |
2022-10-30T02:36:09.7532568Z +                   +------------------+
+                   +---------------+-----------------------------------
------+
2022-10-30T02:36:09.7533335Z |                   | CVE-2020-14556   |
|                   | 8.272.10-r0   | OpenJDK: Incorrect handling
|
2022-10-30T02:36:09.7533835Z |                   |                  |
|                   |               | of access control context in
|
2022-10-30T02:36:09.7534296Z |                   |                  |
|                   |               | ForkJoinPool (Libraries, 8237117)
|
2022-10-30T02:36:09.7534981Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
14556    |
2022-10-30T02:36:09.7535692Z +                   +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7536427Z |                   | CVE-2020-14621   |
|                   |               | OpenJDK: XML validation
manipulation     |
2022-10-30T02:36:09.7536916Z |                   |                  |
|                   |               | due to incomplete application of
|
2022-10-30T02:36:09.7537597Z |                   |                  |
|                   |               | the use-grammar-pool-only
feature...     |
2022-10-30T02:36:09.7538287Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
14621    |
2022-10-30T02:36:09.7538987Z +                   +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7539712Z |                   | CVE-2020-14792   |
|                   |               | OpenJDK: Integer overflow
|
2022-10-30T02:36:09.7540387Z |                   |                  |
|                   |               | leading to out-of-bounds
|
2022-10-30T02:36:09.7540836Z |                   |                  |
|                   |               | access (Hotspot, 8241114)
|
2022-10-30T02:36:09.7541506Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
14792    |
2022-10-30T02:36:09.7542311Z +                   +------------------+
+                   +               +-----------------------------------
------+
```

```
2022-10-30T02:36:09.7543050Z |                   | CVE-2020-14803   |
|                   |               | OpenJDK: Race condition in NIO
Buffer    |
2022-10-30T02:36:09.7543552Z |                   |                  |
|                   |               | boundary checks (Libraries,
8244136)     |
2022-10-30T02:36:09.7544240Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
14803    |
2022-10-30T02:36:09.7544972Z +                   +------------------+
+                   +---------------+-----------------------------------
------+
2022-10-30T02:36:09.7545734Z |                   | CVE-2020-2593    |
|                   | 8.242.08-r0   | OpenJDK: Incorrect
|
2022-10-30T02:36:09.7546293Z |                   |                  |
|                   |               | isBuiltinStreamHandler check
|
2022-10-30T02:36:09.7546743Z |                   |                  |
|                   |               | causing URL normalization
|
2022-10-30T02:36:09.7547188Z |                   |                  |
|                   |               | issues (Networking, 8228548)
|
2022-10-30T02:36:09.7547873Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
2593     |
2022-10-30T02:36:09.7548583Z +                   +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7549306Z |                   | CVE-2020-2601    |
|                   |               | OpenJDK: Use of unsafe
|
2022-10-30T02:36:09.7549974Z |                   |                  |
|                   |               | RSA-MD5 checksum in Kerberos
|
2022-10-30T02:36:09.7550434Z |                   |                  |
|                   |               | TGS (Security, 8229951)
|
2022-10-30T02:36:09.7551096Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
2601     |
2022-10-30T02:36:09.7551830Z +                   +------------------+
+                   +---------------+-----------------------------------
------+
2022-10-30T02:36:09.7552593Z |                   | CVE-2020-2781    |
|                   | 8.252.09-r0   | OpenJDK: Re-use of single
|
2022-10-30T02:36:09.7553067Z |                   |                  |
|                   |               | TLS session for new
|
2022-10-30T02:36:09.7553503Z |                   |                  |
|                   |               | connections (JSSE, 8234408)
|
2022-10-30T02:36:09.7554182Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
2781     |
```

```
2022-10-30T02:36:09.7554897Z +                  +------------------+
+                  +              +-----------------------------------
------+
2022-10-30T02:36:09.7555626Z |                  | CVE-2020-2800    |
|                  |              | OpenJDK: CRLF injection into HTTP
|
2022-10-30T02:36:09.7556118Z |                  |                  |
|                  |              | headers in HttpServer (Lightweight
|
2022-10-30T02:36:09.7556575Z |                  |                  |
|                  |              | HTTP Server, 8234825)...
|
2022-10-30T02:36:09.7557239Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2020-
2800     |
2022-10-30T02:36:09.7558047Z +                  +------------------+
+                  +              +-----------------------------------
------+
2022-10-30T02:36:09.7558787Z |                  | CVE-2020-2830    |
|                  |              | OpenJDK: Regular expression DoS
|
2022-10-30T02:36:09.7559274Z |                  |                  |
|                  |              | in Scanner (Concurrency, 8236201)
|
2022-10-30T02:36:09.7559955Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2020-
2830     |
2022-10-30T02:36:09.7560681Z +                  +------------------+----
------+                 +---------------+------------------------------
------------+
2022-10-30T02:36:09.7561467Z |                  | CVE-2019-2766    | LOW
|                  | 8.222.10-r0   | OpenJDK: Insufficient permission
|
2022-10-30T02:36:09.7561971Z |                  |                  |
|                  |              | checks for file:// URLs on
|
2022-10-30T02:36:09.7562517Z |                  |                  |
|                  |              | Windows (Networking, 8213431)
|
2022-10-30T02:36:09.7563316Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2019-
2766     |
2022-10-30T02:36:09.7564041Z +                  +------------------+
+                  +              +-----------------------------------
------+
2022-10-30T02:36:09.7564765Z |                  | CVE-2019-2786    |
|                  |              | OpenJDK: Insufficient
|
2022-10-30T02:36:09.7565238Z |                  |                  |
|                  |              | restriction of privileges in
|
2022-10-30T02:36:09.7565708Z |                  |                  |
|                  |              | AccessController (Security,
8216381)     |
2022-10-30T02:36:09.7566412Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2019-
2786     |
```

```
2022-10-30T02:36:09.7567128Z +                  +------------------+
+                  +              +-----------------------------------
------+
2022-10-30T02:36:09.7567875Z |                  | CVE-2019-2842    |
|                  |              | OpenJDK: Missing array bounds check
|
2022-10-30T02:36:09.7568387Z |                  |                  |
|                  |              | in crypto providers (JCE, 8223511)
|
2022-10-30T02:36:09.7569068Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2019-
2842     |
2022-10-30T02:36:09.7569797Z +                  +------------------+
+                  +--------------+-----------------------------------
------+
2022-10-30T02:36:09.7570557Z |                  | CVE-2019-2894    |
|                  | 8.232.09-r0  | OpenJDK: Side-channel
|
2022-10-30T02:36:09.7571051Z |                  |                  |
|                  |              | vulnerability in the ECDSA
|
2022-10-30T02:36:09.7571490Z |                  |                  |
|                  |              | implementation (Security, 8228825)
|
2022-10-30T02:36:09.7572170Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2019-
2894     |
2022-10-30T02:36:09.7572884Z +                  +------------------+
+                  +              +-----------------------------------
------+
2022-10-30T02:36:09.7573624Z |                  | CVE-2019-2933    |
|                  |              | OpenJDK: FilePermission checks
|
2022-10-30T02:36:09.7574102Z |                  |                  |
|                  |              | not preformed correctly on
|
2022-10-30T02:36:09.7574670Z |                  |                  |
|                  |              | Windows (Libraries, 8213429)
|
2022-10-30T02:36:09.7575364Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2019-
2933     |
2022-10-30T02:36:09.7576084Z +                  +------------------+
+                  +              +-----------------------------------
------+
2022-10-30T02:36:09.7576817Z |                  | CVE-2019-2945    |
|                  |              | OpenJDK: Missing restrictions
|
2022-10-30T02:36:09.7577296Z |                  |                  |
|                  |              | on use of custom SocketImpl
|
2022-10-30T02:36:09.7577735Z |                  |                  |
|                  |              | (Networking, 8218573)
|
2022-10-30T02:36:09.7578500Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2019-
2945     |
```

```
2022-10-30T02:36:09.7579248Z +                  +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7579986Z |                  | CVE-2019-2962    |
|                   |               | OpenJDK: NULL pointer dereference
|
2022-10-30T02:36:09.7580474Z |                  |                  |
|                   |               | in DrawGlyphList (2D, 8222690)
|
2022-10-30T02:36:09.7581152Z |                  |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2019-
2962     |
2022-10-30T02:36:09.7581866Z +                  +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7582575Z |                  | CVE-2019-2964    |
|                   |               | OpenJDK: Unexpected exception
|
2022-10-30T02:36:09.7583067Z |                  |                  |
|                   |               | thrown by Pattern processing
|
2022-10-30T02:36:09.7583517Z |                  |                  |
|                   |               | crafted regular expression
|
2022-10-30T02:36:09.7583969Z |                  |                  |
|                   |               | (Concurrency, 8222684)...
|
2022-10-30T02:36:09.7584645Z |                  |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2019-
2964     |
2022-10-30T02:36:09.7585367Z +                  +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7586109Z |                  | CVE-2019-2973    |
|                   |               | OpenJDK: Unexpected exception
thrown     |
2022-10-30T02:36:09.7586610Z |                  |                  |
|                   |               | by XPathParser processing crafted
|
2022-10-30T02:36:09.7587085Z |                  |                  |
|                   |               | XPath expression (JAXP, 8223505)...
|
2022-10-30T02:36:09.7587775Z |                  |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2019-
2973     |
2022-10-30T02:36:09.7588488Z +                  +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7589210Z |                  | CVE-2019-2978    |
|                   |               | OpenJDK: Incorrect handling
|
2022-10-30T02:36:09.7589686Z |                  |                  |
|                   |               | of nested jar: URLs in Jar
|
2022-10-30T02:36:09.7590234Z |                  |                  |
|                   |               | URL handler (Networking,...
|
```

```
2022-10-30T02:36:09.7590920Z |                    |                  |
|                    |                | -->avd.aquasec.com/nvd/cve-2019-
2978     |
2022-10-30T02:36:09.7591635Z +                    +------------------+
+                    +                +-----------------------------------
------+
2022-10-30T02:36:09.7592363Z |                    | CVE-2019-2981    |
|                    |                | OpenJDK: Unexpected exception
|
2022-10-30T02:36:09.7592834Z |                    |                  |
|                    |                | thrown by XPath processing crafted
|
2022-10-30T02:36:09.7593302Z |                    |                  |
|                    |                | XPath expression (JAXP, 8224532)...
|
2022-10-30T02:36:09.7593986Z |                    |                  |
|                    |                | -->avd.aquasec.com/nvd/cve-2019-
2981     |
2022-10-30T02:36:09.7594782Z +                    +------------------+
+                    +                +-----------------------------------
------+
2022-10-30T02:36:09.7595518Z |                    | CVE-2019-2983    |
|                    |                | OpenJDK: Unexpected exception
thrown     |
2022-10-30T02:36:09.7596018Z |                    |                  |
|                    |                | during Font object deserialization
|
2022-10-30T02:36:09.7596469Z |                    |                  |
|                    |                | (Serialization, 8224915)
|
2022-10-30T02:36:09.7597137Z |                    |                  |
|                    |                | -->avd.aquasec.com/nvd/cve-2019-
2983     |
2022-10-30T02:36:09.7597850Z +                    +------------------+
+                    +                +-----------------------------------
------+
2022-10-30T02:36:09.7598583Z |                    | CVE-2019-2987    |
|                    |                | OpenJDK: Missing glyph bitmap
|
2022-10-30T02:36:09.7599051Z |                    |                  |
|                    |                | image dimension check in
|
2022-10-30T02:36:09.7599505Z |                    |                  |
|                    |                | FreetypeFontScaler (2D, 8225286)
|
2022-10-30T02:36:09.7600185Z |                    |                  |
|                    |                | -->avd.aquasec.com/nvd/cve-2019-
2987     |
2022-10-30T02:36:09.7600897Z +                    +------------------+
+                    +                +-----------------------------------
------+
2022-10-30T02:36:09.7601626Z |                    | CVE-2019-2988    |
|                    |                | OpenJDK: Integer overflow in bounds
|
2022-10-30T02:36:09.7602119Z |                    |                  |
|                    |                | check in SunGraphics2D (2D,
8225292)     |
```

```
2022-10-30T02:36:09.7602811Z |                   |                   |
|                   |               | -->avd.aquasec.com/nvd/cve-2019-
2988     |
2022-10-30T02:36:09.7603711Z +                   +-------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7604440Z |                   | CVE-2019-2992     |
|                   |               | OpenJDK: Excessive memory
|
2022-10-30T02:36:09.7604915Z |                   |                   |
|                   |               | allocation in CMap when reading
|
2022-10-30T02:36:09.7605371Z |                   |                   |
|                   |               | TrueType font (2D, 8225597)...
|
2022-10-30T02:36:09.7606046Z |                   |                   |
|                   |               | -->avd.aquasec.com/nvd/cve-2019-
2992     |
2022-10-30T02:36:09.7606892Z +                   +-------------------+
+                   +---------------+-----------------------------------
------+
2022-10-30T02:36:09.7607665Z |                   | CVE-2020-14577    |
|                   | 8.272.10-r0   | OpenJDK: HostnameChecker does
|
2022-10-30T02:36:09.7608162Z |                   |                   |
|                   |               | not ensure X.509 certificate
|
2022-10-30T02:36:09.7608617Z |                   |                   |
|                   |               | names are in normalized form...
|
2022-10-30T02:36:09.7609294Z |                   |                   |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
14577    |
2022-10-30T02:36:09.7610006Z +                   +-------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7610726Z |                   | CVE-2020-14578    |
|                   |               | OpenJDK: Unexpected exception
|
2022-10-30T02:36:09.7611280Z |                   |                   |
|                   |               | raised by DerInputStream
|
2022-10-30T02:36:09.7611714Z |                   |                   |
|                   |               | (Libraries, 8237731)
|
2022-10-30T02:36:09.7612382Z |                   |                   |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
14578    |
2022-10-30T02:36:09.7613097Z +                   +-------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7613828Z |                   | CVE-2020-14579    |
|                   |               | OpenJDK: Unexpected exception
|
2022-10-30T02:36:09.7614310Z |                   |                   |
|                   |               | raised by DerValue.equals()
|
```

```
2022-10-30T02:36:09.7614759Z |                    |                    |
|                    |               | (Libraries, 8237736)
|
2022-10-30T02:36:09.7615421Z |                    |                    |
|                    |               | -->avd.aquasec.com/nvd/cve-2020-
14579    |
2022-10-30T02:36:09.7616134Z +                    +--------------------+
+                    +               +-----------------------------------
------+
2022-10-30T02:36:09.7616860Z |                    | CVE-2020-14581     |
|                    |               | OpenJDK: Information disclosure
|
2022-10-30T02:36:09.7617345Z |                    |                    |
|                    |               | in color management (2D, 8238002)
|
2022-10-30T02:36:09.7618023Z |                    |                    |
|                    |               | -->avd.aquasec.com/nvd/cve-2020-
14581    |
2022-10-30T02:36:09.7618744Z +                    +--------------------+
+                    +               +-----------------------------------
------+
2022-10-30T02:36:09.7619451Z |                    | CVE-2020-14779     |
|                    |               | OpenJDK: High memory usage
|
2022-10-30T02:36:09.7619931Z |                    |                    |
|                    |               | during deserialization of Proxy
|
2022-10-30T02:36:09.7620384Z |                    |                    |
|                    |               | class with many interfaces...
|
2022-10-30T02:36:09.7621063Z |                    |                    |
|                    |               | -->avd.aquasec.com/nvd/cve-2020-
14779    |
2022-10-30T02:36:09.7621788Z +                    +--------------------+
+                    +               +-----------------------------------
------+
2022-10-30T02:36:09.7622516Z |                    | CVE-2020-14781     |
|                    |               | OpenJDK: Credentials sent
|
2022-10-30T02:36:09.7623059Z |                    |                    |
|                    |               | over unencrypted LDAP
|
2022-10-30T02:36:09.7623497Z |                    |                    |
|                    |               | connection (JNDI, 8237990)
|
2022-10-30T02:36:09.7624177Z |                    |                    |
|                    |               | -->avd.aquasec.com/nvd/cve-2020-
14781    |
2022-10-30T02:36:09.7624893Z +                    +--------------------+
+                    +               +-----------------------------------
------+
2022-10-30T02:36:09.7625628Z |                    | CVE-2020-14782     |
|                    |               | OpenJDK: Certificate blacklist
|
2022-10-30T02:36:09.7626112Z |                    |                    |
|                    |               | bypass via alternate certificate
|
```

```
2022-10-30T02:36:09.7626669Z |                   |                   |
|                   |               | encodings (Libraries, 8237995)
|
2022-10-30T02:36:09.7627359Z |                   |                   |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
14782    |
2022-10-30T02:36:09.7628074Z +                   +-------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7628803Z |                   | CVE-2020-14796    |
|                   |               | OpenJDK: Missing permission
|
2022-10-30T02:36:09.7629270Z |                   |                   |
|                   |               | check in path to URI
|
2022-10-30T02:36:09.7629699Z |                   |                   |
|                   |               | conversion (Libraries, 8242680)
|
2022-10-30T02:36:09.7630383Z |                   |                   |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
14796    |
2022-10-30T02:36:09.7631108Z +                   +-------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7631837Z |                   | CVE-2020-14797    |
|                   |               | OpenJDK: Incomplete check for
|
2022-10-30T02:36:09.7632317Z |                   |                   |
|                   |               | invalid characters in URI to
|
2022-10-30T02:36:09.7632770Z |                   |                   |
|                   |               | path conversion (Libraries,...
|
2022-10-30T02:36:09.7637044Z |                   |                   |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
14797    |
2022-10-30T02:36:09.7637860Z +                   +-------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7638625Z |                   | CVE-2020-14798    |
|                   |               | OpenJDK: Missing maximum length
check in |
2022-10-30T02:36:09.7639139Z |                   |                   |
|                   |               |
WindowsNativeDispatcher.asNativeBuffer() |
2022-10-30T02:36:09.7639601Z |                   |                   |
|                   |               | (Libraries, 8242695)
|
2022-10-30T02:36:09.7640272Z |                   |                   |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
14798    |
2022-10-30T02:36:09.7641007Z +                   +-------------------+
+                   +---------------+-----------------------------------
------+
2022-10-30T02:36:09.7641772Z |                   | CVE-2020-2583     |
|                   | 8.242.08-r0   | OpenJDK: Incorrect exception
|
```

```
2022-10-30T02:36:09.7642426Z |                  |                  |
|                   |              | processing during deserialization
|
2022-10-30T02:36:09.7642875Z |                  |                  |
|                   |              | in BeanContextSupport
|
2022-10-30T02:36:09.7643489Z |                  |                  |
|                   |              | (Serialization, 8224909)
|
2022-10-30T02:36:09.7644173Z |                  |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2020-
2583     |
2022-10-30T02:36:09.7644894Z +                  +------------------+
+                   +              +-----------------------------------
------+
2022-10-30T02:36:09.7645623Z |                  | CVE-2020-2590    |
|                   |              | OpenJDK: Improper checks of
|
2022-10-30T02:36:09.7646098Z |                  |                  |
|                   |              | SASL message properties in
|
2022-10-30T02:36:09.7646661Z |                  |                  |
|                   |              | GssKrb5Base (Security, 8226352)
|
2022-10-30T02:36:09.7647356Z |                  |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2020-
2590     |
2022-10-30T02:36:09.7648074Z +                  +------------------+
+                   +              +-----------------------------------
------+
2022-10-30T02:36:09.7648806Z |                  | CVE-2020-2654    |
|                   |              | OpenJDK: Excessive memory usage
|
2022-10-30T02:36:09.7649287Z |                  |                  |
|                   |              | in OID processing in X.509
|
2022-10-30T02:36:09.7649749Z |                  |                  |
|                   |              | certificate parsing (Libraries,...
|
2022-10-30T02:36:09.7650441Z |                  |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2020-
2654     |
2022-10-30T02:36:09.7651157Z +                  +------------------+
+                   +              +-----------------------------------
------+
2022-10-30T02:36:09.7651890Z |                  | CVE-2020-2659    |
|                   |              | OpenJDK: Incomplete enforcement
|
2022-10-30T02:36:09.7652372Z |                  |                  |
|                   |              | of maxDatagramSockets limit
|
2022-10-30T02:36:09.7652813Z |                  |                  |
|                   |              | in DatagramChannelImpl
|
2022-10-30T02:36:09.7653247Z |                  |                  |
|                   |              | (Networking, 8231795)
|
```

```
2022-10-30T02:36:09.7653918Z |                    |                  |
|                    |               | -->avd.aquasec.com/nvd/cve-2020-
2659     |
2022-10-30T02:36:09.7654637Z +                    +------------------+
+                    +---------------+-----------------------------------
------+
2022-10-30T02:36:09.7655402Z |                    | CVE-2020-2754    |
|                    | 8.252.09-r0   | OpenJDK: Misplaced regular
|
2022-10-30T02:36:09.7655896Z |                    |                  |
|                    |               | expression syntax error check in
|
2022-10-30T02:36:09.7656360Z |                    |                  |
|                    |               | RegExpScanner (Scripting, 8223898)
|
2022-10-30T02:36:09.7657052Z |                    |                  |
|                    |               | -->avd.aquasec.com/nvd/cve-2020-
2754     |
2022-10-30T02:36:09.7657768Z +                    +------------------+
+                    +               +-----------------------------------
------+
2022-10-30T02:36:09.7658601Z |                    | CVE-2020-2755    |
|                    |               | OpenJDK: Incorrect handling of
|
2022-10-30T02:36:09.7659080Z |                    |                  |
|                    |               | empty string nodes in regular
|
2022-10-30T02:36:09.7659534Z |                    |                  |
|                    |               | expression Parser (Scripting,...
|
2022-10-30T02:36:09.7660219Z |                    |                  |
|                    |               | -->avd.aquasec.com/nvd/cve-2020-
2755     |
2022-10-30T02:36:09.7660933Z +                    +------------------+
+                    +               +-----------------------------------
------+
2022-10-30T02:36:09.7661661Z |                    | CVE-2020-2756    |
|                    |               | OpenJDK: Incorrect handling
|
2022-10-30T02:36:09.7662227Z |                    |                  |
|                    |               | of references to uninitialized
|
2022-10-30T02:36:09.7662670Z |                    |                  |
|                    |               | class descriptors during
|
2022-10-30T02:36:09.7663122Z |                    |                  |
|                    |               | deserialization (Serialization,...
|
2022-10-30T02:36:09.7663887Z |                    |                  |
|                    |               | -->avd.aquasec.com/nvd/cve-2020-
2756     |
2022-10-30T02:36:09.7664609Z +                    +------------------+
+                    +               +-----------------------------------
------+
2022-10-30T02:36:09.7665337Z |                    | CVE-2020-2757    |
|                    |               | OpenJDK: Uncaught
InstantiationError     |
```

```
2022-10-30T02:36:09.7665831Z |                  |                  |
|                   |              | exception in ObjectStreamClass
|
2022-10-30T02:36:09.7666286Z |                  |                  |
|                   |              | (Serialization, 8224549)
|
2022-10-30T02:36:09.7666957Z |                  |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2020-
2757     |
2022-10-30T02:36:09.7667675Z +                  +------------------+
+                   +              +-----------------------------------
------+
2022-10-30T02:36:09.7668414Z |                  | CVE-2020-2773    |
|                   |              | OpenJDK: Unexpected exceptions
|
2022-10-30T02:36:09.7668893Z |                  |                  |
|                   |              | raised by DOMKeyInfoFactory
|
2022-10-30T02:36:09.7669339Z |                  |                  |
|                   |              | and DOMXMLSignatureFactory
|
2022-10-30T02:36:09.7669784Z |                  |                  |
|                   |              | (Security, 8231415)
|
2022-10-30T02:36:09.7670450Z |                  |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2020-
2773     |
2022-10-30T02:36:09.7671217Z +------------------+------------------+----
------+                  +---------------+------------------------------
------------+
2022-10-30T02:36:09.7672072Z | openjdk8-jre-base | CVE-2020-14583   |
HIGH     |                  | 8.272.10-r0   | OpenJDK: Bypass of
boundary checks       |
2022-10-30T02:36:09.7672612Z |                  |                  |
|                   |              | in nio.Buffer via concurrent
|
2022-10-30T02:36:09.7673066Z |                  |                  |
|                   |              | access (Libraries, 8238920)...
|
2022-10-30T02:36:09.7673833Z |                  |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2020-
14583    |
2022-10-30T02:36:09.7674560Z +                  +------------------+
+                   +              +-----------------------------------
------+
2022-10-30T02:36:09.7675306Z |                  | CVE-2020-14593   |
|                   |              | OpenJDK: Incomplete bounds checks
in     |
2022-10-30T02:36:09.7675792Z |                  |                  |
|                   |              | Affine Transformations (2D,
8240119)     |
2022-10-30T02:36:09.7676478Z |                  |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2020-
14593    |
2022-10-30T02:36:09.7677210Z +                  +------------------+
+                   +---------------+-----------------------------------
------+
```

```
2022-10-30T02:36:09.7677981Z |                    | CVE-2020-2604    |
|                    | 8.242.08-r0   | OpenJDK: Serialization filter
|
2022-10-30T02:36:09.7678555Z |                    |                  |
|                    |               | changes via jdk.serialFilter
|
2022-10-30T02:36:09.7679036Z |                    |                  |
|                    |               | property modification
|
2022-10-30T02:36:09.7679474Z |                    |                  |
|                    |               | (Serialization, 8231422)
|
2022-10-30T02:36:09.7680168Z |                    |                  |
|                    |               | -->avd.aquasec.com/nvd/cve-2020-
2604     |
2022-10-30T02:36:09.7680900Z +                    +------------------+
+                    +---------------+-----------------------------------
------+
2022-10-30T02:36:09.7681669Z |                    | CVE-2020-2803    |
|                    | 8.252.09-r0   | OpenJDK: Incorrect bounds checks
|
2022-10-30T02:36:09.7682184Z |                    |                  |
|                    |               | in NIO Buffers (Libraries, 8234841)
|
2022-10-30T02:36:09.7682870Z |                    |                  |
|                    |               | -->avd.aquasec.com/nvd/cve-2020-
2803     |
2022-10-30T02:36:09.7683700Z +                    +------------------+
+                    +               +-----------------------------------
------+
2022-10-30T02:36:09.7684437Z |                    | CVE-2020-2805    |
|                    |               | OpenJDK: Incorrect type checks
|
2022-10-30T02:36:09.7684913Z |                    |                  |
|                    |               | in MethodType.readObject()
|
2022-10-30T02:36:09.7685350Z |                    |                  |
|                    |               | (Libraries, 8235274)
|
2022-10-30T02:36:09.7686019Z |                    |                  |
|                    |               | -->avd.aquasec.com/nvd/cve-2020-
2805     |
2022-10-30T02:36:09.7686756Z +                    +------------------+----
------+                   +---------------+-------------------------------
------------+
2022-10-30T02:36:09.7687542Z |                    | CVE-2019-2745    |
MEDIUM   |                   | 8.222.10-r0   | OpenJDK: Side-channel
attack             |
2022-10-30T02:36:09.7688046Z |                    |                  |
|                    |               | risks in Elliptic Curve (EC)
|
2022-10-30T02:36:09.7688502Z |                    |                  |
|                    |               | cryptography (Security, 8208698)
|
2022-10-30T02:36:09.7689189Z |                    |                  |
|                    |               | -->avd.aquasec.com/nvd/cve-2019-
2745     |
```

```
2022-10-30T02:36:09.7689907Z +                  +------------------+
+                  +              +-----------------------------------
------+
2022-10-30T02:36:09.7690739Z |                  | CVE-2019-2762    |
|                  |              | OpenJDK: Insufficient checks
|
2022-10-30T02:36:09.7691216Z |                  |                  |
|                  |              | of suppressed exceptions in
|
2022-10-30T02:36:09.7691677Z |                  |                  |
|                  |              | deserialization (Utilities,
8212328)     |
2022-10-30T02:36:09.7692364Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2019-
2762     |
2022-10-30T02:36:09.7693087Z +                  +------------------+
+                  +              +-----------------------------------
------+
2022-10-30T02:36:09.7693819Z |                  | CVE-2019-2769    |
|                  |              | OpenJDK: Unbounded memory
|
2022-10-30T02:36:09.7694304Z |                  |                  |
|                  |              | allocation during deserialization
|
2022-10-30T02:36:09.7694847Z |                  |                  |
|                  |              | in Collections (Utilities, 8213432)
|
2022-10-30T02:36:09.7695553Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2019-
2769     |
2022-10-30T02:36:09.7696267Z +                  +------------------+
+                  +              +-----------------------------------
------+
2022-10-30T02:36:09.7696993Z |                  | CVE-2019-2816    |
|                  |              | OpenJDK: Missing URL format
|
2022-10-30T02:36:09.7697459Z |                  |                  |
|                  |              | validation (Networking, 8221518)
|
2022-10-30T02:36:09.7698141Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2019-
2816     |
2022-10-30T02:36:09.7698879Z +                  +------------------+
+                  +--------------+-----------------------------------
------+
2022-10-30T02:36:09.7699642Z |                  | CVE-2019-2949    |
|                  | 8.232.09-r0  | OpenJDK: Improper handling
|
2022-10-30T02:36:09.7700138Z |                  |                  |
|                  |              | of Kerberos proxy credentials
|
2022-10-30T02:36:09.7700581Z |                  |                  |
|                  |              | (Kerberos, 8220302)
|
2022-10-30T02:36:09.7701248Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2019-
2949     |
```

```
2022-10-30T02:36:09.7701963Z +                  +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7702688Z |                  | CVE-2019-2958    |
|                   |               | OpenJDK: Incorrect
|
2022-10-30T02:36:09.7703159Z |                  |                  |
|                   |               | escaping of command line
|
2022-10-30T02:36:09.7703599Z |                  |                  |
|                   |               | arguments in ProcessImpl
|
2022-10-30T02:36:09.7704040Z |                  |                  |
|                   |               | on Windows (Libraries,...
|
2022-10-30T02:36:09.7704706Z |                  |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2019-
2958     |
2022-10-30T02:36:09.7705418Z +                  +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7706166Z |                  | CVE-2019-2975    |
|                   |               | OpenJDK: Unexpected exception
thrown     |
2022-10-30T02:36:09.7706740Z |                  |                  |
|                   |               | during regular expression
processing     |
2022-10-30T02:36:09.7707213Z |                  |                  |
|                   |               | in Nashorn (Scripting, 8223518)...
|
2022-10-30T02:36:09.7707890Z |                  |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2019-
2975     |
2022-10-30T02:36:09.7708605Z +                  +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7709353Z |                  | CVE-2019-2989    |
|                   |               | OpenJDK: Incorrect handling of HTTP
|
2022-10-30T02:36:09.7709856Z |                  |                  |
|                   |               | proxy responses in
HttpURLConnection     |
2022-10-30T02:36:09.7710415Z |                  |                  |
|                   |               | (Networking, 8225298)
|
2022-10-30T02:36:09.7711091Z |                  |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2019-
2989     |
2022-10-30T02:36:09.7711806Z +                  +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7712541Z |                  | CVE-2019-2999    |
|                   |               | OpenJDK: Insufficient filtering
|
2022-10-30T02:36:09.7713019Z |                  |                  |
|                   |               | of HTML event attributes in
|
```

```
2022-10-30T02:36:09.7713466Z |                   |                  |
|                   |               | Javadoc (Javadoc, 8226765)
|
2022-10-30T02:36:09.7714142Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2019-
2999     |
2022-10-30T02:36:09.7714878Z +                   +------------------+
+                   +---------------+-----------------------------------
------+
2022-10-30T02:36:09.7715638Z |                   | CVE-2019-7317    |
|                   | 8.222.10-r0   | libpng: use-after-free in
|
2022-10-30T02:36:09.7716118Z |                   |                  |
|                   |               | png_image_free in png.c
|
2022-10-30T02:36:09.7716786Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2019-
7317     |
2022-10-30T02:36:09.7717518Z +                   +------------------+
+                   +---------------+-----------------------------------
------+
2022-10-30T02:36:09.7718287Z |                   | CVE-2020-14556   |
|                   | 8.272.10-r0   | OpenJDK: Incorrect handling
|
2022-10-30T02:36:09.7718774Z |                   |                  |
|                   |               | of access control context in
|
2022-10-30T02:36:09.7719231Z |                   |                  |
|                   |               | ForkJoinPool (Libraries, 8237117)
|
2022-10-30T02:36:09.7719918Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
14556    |
2022-10-30T02:36:09.7720633Z +                   +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7721373Z |                   | CVE-2020-14621   |
|                   |               | OpenJDK: XML validation
manipulation     |
2022-10-30T02:36:09.7721868Z |                   |                  |
|                   |               | due to incomplete application of
|
2022-10-30T02:36:09.7722665Z |                   |                  |
|                   |               | the use-grammar-pool-only
feature...     |
2023-10-30T02:36:09.7723569Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
14621    |
2022-10-30T02:36:09.7724300Z +                   +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7725029Z |                   | CVE-2020-14792   |
|                   |               | OpenJDK: Integer overflow
|
2022-10-30T02:36:09.7725705Z |                   |                  |
|                   |               | leading to out-of-bounds
|
```

```
2022-10-30T02:36:09.7726153Z |                   |                  |
|                   |               | access (Hotspot, 8241114)
|
2022-10-30T02:36:09.7726828Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
14792    |
2022-10-30T02:36:09.7727664Z +                   +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7728401Z |                   | CVE-2020-14803   |
|                   |               | OpenJDK: Race condition in NIO
Buffer    |
2022-10-30T02:36:09.7728904Z |                   |                  |
|                   |               | boundary checks (Libraries,
8244136)     |
2022-10-30T02:36:09.7729592Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
14803    |
2022-10-30T02:36:09.7730308Z +                   +------------------+
+                   +---------------+-----------------------------------
------+
2022-10-30T02:36:09.7731060Z |                   | CVE-2020-2593    |
|                   | 8.242.08-r0   | OpenJDK: Incorrect
|
2022-10-30T02:36:09.7731551Z |                   |                  |
|                   |               | isBuiltinStreamHandler check
|
2022-10-30T02:36:09.7732002Z |                   |                  |
|                   |               | causing URL normalization
|
2022-10-30T02:36:09.7732449Z |                   |                  |
|                   |               | issues (Networking, 8228548)
|
2022-10-30T02:36:09.7733134Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
2593     |
2022-10-30T02:36:09.7733851Z +                   +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7734576Z |                   | CVE-2020-2601    |
|                   |               | OpenJDK: Use of unsafe
|
2022-10-30T02:36:09.7735256Z |                   |                  |
|                   |               | RSA-MD5 checksum in Kerberos
|
2022-10-30T02:36:09.7735712Z |                   |                  |
|                   |               | TGS (Security, 8229951)
|
2022-10-30T02:36:09.7736383Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
2601     |
2022-10-30T02:36:09.7737111Z +                   +------------------+
+                   +---------------+-----------------------------------
------+
2022-10-30T02:36:09.7737873Z |                   | CVE-2020-2781    |
|                   | 8.252.09-r0   | OpenJDK: Re-use of single
|
```

```
2022-10-30T02:36:09.7738348Z |                   |                  |
|                   |               | TLS session for new
|
2022-10-30T02:36:09.7738790Z |                   |                  |
|                   |               | connections (JSSE, 8234408)
|
2022-10-30T02:36:09.7739565Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
2781     |
2022-10-30T02:36:09.7740280Z +                   +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7740998Z |                   | CVE-2020-2800    |
|                   |               | OpenJDK: CRLF injection into HTTP
|
2022-10-30T02:36:09.7741485Z |                   |                  |
|                   |               | headers in HttpServer (Lightweight
|
2022-10-30T02:36:09.7741935Z |                   |                  |
|                   |               | HTTP Server, 8234825)...
|
2022-10-30T02:36:09.7742605Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
2800     |
2022-10-30T02:36:09.7743398Z +                   +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7744131Z |                   | CVE-2020-2830    |
|                   |               | OpenJDK: Regular expression DoS
|
2022-10-30T02:36:09.7744621Z |                   |                  |
|                   |               | in Scanner (Concurrency, 8236201)
|
2022-10-30T02:36:09.7745310Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
2830     |
2022-10-30T02:36:09.7746048Z +                   +------------------+----
------+                   +---------------+------------------------------
------------+
2022-10-30T02:36:09.7746838Z |                   | CVE-2019-2766    | LOW
|                   | 8.222.10-r0   | OpenJDK: Insufficient permission
|
2022-10-30T02:36:09.7747334Z |                   |                  |
|                   |               | checks for file:// URLs on
|
2022-10-30T02:36:09.7747787Z |                   |                  |
|                   |               | Windows (Networking, 8213431)
|
2022-10-30T02:36:09.7748464Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2019-
2766     |
2022-10-30T02:36:09.7749176Z +                   +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7749893Z |                   | CVE-2019-2786    |
|                   |               | OpenJDK: Insufficient
|
```

```
2022-10-30T02:36:09.7750358Z |                  |                  |
|                   |              | restriction of privileges in
|
2022-10-30T02:36:09.7750819Z |                  |                  |
|                   |              | AccessController (Security,
8216381)     |
2022-10-30T02:36:09.7751501Z |                  |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2019-
2786     |
2022-10-30T02:36:09.7752213Z +                  +------------------+
+                   +              +-----------------------------------
------+
2022-10-30T02:36:09.7752947Z |                  | CVE-2019-2842    |
|                   |              | OpenJDK: Missing array bounds check
|
2022-10-30T02:36:09.7753435Z |                  |                  |
|                   |              | in crypto providers (JCE, 8223511)
|
2022-10-30T02:36:09.7754116Z |                  |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2019-
2842     |
2022-10-30T02:36:09.7754852Z +                  +------------------+
+                   +--------------+-----------------------------------
------+
2022-10-30T02:36:09.7755715Z |                  | CVE-2019-2894    |
|                   | 8.232.09-r0  | OpenJDK: Side-channel
|
2022-10-30T02:36:09.7756197Z |                  |                  |
|                   |              | vulnerability in the ECDSA
|
2022-10-30T02:36:09.7756648Z |                  |                  |
|                   |              | implementation (Security, 8228825)
|
2022-10-30T02:36:09.7757332Z |                  |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2019-
2894     |
2022-10-30T02:36:09.7758049Z +                  +------------------+
+                   +              +-----------------------------------
------+
2022-10-30T02:36:09.7758791Z |                  | CVE-2019-2933    |
|                   |              | OpenJDK: FilePermission checks
|
2022-10-30T02:36:09.7759266Z |                  |                  |
|                   |              | not preformed correctly on
|
2022-10-30T02:36:09.7759800Z |                  |                  |
|                   |              | Windows (Libraries, 8213429)
|
2022-10-30T02:36:09.7760487Z |                  |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2019-
2933     |
2022-10-30T02:36:09.7761206Z +                  +------------------+
+                   +              +-----------------------------------
------+
2022-10-30T02:36:09.7761935Z |                  | CVE-2019-2945    |
|                   |              | OpenJDK: Missing restrictions
|
```

```
2022-10-30T02:36:09.7762395Z |                  |                  |
|                   |              | on use of custom SocketImpl
|
2022-10-30T02:36:09.7762831Z |                  |                  |
|                   |              | (Networking, 8218573)
|
2022-10-30T02:36:09.7764151Z |                  |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2019-
2945     |
2022-10-30T02:36:09.7764879Z +                  +------------------+
+                   +              +-----------------------------------
------+
2022-10-30T02:36:09.7765619Z |                  | CVE-2019-2962    |
|                   |              | OpenJDK: NULL pointer dereference
|
2022-10-30T02:36:09.7766108Z |                  |                  |
|                   |              | in DrawGlyphList (2D, 8222690)
|
2022-10-30T02:36:09.7766789Z |                  |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2019-
2962     |
2022-10-30T02:36:09.7767503Z +                  +------------------+
+                   +              +-----------------------------------
------+
2022-10-30T02:36:09.7768234Z |                  | CVE-2019-2964    |
|                   |              | OpenJDK: Unexpected exception
|
2022-10-30T02:36:09.7768725Z |                  |                  |
|                   |              | thrown by Pattern processing
|
2022-10-30T02:36:09.7769173Z |                  |                  |
|                   |              | crafted regular expression
|
2022-10-30T02:36:09.7769621Z |                  |                  |
|                   |              | (Concurrency, 8222684)...
|
2022-10-30T02:36:09.7770292Z |                  |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2019-
2964     |
2022-10-30T02:36:09.7771007Z +                  +------------------+
+                   +              +-----------------------------------
------+
2022-10-30T02:36:09.7771746Z |                  | CVE-2019-2973    |
|                   |              | OpenJDK: Unexpected exception
thrown     |
2022-10-30T02:36:09.7772387Z |                  |                  |
|                   |              | by XPathParser processing crafted
|
2022-10-30T02:36:09.7772856Z |                  |                  |
|                   |              | XPath expression (JAXP, 8223505)...
|
2022-10-30T02:36:09.7773549Z |                  |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2019-
2973     |
2022-10-30T02:36:09.7774247Z +                  +------------------+
+                   +              +-----------------------------------
------+
```

```
2022-10-30T02:36:09.7774978Z |                    | CVE-2019-2978    |
|                    |               | OpenJDK: Incorrect handling
|
2022-10-30T02:36:09.7775449Z |                    |                  |
|                    |               | of nested jar: URLs in Jar
|
2022-10-30T02:36:09.7775898Z |                    |                  |
|                    |               | URL handler (Networking,...
|
2022-10-30T02:36:09.7776665Z |                    |                  |
|                    |               | -->avd.aquasec.com/nvd/cve-2019-
2978     |
2022-10-30T02:36:09.7777380Z +                    +------------------+
+                    +               +-----------------------------------
------+
2022-10-30T02:36:09.7778118Z |                    | CVE-2019-2981    |
|                    |               | OpenJDK: Unexpected exception
|
2022-10-30T02:36:09.7778606Z |                    |                  |
|                    |               | thrown by XPath processing crafted
|
2022-10-30T02:36:09.7779107Z |                    |                  |
|                    |               | XPath expression (JAXP, 8224532)...
|
2022-10-30T02:36:09.7779795Z |                    |                  |
|                    |               | -->avd.aquasec.com/nvd/cve-2019-
2981     |
2022-10-30T02:36:09.7780521Z +                    +------------------+
+                    +               +-----------------------------------
------+
2022-10-30T02:36:09.7781260Z |                    | CVE-2019-2983    |
|                    |               | OpenJDK: Unexpected exception
thrown     |
2022-10-30T02:36:09.7781755Z |                    |                  |
|                    |               | during Font object deserialization
|
2022-10-30T02:36:09.7782206Z |                    |                  |
|                    |               | (Serialization, 8224915)
|
2022-10-30T02:36:09.7782878Z |                    |                  |
|                    |               | -->avd.aquasec.com/nvd/cve-2019-
2983     |
2022-10-30T02:36:09.7783592Z +                    +------------------+
+                    +               +-----------------------------------
------+
2022-10-30T02:36:09.7784324Z |                    | CVE-2019-2987    |
|                    |               | OpenJDK: Missing glyph bitmap
|
2022-10-30T02:36:09.7784781Z |                    |                  |
|                    |               | image dimension check in
|
2022-10-30T02:36:09.7785228Z |                    |                  |
|                    |               | FreetypeFontScaler (2D, 8225286)
|
2022-10-30T02:36:09.7785909Z |                    |                  |
|                    |               | -->avd.aquasec.com/nvd/cve-2019-
2987     |
```

```
2022-10-30T02:36:09.7786627Z +                  +------------------+
+                  +              +-----------------------------------
------+
2022-10-30T02:36:09.7787368Z |                  | CVE-2019-2988    |
|                  |              | OpenJDK: Integer overflow in bounds
|
2022-10-30T02:36:09.7787861Z |                  |                  |
|                  |              | check in SunGraphics2D (2D,
8225292)     |
2022-10-30T02:36:09.7788646Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2019-
2988     |
2022-10-30T02:36:09.7789362Z +                  +------------------+
+                  +              +-----------------------------------
------+
2022-10-30T02:36:09.7790087Z |                  | CVE-2019-2992    |
|                  |              | OpenJDK: Excessive memory
|
2022-10-30T02:36:09.7790566Z |                  |                  |
|                  |              | allocation in CMap when reading
|
2022-10-30T02:36:09.7791020Z |                  |                  |
|                  |              | TrueType font (2D, 8225597)...
|
2022-10-30T02:36:09.7791698Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2019-
2992     |
2022-10-30T02:36:09.7792511Z +                  +------------------+
+                  +--------------+-----------------------------------
------+
2022-10-30T02:36:09.7793279Z |                  | CVE-2020-14577   |
|                  | 8.272.10-r0  | OpenJDK: HostnameChecker does
|
2022-10-30T02:36:09.7793776Z |                  |                  |
|                  |              | not ensure X.509 certificate
|
2022-10-30T02:36:09.7794226Z |                  |                  |
|                  |              | names are in normalized form...
|
2022-10-30T02:36:09.7794904Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2020-
14577    |
2022-10-30T02:36:09.7795602Z +                  +------------------+
+                  +              +-----------------------------------
------+
2022-10-30T02:36:09.7796336Z |                  | CVE-2020-14578   |
|                  |              | OpenJDK: Unexpected exception
|
2022-10-30T02:36:09.7796815Z |                  |                  |
|                  |              | raised by DerInputStream
|
2022-10-30T02:36:09.7797251Z |                  |                  |
|                  |              | (Libraries, 8237731)
|
2022-10-30T02:36:09.7797921Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2020-
14578    |
```

```
2022-10-30T02:36:09.7798639Z +                  +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7799373Z |                  | CVE-2020-14579   |
|                   |               | OpenJDK: Unexpected exception
|
2022-10-30T02:36:09.7799855Z |                  |                  |
|                   |               | raised by DerValue.equals()
|
2022-10-30T02:36:09.7800304Z |                  |                  |
|                   |               | (Libraries, 8237736)
|
2022-10-30T02:36:09.7800971Z |                  |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
14579    |
2022-10-30T02:36:09.7801690Z +                  +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7802422Z |                  | CVE-2020-14581   |
|                   |               | OpenJDK: Information disclosure
|
2022-10-30T02:36:09.7802907Z |                  |                  |
|                   |               | in color management (2D, 8238002)
|
2022-10-30T02:36:09.7803775Z |                  |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
14581    |
2022-10-30T02:36:09.7804606Z +                  +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7805337Z |                  | CVE-2020-14779   |
|                   |               | OpenJDK: High memory usage
|
2022-10-30T02:36:09.7805818Z |                  |                  |
|                   |               | during deserialization of Proxy
|
2022-10-30T02:36:09.7806254Z |                  |                  |
|                   |               | class with many interfaces...
|
2022-10-30T02:36:09.7806928Z |                  |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
14779    |
2022-10-30T02:36:09.7807649Z +                  +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7808384Z |                  | CVE-2020-14781   |
|                   |               | OpenJDK: Credentials sent
|
2022-10-30T02:36:09.7808942Z |                  |                  |
|                   |               | over unencrypted LDAP
|
2022-10-30T02:36:09.7809380Z |                  |                  |
|                   |               | connection (JNDI, 8237990)
|
2022-10-30T02:36:09.7810061Z |                  |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
14781    |
```

```
2022-10-30T02:36:09.7810776Z +                  +------------------+
+                  +              +-----------------------------------
------+
2022-10-30T02:36:09.7811507Z |                  | CVE-2020-14782   |
|                  |              | OpenJDK: Certificate blacklist
|
2022-10-30T02:36:09.7811996Z |                  |                  |
|                  |              | bypass via alternate certificate
|
2022-10-30T02:36:09.7812461Z |                  |                  |
|                  |              | encodings (Libraries, 8237995)
|
2022-10-30T02:36:09.7813138Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2020-
14782    |
2022-10-30T02:36:09.7813848Z +                  +------------------+
+                  +              +-----------------------------------
------+
2022-10-30T02:36:09.7814578Z |                  | CVE-2020-14796   |
|                  |              | OpenJDK: Missing permission
|
2022-10-30T02:36:09.7815044Z |                  |                  |
|                  |              | check in path to URI
|
2022-10-30T02:36:09.7815485Z |                  |                  |
|                  |              | conversion (Libraries, 8242680)
|
2022-10-30T02:36:09.7816168Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2020-
14796    |
2022-10-30T02:36:09.7816870Z +                  +------------------+
+                  +              +-----------------------------------
------+
2022-10-30T02:36:09.7817602Z |                  | CVE-2020-14797   |
|                  |              | OpenJDK: Incomplete check for
|
2022-10-30T02:36:09.7818087Z |                  |                  |
|                  |              | invalid characters in URI to
|
2022-10-30T02:36:09.7818538Z |                  |                  |
|                  |              | path conversion (Libraries,...
|
2022-10-30T02:36:09.7819220Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2020-
14797    |
2022-10-30T02:36:09.7819937Z +                  +------------------+
+                  +              +-----------------------------------
------+
2022-10-30T02:36:09.7820780Z |                  | CVE-2020-14798   |
|                  |              | OpenJDK: Missing maximum length
check in |
2022-10-30T02:36:09.7821288Z |                  |                  |
|                  |              |
WindowsNativeDispatcher.asNativeBuffer() |
2022-10-30T02:36:09.7821754Z |                  |                  |
|                  |              | (Libraries, 8242695)
|
```

```
2022-10-30T02:36:09.7822416Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
14798    |
2022-10-30T02:36:09.7823146Z +                   +------------------+
+                   +---------------+-----------------------------------
------+
2022-10-30T02:36:09.7823912Z |                   | CVE-2020-2583    |
|                   | 8.242.08-r0   | OpenJDK: Incorrect exception
|
2022-10-30T02:36:09.7824491Z |                   |                  |
|                   |               | processing during deserialization
|
2022-10-30T02:36:09.7824939Z |                   |                  |
|                   |               | in BeanContextSupport
|
2022-10-30T02:36:09.7825371Z |                   |                  |
|                   |               | (Serialization, 8224909)
|
2022-10-30T02:36:09.7826044Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
2583     |
2022-10-30T02:36:09.7826765Z +                   +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7827473Z |                   | CVE-2020-2590    |
|                   |               | OpenJDK: Improper checks of
|
2022-10-30T02:36:09.7827955Z |                   |                  |
|                   |               | SASL message properties in
|
2022-10-30T02:36:09.7828418Z |                   |                  |
|                   |               | GssKrb5Base (Security, 8226352)
|
2022-10-30T02:36:09.7829101Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
2590     |
2022-10-30T02:36:09.7829823Z +                   +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7830556Z |                   | CVE-2020-2654    |
|                   |               | OpenJDK: Excessive memory usage
|
2022-10-30T02:36:09.7831037Z |                   |                  |
|                   |               | in OID processing in X.509
|
2022-10-30T02:36:09.7831495Z |                   |                  |
|                   |               | certificate parsing (Libraries,...
|
2022-10-30T02:36:09.7832186Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
2654     |
2022-10-30T02:36:09.7832896Z +                   +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7833626Z |                   | CVE-2020-2659    |
|                   |               | OpenJDK: Incomplete enforcement
|
```

```
2022-10-30T02:36:09.7834104Z |                   |                   |
|                   |               | of maxDatagramSockets limit
|
2022-10-30T02:36:09.7834544Z |                   |                   |
|                   |               | in DatagramChannelImpl
|
2022-10-30T02:36:09.7834979Z |                   |                   |
|                   |               | (Networking, 8231795)
|
2022-10-30T02:36:09.7835756Z |                   |                   |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
2659     |
2022-10-30T02:36:09.7836492Z +                   +------------------+
+                   +---------------+-----------------------------------
------+
2022-10-30T02:36:09.7837263Z |                   | CVE-2020-2754    |
|                   | 8.252.09-r0   | OpenJDK: Misplaced regular
|
2022-10-30T02:36:09.7837744Z |                   |                   |
|                   |               | expression syntax error check in
|
2022-10-30T02:36:09.7838209Z |                   |                   |
|                   |               | RegExpScanner (Scripting, 8223898)
|
2022-10-30T02:36:09.7838891Z |                   |                   |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
2754     |
2022-10-30T02:36:09.7839609Z +                   +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7840423Z |                   | CVE-2020-2755    |
|                   |               | OpenJDK: Incorrect handling of
|
2022-10-30T02:36:09.7840901Z |                   |                   |
|                   |               | empty string nodes in regular
|
2022-10-30T02:36:09.7841361Z |                   |                   |
|                   |               | expression Parser (Scripting,...
|
2022-10-30T02:36:09.7842045Z |                   |                   |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
2755     |
2022-10-30T02:36:09.7842757Z +                   +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7843662Z |                   | CVE-2020-2756    |
|                   |               | OpenJDK: Incorrect handling
|
2022-10-30T02:36:09.7844152Z |                   |                   |
|                   |               | of references to uninitialized
|
2022-10-30T02:36:09.7844600Z |                   |                   |
|                   |               | class descriptors during
|
2022-10-30T02:36:09.7845063Z |                   |                   |
|                   |               | deserialization (Serialization,...
|
```

```
2022-10-30T02:36:09.7845743Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2020-
2756     |
2022-10-30T02:36:09.7846456Z +                  +------------------+
+                  +              +-----------------------------------
------+
2022-10-30T02:36:09.7847198Z |                  | CVE-2020-2757    |
|                  |              | OpenJDK: Uncaught
InstantiationError     |
2022-10-30T02:36:09.7847692Z |                  |                  |
|                  |              | exception in ObjectStreamClass
|
2022-10-30T02:36:09.7848135Z |                  |                  |
|                  |              | (Serialization, 8224549)
|
2022-10-30T02:36:09.7848804Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2020-
2757     |
2022-10-30T02:36:09.7849518Z +                  +------------------+
+                  +              +-----------------------------------
------+
2022-10-30T02:36:09.7850255Z |                  | CVE-2020-2773    |
|                  |              | OpenJDK: Unexpected exceptions
|
2022-10-30T02:36:09.7850736Z |                  |                  |
|                  |              | raised by DOMKeyInfoFactory
|
2022-10-30T02:36:09.7851188Z |                  |                  |
|                  |              | and DOMXMLSignatureFactory
|
2022-10-30T02:36:09.7851741Z |                  |                  |
|                  |              | (Security, 8231415)
|
2022-10-30T02:36:09.7852434Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2020-
2773     |
2022-10-30T02:36:09.7853199Z +------------------+------------------+----
------+                  +--------------+-------------------------------
------------+
2022-10-30T02:36:09.7854034Z | openjdk8-jre-lib  | CVE-2020-14583   |
HIGH     |                  | 8.272.10-r0   | OpenJDK: Bypass of
boundary checks       |
2022-10-30T02:36:09.7854569Z |                  |                  |
|                  |              | in nio.Buffer via concurrent
|
2022-10-30T02:36:09.7855023Z |                  |                  |
|                  |              | access (Libraries, 8238920)...
|
2022-10-30T02:36:09.7855728Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2020-
14583    |
2022-10-30T02:36:09.7856545Z +                  +------------------+
+                  +              +-----------------------------------
------+
2022-10-30T02:36:09.7857283Z |                  | CVE-2020-14593   |
|                  |              | OpenJDK: Incomplete bounds checks
in     |
```

```
2022-10-30T02:36:09.7857784Z |                   |                  |
|                   |               | Affine Transformations (2D,
8240119)     |
2022-10-30T02:36:09.7858469Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
14593    |
2022-10-30T02:36:09.7859184Z +                   +------------------+
+                   +---------------+-----------------------------------
------+
2022-10-30T02:36:09.7859947Z |                   | CVE-2020-2604    |
|                   | 8.242.08-r0   | OpenJDK: Serialization filter
|
2022-10-30T02:36:09.7860450Z |                   |                  |
|                   |               | changes via jdk.serialFilter
|
2022-10-30T02:36:09.7860893Z |                   |                  |
|                   |               | property modification
|
2022-10-30T02:36:09.7861332Z |                   |                  |
|                   |               | (Serialization, 8231422)
|
2022-10-30T02:36:09.7862005Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
2604     |
2022-10-30T02:36:09.7862733Z +                   +------------------+
+                   +---------------+-----------------------------------
------+
2022-10-30T02:36:09.7863517Z |                   | CVE-2020-2803    |
|                   | 8.252.09-r0   | OpenJDK: Incorrect bounds checks
|
2022-10-30T02:36:09.7864033Z |                   |                  |
|                   |               | in NIO Buffers (Libraries, 8234841)
|
2022-10-30T02:36:09.7864721Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
2803     |
2022-10-30T02:36:09.7865435Z +                   +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7866164Z |                   | CVE-2020-2805    |
|                   |               | OpenJDK: Incorrect type checks
|
2022-10-30T02:36:09.7866643Z |                   |                  |
|                   |               | in MethodType.readObject()
|
2022-10-30T02:36:09.7867081Z |                   |                  |
|                   |               | (Libraries, 8235274)
|
2022-10-30T02:36:09.7867747Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
2805     |
2022-10-30T02:36:09.7868591Z +                   +------------------+----
------+                   +---------------+-------------------------------
------------+
2022-10-30T02:36:09.7869379Z |                   | CVE-2019-2745    |
MEDIUM   |                   | 8.222.10-r0   | OpenJDK: Side-channel
attack             |
```

```
2022-10-30T02:36:09.7869865Z |                  |                  |
|                   |              | risks in Elliptic Curve (EC)
|
2022-10-30T02:36:09.7870319Z |                  |                  |
|                   |              | cryptography (Security, 8208698)
|
2022-10-30T02:36:09.7870999Z |                  |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2019-
2745     |
2022-10-30T02:36:09.7871715Z +                  +------------------+
+                   +              +-----------------------------------
------+
2022-10-30T02:36:09.7872528Z |                  | CVE-2019-2762    |
|                   |              | OpenJDK: Insufficient checks
|
2022-10-30T02:36:09.7873002Z |                  |                  |
|                   |              | of suppressed exceptions in
|
2022-10-30T02:36:09.7873458Z |                  |                  |
|                   |              | deserialization (Utilities,
8212328)     |
2022-10-30T02:36:09.7874139Z |                  |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2019-
2762     |
2022-10-30T02:36:09.7874856Z +                  +------------------+
+                   +              +-----------------------------------
------+
2022-10-30T02:36:09.7875581Z |                  | CVE-2019-2769    |
|                   |              | OpenJDK: Unbounded memory
|
2022-10-30T02:36:09.7876067Z |                  |                  |
|                   |              | allocation during deserialization
|
2022-10-30T02:36:09.7876538Z |                  |                  |
|                   |              | in Collections (Utilities, 8213432)
|
2022-10-30T02:36:09.7877222Z |                  |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2019-
2769     |
2022-10-30T02:36:09.7877939Z +                  +------------------+
+                   +              +-----------------------------------
------+
2022-10-30T02:36:09.7878669Z |                  | CVE-2019-2816    |
|                   |              | OpenJDK: Missing URL format
|
2022-10-30T02:36:09.7879194Z |                  |                  |
|                   |              | validation (Networking, 8221518)
|
2022-10-30T02:36:09.7910582Z |                  |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2019-
2816     |
2022-10-30T02:36:09.7911491Z +                  +------------------+
+                   +--------------+-----------------------------------
------+
2022-10-30T02:36:09.7912261Z |                  | CVE-2019-2949    |
|                   | 8.232.09-r0  | OpenJDK: Improper handling
|
```

```
2022-10-30T02:36:09.7912766Z |                  |                  |
|                   |              | of Kerberos proxy credentials
|
2022-10-30T02:36:09.7913213Z |                  |                  |
|                   |              | (Kerberos, 8220302)
|
2022-10-30T02:36:09.7913882Z |                  |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2019-
2949     |
2022-10-30T02:36:09.7914597Z +                  +------------------+
+                   +              +-----------------------------------
------+
2022-10-30T02:36:09.7915482Z |                  | CVE-2019-2958    |
|                   |              | OpenJDK: Incorrect
|
2022-10-30T02:36:09.7915946Z |                  |                  |
|                   |              | escaping of command line
|
2022-10-30T02:36:09.7916385Z |                  |                  |
|                   |              | arguments in ProcessImpl
|
2022-10-30T02:36:09.7916829Z |                  |                  |
|                   |              | on Windows (Libraries,...
|
2022-10-30T02:36:09.7917501Z |                  |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2019-
2958     |
2022-10-30T02:36:09.7918215Z +                  +------------------+
+                   +              +-----------------------------------
------+
2022-10-30T02:36:09.7918949Z |                  | CVE-2019-2975    |
|                   |              | OpenJDK: Unexpected exception
thrown     |
2022-10-30T02:36:09.7919538Z |                  |                  |
|                   |              | during regular expression
processing     |
2022-10-30T02:36:09.7920006Z |                  |                  |
|                   |              | in Nashorn (Scripting, 8223518)...
|
2022-10-30T02:36:09.7920699Z |                  |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2019-
2975     |
2022-10-30T02:36:09.7921412Z +                  +------------------+
+                   +              +-----------------------------------
------+
2022-10-30T02:36:09.7922135Z |                  | CVE-2019-2989    |
|                   |              | OpenJDK: Incorrect handling of HTTP
|
2022-10-30T02:36:09.7922632Z |                  |                  |
|                   |              | proxy responses in
HttpURLConnection     |
2022-10-30T02:36:09.7923100Z |                  |                  |
|                   |              | (Networking, 8225298)
|
2022-10-30T02:36:09.7924070Z |                  |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2019-
2989     |
```

```
2022-10-30T02:36:09.7924790Z +                   +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7925526Z |                   | CVE-2019-2999    |
|                   |               | OpenJDK: Insufficient filtering
|
2022-10-30T02:36:09.7926007Z |                   |                  |
|                   |               | of HTML event attributes in
|
2022-10-30T02:36:09.7926453Z |                   |                  |
|                   |               | Javadoc (Javadoc, 8226765)
|
2022-10-30T02:36:09.7927131Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2019-
2999     |
2022-10-30T02:36:09.7927869Z +                   +------------------+
+                   +---------------+-----------------------------------
------+
2022-10-30T02:36:09.7928630Z |                   | CVE-2019-7317    |
|                   | 8.222.10-r0   | libpng: use-after-free in
|
2022-10-30T02:36:09.7929112Z |                   |                  |
|                   |               | png_image_free in png.c
|
2022-10-30T02:36:09.7929778Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2019-
7317     |
2022-10-30T02:36:09.7930513Z +                   +------------------+
+                   +---------------+-----------------------------------
------+
2022-10-30T02:36:09.7931284Z |                   | CVE-2020-14556   |
|                   | 8.272.10-r0   | OpenJDK: Incorrect handling
|
2022-10-30T02:36:09.7931878Z |                   |                  |
|                   |               | of access control context in
|
2022-10-30T02:36:09.7932335Z |                   |                  |
|                   |               | ForkJoinPool (Libraries, 8237117)
|
2022-10-30T02:36:09.7933021Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
14556    |
2022-10-30T02:36:09.7933735Z +                   +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7934476Z |                   | CVE-2020-14621   |
|                   |               | OpenJDK: XML validation
manipulation     |
2022-10-30T02:36:09.7934969Z |                   |                  |
|                   |               | due to incomplete application of
|
2022-10-30T02:36:09.7935737Z |                   |                  |
|                   |               | the use-grammar-pool-only
feature...     |
2022-10-30T02:36:09.7936436Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
14621    |
```

```
2022-10-30T02:36:09.7937149Z +                  +------------------+
+                  +              +-----------------------------------
------+
2022-10-30T02:36:09.7937873Z |                  | CVE-2020-14792   |
|                  |              | OpenJDK: Integer overflow
|
2022-10-30T02:36:09.7938547Z |                  |                  |
|                  |              | leading to out-of-bounds
|
2022-10-30T02:36:09.7938993Z |                  |                  |
|                  |              | access (Hotspot, 8241114)
|
2022-10-30T02:36:09.7939667Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2020-
14792    |
2022-10-30T02:36:09.7940391Z +                  +------------------+
+                  +              +-----------------------------------
------+
2022-10-30T02:36:09.7941127Z |                  | CVE-2020-14803   |
|                  |              | OpenJDK: Race condition in NIO
Buffer    |
2022-10-30T02:36:09.7941627Z |                  |                  |
|                  |              | boundary checks (Libraries,
8244136)     |
2022-10-30T02:36:09.7942314Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2020-
14803    |
2022-10-30T02:36:09.7943048Z +                  +------------------+
+                  +--------------+-----------------------------------
------+
2022-10-30T02:36:09.7943798Z |                  | CVE-2020-2593    |
|                  | 8.242.08-r0  | OpenJDK: Incorrect
|
2022-10-30T02:36:09.7944273Z |                  |                  |
|                  |              | isBuiltinStreamHandler check
|
2022-10-30T02:36:09.7944720Z |                  |                  |
|                  |              | causing URL normalization
|
2022-10-30T02:36:09.7945168Z |                  |                  |
|                  |              | issues (Networking, 8228548)
|
2022-10-30T02:36:09.7945849Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2020-
2593     |
2022-10-30T02:36:09.7946565Z +                  +------------------+
+                  +              +-----------------------------------
------+
2022-10-30T02:36:09.7947283Z |                  | CVE-2020-2601    |
|                  |              | OpenJDK: Use of unsafe
|
2022-10-30T02:36:09.7948041Z |                  |                  |
|                  |              | RSA-MD5 checksum in Kerberos
|
2022-10-30T02:36:09.7948497Z |                  |                  |
|                  |              | TGS (Security, 8229951)
|
```

```
2022-10-30T02:36:09.7949167Z |                    |                  |
|                    |               | -->avd.aquasec.com/nvd/cve-2020-
2601     |
2022-10-30T02:36:09.7949900Z +                    +------------------+
+                    +---------------+-----------------------------------
------+
2022-10-30T02:36:09.7950657Z |                    | CVE-2020-2781    |
|                    | 8.252.09-r0   | OpenJDK: Re-use of single
|
2022-10-30T02:36:09.7951132Z |                    |                  |
|                    |               | TLS session for new
|
2022-10-30T02:36:09.7951571Z |                    |                  |
|                    |               | connections (JSSE, 8234408)
|
2022-10-30T02:36:09.7952341Z |                    |                  |
|                    |               | -->avd.aquasec.com/nvd/cve-2020-
2781     |
2022-10-30T02:36:09.7953055Z +                    +------------------+
+                    +               +-----------------------------------
------+
2022-10-30T02:36:09.7953788Z |                    | CVE-2020-2800    |
|                    |               | OpenJDK: CRLF injection into HTTP
|
2022-10-30T02:36:09.7954282Z |                    |                  |
|                    |               | headers in HttpServer (Lightweight
|
2022-10-30T02:36:09.7954718Z |                    |                  |
|                    |               | HTTP Server, 8234825)...
|
2022-10-30T02:36:09.7955392Z |                    |                  |
|                    |               | -->avd.aquasec.com/nvd/cve-2020-
2800     |
2022-10-30T02:36:09.7956113Z +                    +------------------+
+                    +               +-----------------------------------
------+
2022-10-30T02:36:09.7956845Z |                    | CVE-2020-2830    |
|                    |               | OpenJDK: Regular expression DoS
|
2022-10-30T02:36:09.7957334Z |                    |                  |
|                    |               | in Scanner (Concurrency, 8236201)
|
2022-10-30T02:36:09.7958020Z |                    |                  |
|                    |               | -->avd.aquasec.com/nvd/cve-2020-
2830     |
2022-10-30T02:36:09.7958765Z +                    +------------------+----
------+                   +---------------+-------------------------------
------------+
2022-10-30T02:36:09.7959552Z |                    | CVE-2019-2766    | LOW
|                    | 8.222.10-r0   | OpenJDK: Insufficient permission
|
2022-10-30T02:36:09.7960050Z |                    |                  |
|                    |               | checks for file:// URLs on
|
2022-10-30T02:36:09.7960504Z |                    |                  |
|                    |               | Windows (Networking, 8213431)
|
```

```
2022-10-30T02:36:09.7961181Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2019-
2766     |
2022-10-30T02:36:09.7961892Z +                   +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7962622Z |                   | CVE-2019-2786    |
|                   |               | OpenJDK: Insufficient
|
2022-10-30T02:36:09.7963089Z |                   |                  |
|                   |               | restriction of privileges in
|
2022-10-30T02:36:09.7963644Z |                   |                  |
|                   |               | AccessController (Security,
8216381)     |
2022-10-30T02:36:09.7964453Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2019-
2786     |
2022-10-30T02:36:09.7965165Z +                   +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7965892Z |                   | CVE-2019-2842    |
|                   |               | OpenJDK: Missing array bounds check
|
2022-10-30T02:36:09.7966381Z |                   |                  |
|                   |               | in crypto providers (JCE, 8223511)
|
2022-10-30T02:36:09.7967063Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2019-
2842     |
2022-10-30T02:36:09.7967800Z +                   +------------------+
+                   +---------------+-----------------------------------
------+
2022-10-30T02:36:09.7968565Z |                   | CVE-2019-2894    |
|                   | 8.232.09-r0   | OpenJDK: Side-channel
|
2022-10-30T02:36:09.7969121Z |                   |                  |
|                   |               | vulnerability in the ECDSA
|
2022-10-30T02:36:09.7969579Z |                   |                  |
|                   |               | implementation (Security, 8228825)
|
2022-10-30T02:36:09.7970269Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2019-
2894     |
2022-10-30T02:36:09.7970983Z +                   +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7971715Z |                   | CVE-2019-2933    |
|                   |               | OpenJDK: FilePermission checks
|
2022-10-30T02:36:09.7972192Z |                   |                  |
|                   |               | not preformed correctly on
|
2022-10-30T02:36:09.7972646Z |                   |                  |
|                   |               | Windows (Libraries, 8213429)
|
```

```
2022-10-30T02:36:09.7973318Z |                    |                  |
|                    |               | -->avd.aquasec.com/nvd/cve-2019-
2933     |
2022-10-30T02:36:09.7974032Z +                    +------------------+
+                    +               +-----------------------------------
------+
2022-10-30T02:36:09.7974760Z |                    | CVE-2019-2945    |
|                    |               | OpenJDK: Missing restrictions
|
2022-10-30T02:36:09.7975233Z |                    |                  |
|                    |               | on use of custom SocketImpl
|
2022-10-30T02:36:09.7975670Z |                    |                  |
|                    |               | (Networking, 8218573)
|
2022-10-30T02:36:09.7976328Z |                    |                  |
|                    |               | -->avd.aquasec.com/nvd/cve-2019-
2945     |
2022-10-30T02:36:09.7977042Z +                    +------------------+
+                    +               +-----------------------------------
------+
2022-10-30T02:36:09.7977776Z |                    | CVE-2019-2962    |
|                    |               | OpenJDK: NULL pointer dereference
|
2022-10-30T02:36:09.7978266Z |                    |                  |
|                    |               | in DrawGlyphList (2D, 8222690)
|
2022-10-30T02:36:09.7978980Z |                    |                  |
|                    |               | -->avd.aquasec.com/nvd/cve-2019-
2962     |
2022-10-30T02:36:09.7979700Z +                    +------------------+
+                    +               +-----------------------------------
------+
2022-10-30T02:36:09.7980423Z |                    | CVE-2019-2964    |
|                    |               | OpenJDK: Unexpected exception
|
2022-10-30T02:36:09.7980981Z |                    |                  |
|                    |               | thrown by Pattern processing
|
2022-10-30T02:36:09.7981430Z |                    |                  |
|                    |               | crafted regular expression
|
2022-10-30T02:36:09.7981876Z |                    |                  |
|                    |               | (Concurrency, 8222684)...
|
2022-10-30T02:36:09.7982558Z |                    |                  |
|                    |               | -->avd.aquasec.com/nvd/cve-2019-
2964     |
2022-10-30T02:36:09.7983277Z +                    +------------------+
+                    +               +-----------------------------------
------+
2022-10-30T02:36:09.7984011Z |                    | CVE-2019-2973    |
|                    |               | OpenJDK: Unexpected exception
thrown     |
2022-10-30T02:36:09.7984575Z |                    |                  |
|                    |               | by XPathParser processing crafted
|
```

```
2022-10-30T02:36:09.7985043Z |                  |                  |
|                   |              | XPath expression (JAXP, 8223505)...
|
2022-10-30T02:36:09.7985732Z |                  |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2019-
2973     |
2022-10-30T02:36:09.7986447Z +                  +------------------+
+                   +              +-----------------------------------
------+
2022-10-30T02:36:09.7987162Z |                  | CVE-2019-2978    |
|                   |              | OpenJDK: Incorrect handling
|
2022-10-30T02:36:09.7987630Z |                  |                  |
|                   |              | of nested jar: URLs in Jar
|
2022-10-30T02:36:09.7988084Z |                  |                  |
|                   |              | URL handler (Networking,...
|
2022-10-30T02:36:09.7988768Z |                  |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2019-
2978     |
2022-10-30T02:36:09.7989485Z +                  +------------------+
+                   +              +-----------------------------------
------+
2022-10-30T02:36:09.7990214Z |                  | CVE-2019-2981    |
|                   |              | OpenJDK: Unexpected exception
|
2022-10-30T02:36:09.7990697Z |                  |                  |
|                   |              | thrown by XPath processing crafted
|
2022-10-30T02:36:09.7991172Z |                  |                  |
|                   |              | XPath expression (JAXP, 8224532)...
|
2022-10-30T02:36:09.7991858Z |                  |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2019-
2981     |
2022-10-30T02:36:09.7992587Z +                  +------------------+
+                   +              +-----------------------------------
------+
2022-10-30T02:36:09.7993325Z |                  | CVE-2019-2983    |
|                   |              | OpenJDK: Unexpected exception
thrown     |
2022-10-30T02:36:09.7993820Z |                  |                  |
|                   |              | during Font object deserialization
|
2022-10-30T02:36:09.7994272Z |                  |                  |
|                   |              | (Serialization, 8224915)
|
2022-10-30T02:36:09.7994939Z |                  |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2019-
2983     |
2022-10-30T02:36:09.7995649Z +                  +------------------+
+                   +              +-----------------------------------
------+
2022-10-30T02:36:09.7996483Z |                  | CVE-2019-2987    |
|                   |              | OpenJDK: Missing glyph bitmap
|
```

```
2022-10-30T02:36:09.7996958Z |                  |                  |
|                   |               | image dimension check in
|
2022-10-30T02:36:09.7997388Z |                  |                  |
|                   |               | FreetypeFontScaler (2D, 8225286)
|
2022-10-30T02:36:09.7998069Z |                  |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2019-
2987     |
2022-10-30T02:36:09.7998787Z +                  +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.7999526Z |                  | CVE-2019-2988    |
|                   |               | OpenJDK: Integer overflow in bounds
|
2022-10-30T02:36:09.8000024Z |                  |                  |
|                   |               | check in SunGraphics2D (2D,
8225292)     |
2022-10-30T02:36:09.8000795Z |                  |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2019-
2988     |
2022-10-30T02:36:09.8001511Z +                  +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.8002239Z |                  | CVE-2019-2992    |
|                   |               | OpenJDK: Excessive memory
|
2022-10-30T02:36:09.8002717Z |                  |                  |
|                   |               | allocation in CMap when reading
|
2022-10-30T02:36:09.8003302Z |                  |                  |
|                   |               | TrueType font (2D, 8225597)...
|
2022-10-30T02:36:09.8003999Z |                  |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2019-
2992     |
2022-10-30T02:36:09.8004734Z +                  +------------------+
+                   +---------------+-----------------------------------
------+
2022-10-30T02:36:09.8005499Z |                  | CVE-2020-14577   |
|                   | 8.272.10-r0   | OpenJDK: HostnameChecker does
|
2022-10-30T02:36:09.8005994Z |                  |                  |
|                   |               | not ensure X.509 certificate
|
2022-10-30T02:36:09.8006443Z |                  |                  |
|                   |               | names are in normalized form...
|
2022-10-30T02:36:09.8007116Z |                  |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
14577    |
2022-10-30T02:36:09.8007831Z +                  +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.8008564Z |                  | CVE-2020-14578   |
|                   |               | OpenJDK: Unexpected exception
|
```

```
2022-10-30T02:36:09.8009043Z |                  |                  |
|                   |              | raised by DerInputStream
|
2022-10-30T02:36:09.8009481Z |                  |                  |
|                   |              | (Libraries, 8237731)
|
2022-10-30T02:36:09.8010154Z |                  |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2020-
14578    |
2022-10-30T02:36:09.8010871Z +                  +------------------+
+                   +              +-----------------------------------
------+
2022-10-30T02:36:09.8011601Z |                  | CVE-2020-14579   |
|                   |              | OpenJDK: Unexpected exception
|
2022-10-30T02:36:09.8012077Z |                  |                  |
|                   |              | raised by DerValue.equals()
|
2022-10-30T02:36:09.8012612Z |                  |                  |
|                   |              | (Libraries, 8237736)
|
2022-10-30T02:36:09.8013293Z |                  |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2020-
14579    |
2022-10-30T02:36:09.8014006Z +                  +------------------+
+                   +              +-----------------------------------
------+
2022-10-30T02:36:09.8014741Z |                  | CVE-2020-14581   |
|                   |              | OpenJDK: Information disclosure
|
2022-10-30T02:36:09.8015226Z |                  |                  |
|                   |              | in color management (2D, 8238002)
|
2022-10-30T02:36:09.8015904Z |                  |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2020-
14581    |
2022-10-30T02:36:09.8016706Z +                  +------------------+
+                   +              +-----------------------------------
------+
2022-10-30T02:36:09.8017431Z |                  | CVE-2020-14779   |
|                   |              | OpenJDK: High memory usage
|
2022-10-30T02:36:09.8017914Z |                  |                  |
|                   |              | during deserialization of Proxy
|
2022-10-30T02:36:09.8018368Z |                  |                  |
|                   |              | class with many interfaces...
|
2022-10-30T02:36:09.8019029Z |                  |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2020-
14779    |
2022-10-30T02:36:09.8019799Z +                  +------------------+
+                   +              +-----------------------------------
------+
2022-10-30T02:36:09.8020524Z |                  | CVE-2020-14781   |
|                   |              | OpenJDK: Credentials sent
|
```

```
2022-10-30T02:36:09.8021000Z |                  |                  |
|                   |              | over unencrypted LDAP
|
2022-10-30T02:36:09.8021437Z |                  |                  |
|                   |              | connection (JNDI, 8237990)
|
2022-10-30T02:36:09.8022113Z |                  |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2020-
14781    |
2022-10-30T02:36:09.8022826Z +                  +------------------+
+                   +              +-----------------------------------
------+
2022-10-30T02:36:09.8023558Z |                  | CVE-2020-14782   |
|                   |              | OpenJDK: Certificate blacklist
|
2022-10-30T02:36:09.8024048Z |                  |                  |
|                   |              | bypass via alternate certificate
|
2022-10-30T02:36:09.8024516Z |                  |                  |
|                   |              | encodings (Libraries, 8237995)
|
2022-10-30T02:36:09.8025196Z |                  |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2020-
14782    |
2022-10-30T02:36:09.8025911Z +                  +------------------+
+                   +              +-----------------------------------
------+
2022-10-30T02:36:09.8026637Z |                  | CVE-2020-14796   |
|                   |              | OpenJDK: Missing permission
|
2022-10-30T02:36:09.8027101Z |                  |                  |
|                   |              | check in path to URI
|
2022-10-30T02:36:09.8027548Z |                  |                  |
|                   |              | conversion (Libraries, 8242680)
|
2022-10-30T02:36:09.8028343Z |                  |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2020-
14796    |
2022-10-30T02:36:09.8029065Z +                  +------------------+
+                   +              +-----------------------------------
------+
2022-10-30T02:36:09.8029785Z |                  | CVE-2020-14797   |
|                   |              | OpenJDK: Incomplete check for
|
2022-10-30T02:36:09.8030258Z |                  |                  |
|                   |              | invalid characters in URI to
|
2022-10-30T02:36:09.8030711Z |                  |                  |
|                   |              | path conversion (Libraries,...
|
2022-10-30T02:36:09.8031397Z |                  |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2020-
14797    |
2022-10-30T02:36:09.8032116Z +                  +------------------+
+                   +              +-----------------------------------
------+
```

```
2022-10-30T02:36:09.8032940Z |                   | CVE-2020-14798   |
|                   |               | OpenJDK: Missing maximum length
check in |
2022-10-30T02:36:09.8033451Z |                   |                  |
|                   |               |
WindowsNativeDispatcher.asNativeBuffer() |
2022-10-30T02:36:09.8033910Z |                   |                  |
|                   |               | (Libraries, 8242695)
|
2022-10-30T02:36:09.8034578Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
14798    |
2022-10-30T02:36:09.8035312Z +                   +------------------+
+                   +---------------+-----------------------------------
------+
2022-10-30T02:36:09.8036079Z |                   | CVE-2020-2583    |
|                   | 8.242.08-r0   | OpenJDK: Incorrect exception
|
2022-10-30T02:36:09.8036591Z |                   |                  |
|                   |               | processing during deserialization
|
2022-10-30T02:36:09.8037048Z |                   |                  |
|                   |               | in BeanContextSupport
|
2022-10-30T02:36:09.8037485Z |                   |                  |
|                   |               | (Serialization, 8224909)
|
2022-10-30T02:36:09.8038156Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
2583     |
2022-10-30T02:36:09.8038871Z +                   +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.8039595Z |                   | CVE-2020-2590    |
|                   |               | OpenJDK: Improper checks of
|
2022-10-30T02:36:09.8040051Z |                   |                  |
|                   |               | SASL message properties in
|
2022-10-30T02:36:09.8040511Z |                   |                  |
|                   |               | GssKrb5Base (Security, 8226352)
|
2022-10-30T02:36:09.8041192Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
2590     |
2022-10-30T02:36:09.8041909Z +                   +------------------+
+                   +               +-----------------------------------
------+
2022-10-30T02:36:09.8042642Z |                   | CVE-2020-2654    |
|                   |               | OpenJDK: Excessive memory usage
|
2022-10-30T02:36:09.8043211Z |                   |                  |
|                   |               | in OID processing in X.509
|
2022-10-30T02:36:09.8043672Z |                   |                  |
|                   |               | certificate parsing (Libraries,...
|
```

```
2022-10-30T02:36:09.8044457Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2020-
2654     |
2022-10-30T02:36:09.8045171Z +                  +------------------+
+                  +              +-----------------------------------
------+
2022-10-30T02:36:09.8045902Z |                  | CVE-2020-2659    |
|                  |              | OpenJDK: Incomplete enforcement
|
2022-10-30T02:36:09.8046383Z |                  |                  |
|                  |              | of maxDatagramSockets limit
|
2022-10-30T02:36:09.8046824Z |                  |                  |
|                  |              | in DatagramChannelImpl
|
2022-10-30T02:36:09.8047261Z |                  |                  |
|                  |              | (Networking, 8231795)
|
2022-10-30T02:36:09.8047928Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2020-
2659     |
2022-10-30T02:36:09.8048742Z +                  +------------------+
+                  +--------------+-----------------------------------
------+
2022-10-30T02:36:09.8049513Z |                  | CVE-2020-2754    |
|                  | 8.252.09-r0  | OpenJDK: Misplaced regular
|
2022-10-30T02:36:09.8050006Z |                  |                  |
|                  |              | expression syntax error check in
|
2022-10-30T02:36:09.8050451Z |                  |                  |
|                  |              | RegExpScanner (Scripting, 8223898)
|
2022-10-30T02:36:09.8051136Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2020-
2754     |
2022-10-30T02:36:09.8051852Z +                  +------------------+
+                  +              +-----------------------------------
------+
2022-10-30T02:36:09.8052593Z |                  | CVE-2020-2755    |
|                  |              | OpenJDK: Incorrect handling of
|
2022-10-30T02:36:09.8053078Z |                  |                  |
|                  |              | empty string nodes in regular
|
2022-10-30T02:36:09.8053536Z |                  |                  |
|                  |              | expression Parser (Scripting,...
|
2022-10-30T02:36:09.8054219Z |                  |                  |
|                  |              | -->avd.aquasec.com/nvd/cve-2020-
2755     |
2022-10-30T02:36:09.8054934Z +                  +------------------+
+                  +              +-----------------------------------
------+
2022-10-30T02:36:09.8055659Z |                  | CVE-2020-2756    |
|                  |              | OpenJDK: Incorrect handling
|
```

```
2022-10-30T02:36:09.8056144Z |                   |                  |
|                   |              | of references to uninitialized
|
2022-10-30T02:36:09.8056591Z |                   |                  |
|                   |              | class descriptors during
|
2022-10-30T02:36:09.8057042Z |                   |                  |
|                   |              | deserialization (Serialization,...
|
2022-10-30T02:36:09.8057728Z |                   |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2020-
2756     |
2022-10-30T02:36:09.8058441Z +                   +------------------+
+                   +              +-----------------------------------
------+
2022-10-30T02:36:09.8059181Z |                   | CVE-2020-2757    |
|                   |              | OpenJDK: Uncaught
InstantiationError     |
2022-10-30T02:36:09.8059678Z |                   |                  |
|                   |              | exception in ObjectStreamClass
|
2022-10-30T02:36:09.8060223Z |                   |                  |
|                   |              | (Serialization, 8224549)
|
2022-10-30T02:36:09.8060886Z |                   |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2020-
2757     |
2022-10-30T02:36:09.8061601Z +                   +------------------+
+                   +              +-----------------------------------
------+
2022-10-30T02:36:09.8062333Z |                   | CVE-2020-2773    |
|                   |              | OpenJDK: Unexpected exceptions
|
2022-10-30T02:36:09.8062819Z |                   |                  |
|                   |              | raised by DOMKeyInfoFactory
|
2022-10-30T02:36:09.8063267Z |                   |                  |
|                   |              | and DOMXMLSignatureFactory
|
2022-10-30T02:36:09.8063778Z |                   |                  |
|                   |              | (Security, 8231415)
|
2022-10-30T02:36:09.8064449Z |                   |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2020-
2773     |
2022-10-30T02:36:09.8065233Z +-------------------+------------------+----
------+-------------------+---------------+------------------------------
------------+
2022-10-30T02:36:09.8066088Z | sqlite-libs       | CVE-2019-8457    |
CRITICAL | 3.26.0-r3         | 3.28.0-r0     | sqlite: heap out-of-bound
|
2022-10-30T02:36:09.8066620Z |                   |                  |
|                   |              | read in function rtreenode()
|
2022-10-30T02:36:09.8067290Z |                   |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2019-
8457     |
```

```
2022-10-30T02:36:09.8068039Z +                   +------------------+----
------+                   +---------------+------------------------------
------------+
2022-10-30T02:36:09.8068812Z |                   | CVE-2019-19244   |
HIGH     |                   | 3.28.0-r2     | sqlite: allows a crash
|
2022-10-30T02:36:09.8069497Z |                   |                  |
|                   |               | if a sub-select uses both
|
2022-10-30T02:36:09.8069938Z |                   |                  |
|                   |               | DISTINCT and window...
|
2022-10-30T02:36:09.8070605Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2019-
19244    |
2022-10-30T02:36:09.8071332Z +                   +------------------+
+                   +---------------+----------------------------------
------+
2022-10-30T02:36:09.8072076Z |                   | CVE-2019-5018    |
|                   | 3.28.0-r0     | sqlite: Use-after-free in
|
2022-10-30T02:36:09.8072561Z |                   |                  |
|                   |               | window function leading
|
2022-10-30T02:36:09.8072997Z |                   |                  |
|                   |               | to remote code execution
|
2022-10-30T02:36:09.8073670Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2019-
5018     |
2022-10-30T02:36:09.8074407Z +                   +------------------+
+                   +---------------+----------------------------------
------+
2022-10-30T02:36:09.8075179Z |                   | CVE-2020-11655   |
|                   | 3.28.0-r3     | sqlite: malformed window-function
|
2022-10-30T02:36:09.8075664Z |                   |                  |
|                   |               | query leads to DoS
|
2022-10-30T02:36:09.8076408Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
11655    |
2022-10-30T02:36:09.8077157Z +                   +------------------+----
------+                   +---------------+------------------------------
------------+
2022-10-30T02:36:09.8077937Z |                   | CVE-2019-16168   |
MEDIUM   |                   | 3.28.0-r1     | sqlite: Division by zero
in               |
2022-10-30T02:36:09.8078448Z |                   |                  |
|                   |               | whereLoopAddBtreeIndex in sqlite3.c
|
2022-10-30T02:36:09.8079178Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2019-
16168    |
2022-10-30T02:36:09.8079912Z +                   +------------------+
+                   +---------------+----------------------------------
------+
```

```
2022-10-30T02:36:09.8080663Z |                    | CVE-2019-19242   |
|                   | 3.28.0-r2     | sqlite: SQL injection in
|
2022-10-30T02:36:09.8081238Z |                    |                  |
|                   |               | sqlite3ExprCodeTarget in expr.c
|
2022-10-30T02:36:09.8081924Z |                    |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2019-
19242    |
2022-10-30T02:36:09.8082708Z +-------------------+------------------+----
------+-------------------+--------------+-----------------------------
------------+
2022-10-30T02:36:09.8083951Z 2022-10-30T02:36:09.725Z [34mINFO [0m
       Table result includes only package filenames. Use '--format json'
option to get the full path to the package file.
2022-10-30T02:36:09.8084667Z
2022-10-30T02:36:09.8084923Z Java (jar)
2022-10-30T02:36:09.8085200Z ==========
2022-10-30T02:36:09.8085582Z Total: 39 (UNKNOWN: 3, LOW: 2, MEDIUM: 20,
HIGH: 11, CRITICAL: 3)
2022-10-30T02:36:09.8085798Z
2022-10-30T02:36:09.8086666Z +-----------------------------------------
-------+---------------------+----------+-------------------+------------
-------------------+-------------------------------------------------------
------------+
2022-10-30T02:36:09.8087464Z |                      LIBRARY
|  VULNERABILITY ID   | SEVERITY | INSTALLED VERSION |         FIXED
VERSION          |                                TITLE
|
2022-10-30T02:36:09.8088529Z +-----------------------------------------
-------+---------------------+----------+-------------------+------------
-------------------+-------------------------------------------------------
------------+
2022-10-30T02:36:09.8089654Z | ch.qos.logback:logback-core
| CVE-2021-42550      | MEDIUM   | 1.2.3             | 1.2.9
| logback: remote code execution                                    |
2022-10-30T02:36:09.8090305Z | (app.jar)
|                     |          |                   |
| through JNDI call from within                                     |
2022-10-30T02:36:09.8090832Z |
|                     |          |                   |
| its configuration file...                                         |
2022-10-30T02:36:09.8091643Z |
|                     |          |                   |
| -->avd.aquasec.com/nvd/cve-2021-42550                             |
2022-10-30T02:36:09.8092646Z +-----------------------------------------
-------+---------------------+----------+-------------------+------------
-------------------+-------------------------------------------------------
------------+
2022-10-30T02:36:09.8093802Z | com.fasterxml.jackson.core:jackson-
databind      | CVE-2020-36518      | HIGH     | 2.11.0            |
2.12.6.1, 2.13.2.1             | jackson-databind: denial of service
|
2022-10-30T02:36:09.8094626Z | (app.jar)
|                     |          |                   |
| via a large depth of nested objects                               |
```

```
2022-10-30T02:36:09.8095465Z |
|                      |          |                    |
| -->avd.aquasec.com/nvd/cve-2020-36518                          |
2022-10-30T02:36:09.8096396Z +
+----------------------+          +                    +------------------
-------------+-------------------------------------------------------------
-----+
2022-10-30T02:36:09.8097346Z |
| CVE-2022-42003       |          |                    | 2.13.4.1
| jackson-databind: deep                                         |
2022-10-30T02:36:09.8097904Z |
|                      |          |                    |
| wrapper array nesting wrt                                      |
2022-10-30T02:36:09.8098511Z |
|                      |          |                    |
| UNWRAP_SINGLE_VALUE_ARRAYS                                     |
2022-10-30T02:36:09.8099336Z |
|                      |          |                    |
| -->avd.aquasec.com/nvd/cve-2022-42003                          |
2022-10-30T02:36:09.8100248Z +
+----------------------+          +                    +------------------
-------------+-------------------------------------------------------------
-----+
2022-10-30T02:36:09.8101175Z |
| CVE-2022-42004       |          |                    | 2.13.4
| jackson-databind: use                                          |
2022-10-30T02:36:09.8101722Z |
|                      |          |                    |
| of deeply nested arrays                                        |
2022-10-30T02:36:09.8102518Z |
|                      |          |                    |
| -->avd.aquasec.com/nvd/cve-2022-42004                          |
2022-10-30T02:36:09.8103510Z +-----------------------------------------
-------+----------------------+          +--------------------+------------
--------------------+-------------------------------------------------------
------------+
2022-10-30T02:36:09.8104628Z | io.fabric8:kubernetes-client
| CVE-2021-20218       |          | 4.4.1              | 4.7.2, 4.11.2,
4.13.2, 5.0.2   | fabric8-kubernetes-client:
|
2022-10-30T02:36:09.8105293Z | (app.jar)
|                      |          |                    |
| vulnerable to a path traversal                                 |
2022-10-30T02:36:09.8105823Z |
|                      |          |                    |
| leading to integrity and                                       |
2022-10-30T02:36:09.8106340Z |
|                      |          |                    |
| availability compromise...                                     |
2022-10-30T02:36:09.8107151Z |
|                      |          |                    |
| -->avd.aquasec.com/nvd/cve-2021-20218                          |
2022-10-30T02:36:09.8108166Z +-----------------------------------------
-------+----------------------+----------+--------------------+------------
--------------------+-------------------------------------------------------
------------+
```

```
2022-10-30T02:36:09.8109381Z | org.apache.logging.log4j:log4j-api
| CVE-2021-45105      | MEDIUM   | 2.13.2            | 2.12.3, 2.17.0
| log4j-core: DoS in log4j                                        |
2022-10-30T02:36:09.8110036Z | (app.jar)
|                     |          |                   |
| 2.x with Thread Context                                         |
2022-10-30T02:36:09.8110555Z |
|                     |          |                   |
| Map (MDC) input data...                                         |
2022-10-30T02:36:09.8111360Z |
|                     |          |                   |
| -->avd.aquasec.com/nvd/cve-2021-45105                           |
2022-10-30T02:36:09.8112439Z +---------------------------------------
-------+---------------------+----------+-------------------+------------
-------------------+-----------------------------------------------------
------------+
2022-10-30T02:36:09.8113574Z | org.apache.tomcat.embed:tomcat-embed-core
| CVE-2020-13934      | HIGH     | 9.0.35            | 8.5.57, 9.0.37
| tomcat: OutOfMemoryException                                    |
2022-10-30T02:36:09.8114251Z | (app.jar)
|                     |          |                   |
| caused by HTTP/2 connection                                     |
2022-10-30T02:36:09.8114768Z |
|                     |          |                   |
| leak could lead to DoS                                          |
2022-10-30T02:36:09.8115563Z |
|                     |          |                   |
| -->avd.aquasec.com/nvd/cve-2020-13934                           |
2022-10-30T02:36:09.8116481Z +
+---------------------+          +                   +------------------
-------------+-----------------------------------------------------------
-----+
2022-10-30T02:36:09.8117457Z |
| CVE-2020-17527      |          |                   | 8.5.60, 9.0.40,
10.0.2         | tomcat: HTTP/2 request header mix-up
|
2022-10-30T02:36:09.8118329Z |
|                     |          |                   |
| -->avd.aquasec.com/nvd/cve-2020-17527                           |
2022-10-30T02:36:09.8119246Z +
+---------------------+          +                   +------------------
-------------+-----------------------------------------------------------
-----+
2022-10-30T02:36:09.8120221Z |
| CVE-2021-25122      |          |                   | 8.5.62, 9.0.42,
10.0.2         | tomcat: Request mix-up with h2c
|
2022-10-30T02:36:09.8121091Z |
|                     |          |                   |
| -->avd.aquasec.com/nvd/cve-2021-25122                           |
2022-10-30T02:36:09.8122007Z +
+---------------------+          +                   +------------------
-------------+-----------------------------------------------------------
-----+
2022-10-30T02:36:09.8122965Z |
| CVE-2021-25329      |          |                   | 7.0.107, 8.5.61,
```

```
9.0.41        | tomcat: Incomplete fix
|
2022-10-30T02:36:09.8124013Z |
|                      |          |                    |
| for CVE-2020-9484 (RCE                                          |
2022-10-30T02:36:09.8124535Z |
|                      |          |                    |
| via session persistence)                                        |
2022-10-30T02:36:09.8125342Z |
|                      |          |                    |
| -->avd.aquasec.com/nvd/cve-2021-25329                           |
2022-10-30T02:36:09.8126264Z +
+----------------------+----------+                    +-------------------
-------------+-----------------------------------------------------------
-----+
2022-10-30T02:36:09.8127259Z |
| CVE-2021-24122       | MEDIUM   |                    | 10.0.0-M10,
9.0.40, 8.5.60,    | tomcat: Information disclosure
|
2022-10-30T02:36:09.8127969Z |
|                      |          |                    | 7.0.107
| when using NTFS file system                                     |
2022-10-30T02:36:09.8128797Z |
|                      |          |                    |
| -->avd.aquasec.com/nvd/cve-2021-24122                           |
2022-10-30T02:36:09.8129722Z +
+----------------------+----------+                    +-------------------
-------------+-----------------------------------------------------------
-----+
2022-10-30T02:36:09.8130645Z |
| CVE-2021-43980       | LOW      |                    |
| : Apache Tomcat:                                                |
2022-10-30T02:36:09.8131185Z |
|                      |          |                    |
| Information disclosure                                          |
2022-10-30T02:36:09.8131985Z |
|                      |          |                    |
| -->avd.aquasec.com/nvd/cve-2021-43980                           |
2022-10-30T02:36:09.8132963Z +-----------------------------------------
-------+----------------------+----------+                   +------------
-------------------+-----------------------------------------------------
------------+
2022-10-30T02:36:09.8134085Z | org.apache.tomcat.embed:tomcat-embed-
websocket   | CVE-2020-13935       | HIGH     |                    |
7.0.105, 8.5.57, 9.0.37,       | tomcat: multiple requests
|
2022-10-30T02:36:09.8134778Z | (app.jar)
|                      |          |                    | 10.0.2
| with invalid payload length                                     |
2022-10-30T02:36:09.8135324Z |
|                      |          |                    |
| in a WebSocket frame could...                                   |
2022-10-30T02:36:09.8136134Z |
|                      |          |                    |
| -->avd.aquasec.com/nvd/cve-2020-13935                           |
2022-10-30T02:36:09.8137064Z +
+----------------------+----------+                    +-------------------
```

```
-------------+-----------------------------------------------------------
-----+
2022-10-30T02:36:09.8138057Z |
| CVE-2021-24122      | MEDIUM   |                   | 10.0.0-M10,
9.0.40, 8.5.60,    | tomcat: Information disclosure
|
2022-10-30T02:36:09.8138751Z |
|                     |          |                   | 7.0.107
| when using NTFS file system                                    |
2022-10-30T02:36:09.8139580Z |
|                     |          |                   |
| -->avd.aquasec.com/nvd/cve-2021-24122                          |
2022-10-30T02:36:09.8140509Z +
+---------------------+----------+                   +-------------------
-------------+-----------------------------------------------------------
-----+
2022-10-30T02:36:09.8141433Z |
| CVE-2021-43980      | LOW      |                   |
| : Apache Tomcat:                                               |
2022-10-30T02:36:09.8142060Z |
|                     |          |                   |
| Information disclosure                                         |
2022-10-30T02:36:09.8142867Z |
|                     |          |                   |
| -->avd.aquasec.com/nvd/cve-2021-43980                          |
2022-10-30T02:36:09.8143869Z +-----------------------------------------
-------+---------------------+----------+-------------------+------------
-------------------+-----------------------------------------------------
------------+
2022-10-30T02:36:09.8144953Z | org.glassfish:jakarta.el
| CVE-2021-28170      | MEDIUM   | 3.0.3             |
| jakarta-el: ELParserTokenManager                               |
2022-10-30T02:36:09.8145578Z | (app.jar)
|                     |          |                   |
| enables invalid EL                                             |
2022-10-30T02:36:09.8146109Z |
|                     |          |                   |
| expressions to be evaluate                                     |
2022-10-30T02:36:09.8146908Z |
|                     |          |                   |
| -->avd.aquasec.com/nvd/cve-2021-28170                          |
2022-10-30T02:36:09.8147908Z +-----------------------------------------
-------+---------------------+----------+-------------------+------------
-------------------+-----------------------------------------------------
------------+
2022-10-30T02:36:09.8149062Z | org.springframework.boot:spring-boot-
starter-web | CVE-2022-22965      | CRITICAL | 2.3.0.RELEASE     | 2.6.6,
2.5.12                  | spring-framework: RCE via
|
2022-10-30T02:36:09.8149758Z | (app.jar)
|                     |          |                   |
| Data Binding on JDK 9+                                         |
2022-10-30T02:36:09.8150567Z |
|                     |          |                   |
| -->avd.aquasec.com/nvd/cve-2022-22965                          |
2022-10-30T02:36:09.8151489Z +
+---------------------+----------+                   +-------------------
```

```
------------+-------------------------------------------------------------
-----+
2022-10-30T02:36:09.8152487Z |
| GHSA-36p3-wjmg-h94x | UNKNOWN  |                   | 2.5.12, 2.6.6
| Improper Neutralization of Special Elements                       |
2022-10-30T02:36:09.8153390Z |
|                     |          |                   |
| used in an OS Command ('OS Command...                             |
2022-10-30T02:36:09.8154300Z |
|                     |          |                   |
| -->github.com/advisories/GHSA-36p3-wjmg-h94x                      |
2022-10-30T02:36:09.8155312Z +-----------------------------------------
-------+---------------------+----------+-------------------+------------
-------------------+-------------------------------------------------------
------------+
2022-10-30T02:36:09.8156446Z | org.springframework:spring-beans
| CVE-2022-22965      | CRITICAL | 5.2.6.RELEASE     | 5.3.18, 5.2.20
| spring-framework: RCE via                                         |
2022-10-30T02:36:09.8157110Z | (app.jar)
|                     |          |                   |
| Data Binding on JDK 9+                                            |
2022-10-30T02:36:09.8158007Z |
|                     |          |                   |
| -->avd.aquasec.com/nvd/cve-2022-22965                             |
2022-10-30T02:36:09.8158930Z +
+---------------------+----------+                  +-------------------
-------------+-------------------------------------------------------------
-----+
2022-10-30T02:36:09.8159930Z |
| GHSA-36p3-wjmg-h94x | UNKNOWN  |                   | 5.2.20, 5.3.18
| Improper Neutralization of Special Elements                       |
2022-10-30T02:36:09.8160815Z |
|                     |          |                   |
| used in an OS Command ('OS Command...                             |
2022-10-30T02:36:09.8161654Z |
|                     |          |                   |
| -->github.com/advisories/GHSA-36p3-wjmg-h94x                      |
2022-10-30T02:36:09.8162652Z +-----------------------------------------
-------+---------------------+----------+                   +------------
-------------------+-------------------------------------------------------
------------+
2022-10-30T02:36:09.8163828Z | org.springframework:spring-core
| CVE-2021-22118      | HIGH     |                   | 5.2.15, 5.3.7
| spring-web: (re)creating the                                      |
2022-10-30T02:36:09.8164486Z | (app.jar)
|                     |          |                   |
| temporary storage directory                                       |
2022-10-30T02:36:09.8165020Z |
|                     |          |                   |
| could result in  a privilege...                                   |
2022-10-30T02:36:09.8165842Z |
|                     |          |                   |
| -->avd.aquasec.com/nvd/cve-2021-22118                             |
2022-10-30T02:36:09.8166768Z +
+---------------------+----------+                  +-------------------
-------------+-------------------------------------------------------------
-----+
```

```
2022-10-30T02:36:09.8167749Z |
| CVE-2020-5421       | MEDIUM   |                   | 4.3.29.RELEASE,
| springframework: RFD protection                                    |
2022-10-30T02:36:09.8168345Z |
|                     |          |                   | 5.0.19.RELEASE,
| bypass via jsessionid                                              |
2022-10-30T02:36:09.8169316Z |
|                     |          |                   | 5.1.18.RELEASE,
5.2.9.RELEASE  | -->avd.aquasec.com/nvd/cve-2020-5421
|
2022-10-30T02:36:09.8170269Z +
+---------------------+          +                   +------------------
-------------+-------------------------------------------------------------
-----+
2022-10-30T02:36:09.8171227Z |
| CVE-2021-22060      |          |                   | 5.3.14, 5.3.14
| springframework: Additional Log                                    |
2022-10-30T02:36:09.8171801Z |
|                     |          |                   |
| Injection in Spring Framework                                      |
2022-10-30T02:36:09.8172601Z |
|                     |          |                   |
| (follow-up to CVE-2021-22096)                                      |
2022-10-30T02:36:09.8173504Z |
|                     |          |                   |
| -->avd.aquasec.com/nvd/cve-2021-22060                              |
2022-10-30T02:36:09.8174412Z +
+---------------------+          +                   +------------------
-------------+-------------------------------------------------------------
-----+
2022-10-30T02:36:09.8175380Z |
| CVE-2021-22096      |          |                   | 5.2.18, 5.3.11
| springframework: malicious                                         |
2022-10-30T02:36:09.8175968Z |
|                     |          |                   |
| input leads to insertion                                           |
2022-10-30T02:36:09.8176484Z |
|                     |          |                   |
| of additional log entries                                          |
2022-10-30T02:36:09.8177289Z |
|                     |          |                   |
| -->avd.aquasec.com/nvd/cve-2021-22096                              |
2022-10-30T02:36:09.8178201Z +
+---------------------+          +                   +------------------
-------------+-------------------------------------------------------------
-----+
2022-10-30T02:36:09.8179220Z |
| CVE-2022-22950      |          |                   | 5.2.20.RELEASE,
5.3.17         | spring-expression: Denial of service
|
2022-10-30T02:36:09.8179835Z |
|                     |          |                   |
| via specially crafted SpEL expression                              |
2022-10-30T02:36:09.8180657Z |
|                     |          |                   |
| -->avd.aquasec.com/nvd/cve-2022-22950                              |
```

```
2022-10-30T02:36:09.8181569Z +
+---------------------+          +                    +-------------------
-------------+-------------------------------------------------------------
-----+
2022-10-30T02:36:09.8182514Z |
| CVE-2022-22968      |          |                    | 5.2.21, 5.3.19
| Spring Framework: Data                                                  |
2022-10-30T02:36:09.8183075Z |
|                     |          |                    |
| Binding Rules Vulnerability                                             |
2022-10-30T02:36:09.8183969Z |
|                     |          |                    |
| -->avd.aquasec.com/nvd/cve-2022-22968                                   |
2022-10-30T02:36:09.8184886Z +
+---------------------+          +                    +-------------------
-------------+-------------------------------------------------------------
-----+
2022-10-30T02:36:09.8185862Z |
| CVE-2022-22970      |          |                    | 5.2.22.RELEASE,
5.3.20         | springframework: DoS via data binding
|
2022-10-30T02:36:09.8186451Z |
|                     |          |                    |
| to multipartFile or servlet part                                        |
2022-10-30T02:36:09.8187346Z |
|                     |          |                    |
| -->avd.aquasec.com/nvd/cve-2022-22970                                   |
2022-10-30T02:36:09.8188222Z +
+---------------------+          +                    +
+-----------------------------------------------------------------------+
2022-10-30T02:36:09.8189103Z |
| CVE-2022-22971      |          |                    |
| springframework: DoS                                                    |
2022-10-30T02:36:09.8189646Z |
|                     |          |                    |
| with STOMP over WebSocket                                               |
2022-10-30T02:36:09.8190454Z |
|                     |          |                    |
| -->avd.aquasec.com/nvd/cve-2022-22971                                   |
2022-10-30T02:36:09.8191382Z +
+---------------------+----------+                    +-------------------
-------------+-------------------------------------------------------------
-----+
2022-10-30T02:36:09.8192383Z |
| GHSA-36p3-wjmg-h94x | UNKNOWN  |                    | 5.2.20, 5.3.18
| Improper Neutralization of Special Elements                             |
2022-10-30T02:36:09.8193267Z |
|                     |          |                    |
| used in an OS Command ('OS Command...                                   |
2022-10-30T02:36:09.8194096Z |
|                     |          |                    |
| -->github.com/advisories/GHSA-36p3-wjmg-h94x                            |
2022-10-30T02:36:09.8195094Z +-----------------------------------------
-------+---------------------+----------+                   +------------
-------------------+-----------------------------------------------------
------------+
```

```
2022-10-30T02:36:09.8196218Z | org.springframework:spring-expression
| CVE-2022-22950      | MEDIUM   |                   | 5.2.20, 5.3.16
| spring-expression: Denial of service                              |
2022-10-30T02:36:09.8196901Z | (app.jar)
|                     |          |                   |
| via specially crafted SpEL expression                             |
2022-10-30T02:36:09.8197752Z |
|                     |          |                   |
| -->avd.aquasec.com/nvd/cve-2022-22950                             |
2022-10-30T02:36:09.8198827Z +-----------------------------------------
-------+---------------------+          +                   +------------
-------------------+-----------------------------------------------------
------------+
2022-10-30T02:36:09.8199900Z | org.springframework:spring-web
| CVE-2020-5421       |          |                   | 4.3.29.RELEASE,
| springframework: RFD protection                                   |
2022-10-30T02:36:09.8200568Z | (app.jar)
|                     |          |                   | 5.0.19.RELEASE,
| bypass via jsessionid                                             |
2022-10-30T02:36:09.8201452Z |
|                     |          |                   | 5.1.18.RELEASE,
5.2.9.RELEASE  | -->avd.aquasec.com/nvd/cve-2020-5421
|
2022-10-30T02:36:09.8202475Z +-----------------------------------------
-------+---------------------+----------+                  +------------
-------------------+-----------------------------------------------------
------------+
2022-10-30T02:36:09.8203735Z | org.springframework:spring-webmvc
| CVE-2022-22965      | CRITICAL |                   | 5.2.20, 5.3.18
| spring-framework: RCE via                                         |
2022-10-30T02:36:09.8204392Z | (app.jar)
|                     |          |                   |
| Data Binding on JDK 9+                                            |
2022-10-30T02:36:09.8205203Z |
|                     |          |                   |
| -->avd.aquasec.com/nvd/cve-2022-22965                             |
2022-10-30T02:36:09.8206129Z +
+---------------------+----------+                  +-------------------
-------------+-------------------------------------------------------------
-----+
2022-10-30T02:36:09.8207114Z |
| CVE-2020-5421       | MEDIUM   |                   | 4.3.29.RELEASE,
| springframework: RFD protection                                   |
2022-10-30T02:36:09.8207708Z |
|                     |          |                   | 5.0.19.RELEASE,
| bypass via jsessionid                                             |
2022-10-30T02:36:09.8208574Z |
|                     |          |                   | 5.1.18.RELEASE,
5.2.9.RELEASE  | -->avd.aquasec.com/nvd/cve-2020-5421
|
2022-10-30T02:36:09.8209520Z +
+---------------------+          +                  +-------------------
-------------+-------------------------------------------------------------
-----+
2022-10-30T02:36:09.8210510Z |
| CVE-2022-22950      |          |                   | 5.2.20.RELEASE,
```

```
5.3.17         | spring-expression: Denial of service
|
2022-10-30T02:36:09.8211119Z |
|                      |          |                    |
| via specially crafted SpEL expression                          |
2022-10-30T02:36:09.8211937Z |
|                      |          |                    |
| -->avd.aquasec.com/nvd/cve-2022-22950                          |
2022-10-30T02:36:09.8212934Z +----------------------------------------
-------+---------------------+----------+-------------------+------------
-------------------+--------------------------------------------------
------------+
2022-10-30T02:36:09.8214018Z | org.yaml:snakeyaml (app.jar)
| CVE-2022-25857      | HIGH     |              1.26 |
1.31 | snakeyaml: Denial of Service                                    |
2022-10-30T02:36:09.8214723Z |
|                      |          |                    |
| due to missing nested depth                                    |
2022-10-30T02:36:09.8215241Z |
|                      |          |                    |
| limitation for collections...                                  |
2022-10-30T02:36:09.8216062Z |
|                      |          |                    |
| -->avd.aquasec.com/nvd/cve-2022-25857                          |
2022-10-30T02:36:09.8216954Z +
+---------------------+----------+                    +
+-------------------------------------------------------------------+
2022-10-30T02:36:09.8217954Z |
| CVE-2022-38749      | MEDIUM   |                    |
| snakeyaml: Uncaught exception in                               |
2022-10-30T02:36:09.8218567Z |
|                      |          |                    |
| org.yaml.snakeyaml.composer.Composer.composeSequenceNode       |
2022-10-30T02:36:09.8219419Z |
|                      |          |                    |
| -->avd.aquasec.com/nvd/cve-2022-38749                          |
2022-10-30T02:36:09.8220290Z +
+---------------------+          +                    +
+-------------------------------------------------------------------+
2022-10-30T02:36:09.8221190Z |
| CVE-2022-38750      |          |                    |
| snakeyaml: Uncaught exception in                               |
2022-10-30T02:36:09.8221829Z |
|                      |          |                    |
| org.yaml.snakeyaml.constructor.BaseConstructor.constructObject |
2022-10-30T02:36:09.8222692Z |
|                      |          |                    |
| -->avd.aquasec.com/nvd/cve-2022-38750                          |
2022-10-30T02:36:09.8223572Z +
+---------------------+          +                    +
+-------------------------------------------------------------------+
2022-10-30T02:36:09.8224479Z |
| CVE-2022-38751      |          |                    |
| snakeyaml: Uncaught exception in                               |
2022-10-30T02:36:09.8225064Z |
|                      |          |                    |
| java.base/java.util.regex.Pattern$Ques.match                   |
```

```
2022-10-30T02:36:09.8225918Z |
|                      |          |                    |
| -->avd.aquasec.com/nvd/cve-2022-38751                          |
2022-10-30T02:36:09.8226868Z +
+----------------------+          +                    +------------------
-------------+-------------------------------------------------------------
-----+
2022-10-30T02:36:09.8227801Z |
| CVE-2022-38752       |          |                    |
1.32 | snakeyaml: Uncaught exception in                                |
2022-10-30T02:36:09.8228440Z |
|                      |          |                    |
| java.base/java.util.ArrayList.hashCode                         |
2022-10-30T02:36:09.8229279Z |
|                      |          |                    |
| -->avd.aquasec.com/nvd/cve-2022-38752                          |
2022-10-30T02:36:09.8230278Z +-----------------------------------------
-------+---------------------+----------+-------------------+------------
-------------------+-------------------------------------------------------
------------+
2022-10-30T02:36:10.2836395Z 2022-10-30T02:36:10.238Z  [34mINFO [0m
       Detected OS: alpine
2022-10-30T02:36:10.2845389Z 2022-10-30T02:36:10.238Z  [34mINFO [0m
       Detecting Alpine vulnerabilities...
2022-10-30T02:36:10.2846327Z 2022-10-30T02:36:10.244Z  [34mINFO [0m
       Number of language-specific files: 1
2022-10-30T02:36:10.2847173Z 2022-10-30T02:36:10.244Z  [34mINFO [0m
       Detecting jar vulnerabilities...
2022-10-30T02:36:10.2848396Z 2022-10-30T02:36:10.248Z  [33mWARN [0m  This
OS version is no longer supported by the distribution: alpine 3.9.4
2022-10-30T02:36:10.2849437Z 2022-10-30T02:36:10.248Z  [33mWARN [0m  The
vulnerability detection may be insufficient because security updates are
not provided
2022-10-30T02:36:10.2849897Z
2022-10-30T02:36:10.2851002Z ***/spring-boot-kubernetes:latest (alpine
3.9.4)
2022-10-30T02:36:10.2851571Z
==========================================================
2022-10-30T02:36:10.2852059Z Total: 36 (HIGH: 32, CRITICAL: 4)
2022-10-30T02:36:10.2852302Z
2022-10-30T02:36:10.2853042Z +-------------------+-----------------+----
------+-------------------+---------------+------------------------------
---------+
2022-10-30T02:36:10.2853664Z |      LIBRARY      | VULNERABILITY ID |
SEVERITY | INSTALLED VERSION | FIXED VERSION |                TITLE
|
2022-10-30T02:36:10.2854484Z +-------------------+-----------------+----
------+-------------------+---------------+------------------------------
---------+
2022-10-30T02:36:10.2855357Z | krb5-libs         | CVE-2020-28196   |
HIGH     | 1.15.5-r0         | 1.15.5-r1     | krb5: unbounded recursion
via an      |
2022-10-30T02:36:10.2856168Z |                   |                  |
|                   |               | ASN.1-encoded Kerberos message
|
```

```
2022-10-30T02:36:10.2856632Z |                   |                  |
|                   |              | in lib/krb5/asn.1/asn1_encode.c
|
2022-10-30T02:36:10.2857201Z |                   |                  |
|                   |              | may lead...
|
2022-10-30T02:36:10.2857957Z |                   |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2020-
28196 |
2022-10-30T02:36:10.2858847Z +-------------------+------------------+----
------+-------------------+--------------+-----------------------------
---------+
2022-10-30T02:36:10.2859807Z | libbz2            | CVE-2019-12900   |
CRITICAL | 1.0.6-r6          | 1.0.6-r7      | bzip2: out-of-bounds write
|
2022-10-30T02:36:10.2860418Z |                   |                  |
|                   |              | in function BZ2_decompress
|
2022-10-30T02:36:10.2861180Z |                   |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2019-
12900 |
2022-10-30T02:36:10.2862071Z +-------------------+------------------+----
------+-------------------+--------------+-----------------------------
---------+
2022-10-30T02:36:10.2863017Z | libcrypto1.1      | CVE-2020-1967    |
HIGH     | 1.1.1b-r1         | 1.1.1g-r0     | openssl: Segmentation
|
2022-10-30T02:36:10.2863624Z |                   |                  |
|                   |              | fault in SSL_check_chain
|
2022-10-30T02:36:10.2864154Z |                   |                  |
|                   |              | causes denial of service
|
2022-10-30T02:36:10.2865114Z |                   |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2020-
1967  |
2022-10-30T02:36:10.2865944Z +                   +------------------+
+                   +--------------+-----------------------------------
---+
2022-10-30T02:36:10.2866788Z |                   | CVE-2021-23840   |
|                   | 1.1.1j-r0     | openssl: integer
|
2022-10-30T02:36:10.2867355Z |                   |                  |
|                   |              | overflow in CipherUpdate
|
2022-10-30T02:36:10.2868116Z |                   |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2021-
23840 |
2022-10-30T02:36:10.2868946Z +                   +------------------+
+                   +--------------+-----------------------------------
---+
2022-10-30T02:36:10.2869922Z |                   | CVE-2021-3450    |
|                   | 1.1.1k-r0     | openssl: CA certificate check
|
2022-10-30T02:36:10.2870520Z |                   |                  |
|                   |              | bypass with X509_V_FLAG_X509_STRICT
|
```

```
2022-10-30T02:36:10.2871305Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2021-
3450  |
2022-10-30T02:36:10.2872174Z +-------------------+------------------+
+-------------------+---------------+-----------------------------------
---+
2022-10-30T02:36:10.2873113Z | libjpeg-turbo     | CVE-2019-2201    |
| 1.5.3-r4          | 1.5.3-r6      | libjpeg-turbo: several integer
|
2022-10-30T02:36:10.2873731Z |                   |                  |
|                   |               | overflows and subsequent
|
2022-10-30T02:36:10.2874260Z |                   |                  |
|                   |               | segfaults when attempting to
|
2022-10-30T02:36:10.2874810Z |                   |                  |
|                   |               | compress/decompress gigapixel...
|
2022-10-30T02:36:10.2875588Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2019-
2201  |
2022-10-30T02:36:10.2876461Z +-------------------+------------------+
+-------------------+---------------+-----------------------------------
---+
2022-10-30T02:36:10.2877392Z | libssl1.1         | CVE-2020-1967    |
| 1.1.1b-r1         | 1.1.1g-r0     | openssl: Segmentation
|
2022-10-30T02:36:10.2877991Z |                   |                  |
|                   |               | fault in SSL_check_chain
|
2022-10-30T02:36:10.2878518Z |                   |                  |
|                   |               | causes denial of service
|
2022-10-30T02:36:10.2879291Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
1967  |
2022-10-30T02:36:10.2880117Z +                   +------------------+
+                   +---------------+-----------------------------------
---+
2022-10-30T02:36:10.2880962Z |                   | CVE-2021-23840   |
|                   | 1.1.1j-r0     | openssl: integer
|
2022-10-30T02:36:10.2881519Z |                   |                  |
|                   |               | overflow in CipherUpdate
|
2022-10-30T02:36:10.2882286Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2021-
23840 |
2022-10-30T02:36:10.2883236Z +                   +------------------+
+                   +---------------+-----------------------------------
---+
2022-10-30T02:36:10.2884118Z |                   | CVE-2021-3450    |
|                   | 1.1.1k-r0     | openssl: CA certificate check
|
2022-10-30T02:36:10.2884839Z |                   |                  |
|                   |               | bypass with X509_V_FLAG_X509_STRICT
|
```

```
2022-10-30T02:36:10.2885637Z |                   |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2021-
3450  |
2022-10-30T02:36:10.2886508Z +-------------------+------------------+
+-------------------+--------------+-----------------------------------
---+
2022-10-30T02:36:10.2887441Z | libx11            | CVE-2020-14363   |
| 1.6.7-r0          | 1.6.12-r0     | libX11: integer overflow leads
|
2022-10-30T02:36:10.2888051Z |                   |                  |
|                   |              | to double free in locale handling
|
2022-10-30T02:36:10.2888823Z |                   |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2020-
14363 |
2022-10-30T02:36:10.2889748Z +-------------------+------------------+----
------+-------------------+--------------+-----------------------------
---------+
2022-10-30T02:36:10.2890812Z | musl              | CVE-2019-14697   |
CRITICAL | 1.1.20-r4         | 1.1.20-r5     | musl libc through 1.1.23
|
2022-10-30T02:36:10.2891643Z |                   |                  |
|                   |              | has an x87 floating-point
|
2022-10-30T02:36:10.2892189Z |                   |                  |
|                   |              | stack adjustment im ......
|
2022-10-30T02:36:10.2892954Z |                   |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2019-
14697 |
2022-10-30T02:36:10.2893744Z +-------------------+                  +
+                   +              +
+
2022-10-30T02:36:10.2894499Z | musl-utils        |                  |
|                   |              |
|
2022-10-30T02:36:10.2894993Z |                   |                  |
|                   |              |
|
2022-10-30T02:36:10.2895459Z |                   |                  |
|                   |              |
|
2022-10-30T02:36:10.2895920Z |                   |                  |
|                   |              |
|
2022-10-30T02:36:10.2896740Z +-------------------+------------------+----
------+-------------------+--------------+-----------------------------
---------+
2022-10-30T02:36:10.2897704Z | openjdk8          | CVE-2020-14583   |
HIGH     | 8.212.04-r0       | 8.272.10-r0   | OpenJDK: Bypass of
boundary checks    |
2022-10-30T02:36:10.2898338Z |                   |                  |
|                   |              | in nio.Buffer via concurrent
|
2022-10-30T02:36:10.2898874Z |                   |                  |
|                   |              | access (Libraries, 8238920)...
|
```

```
2022-10-30T02:36:10.2899655Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
14583 |
2022-10-30T02:36:10.2900470Z +                   +------------------+
+                   +               +-----------------------------------
---+
2022-10-30T02:36:10.2901304Z |                   | CVE-2020-14593   |
|                   |               | OpenJDK: Incomplete bounds checks
in  |
2022-10-30T02:36:10.2901892Z |                   |                  |
|                   |               | Affine Transformations (2D,
8240119)  |
2022-10-30T02:36:10.2902677Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
14593 |
2022-10-30T02:36:10.2903502Z +                   +------------------+
+                   +---------------+-----------------------------------
---+
2022-10-30T02:36:10.2904467Z |                   | CVE-2020-2604    |
|                   | 8.242.08-r0   | OpenJDK: Serialization filter
|
2022-10-30T02:36:10.2905055Z |                   |                  |
|                   |               | changes via jdk.serialFilter
|
2022-10-30T02:36:10.2905583Z |                   |                  |
|                   |               | property modification
|
2022-10-30T02:36:10.2906101Z |                   |                  |
|                   |               | (Serialization, 8231422)
|
2022-10-30T02:36:10.2906873Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
2604  |
2022-10-30T02:36:10.2907703Z +                   +------------------+
+                   +---------------+-----------------------------------
---+
2022-10-30T02:36:10.2908572Z |                   | CVE-2020-2803    |
|                   | 8.252.09-r0   | OpenJDK: Incorrect bounds checks
|
2022-10-30T02:36:10.2909281Z |                   |                  |
|                   |               | in NIO Buffers (Libraries, 8234841)
|
2022-10-30T02:36:10.2910066Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
2803  |
2022-10-30T02:36:10.2910881Z +                   +------------------+
+                   +               +-----------------------------------
---+
2022-10-30T02:36:10.2911718Z |                   | CVE-2020-2805    |
|                   |               | OpenJDK: Incorrect type checks
|
2022-10-30T02:36:10.2912290Z |                   |                  |
|                   |               | in MethodType.readObject()
|
2022-10-30T02:36:10.2912814Z |                   |                  |
|                   |               | (Libraries, 8235274)
|
```

```
2022-10-30T02:36:10.2913585Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
2805  |
2022-10-30T02:36:10.2914436Z +-------------------+------------------+
+                   +---------------+-----------------------------------
---+
2022-10-30T02:36:10.2915344Z | openjdk8-jre      | CVE-2020-14583   |
|                   | 8.272.10-r0   | OpenJDK: Bypass of boundary checks
|
2022-10-30T02:36:10.2915950Z |                   |                  |
|                   |               | in nio.Buffer via concurrent
|
2022-10-30T02:36:10.2916483Z |                   |                  |
|                   |               | access (Libraries, 8238920)...
|
2022-10-30T02:36:10.2917257Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
14583 |
2022-10-30T02:36:10.2918072Z +                   +------------------+
+                   +               +-----------------------------------
---+
2022-10-30T02:36:10.2918917Z |                   | CVE-2020-14593   |
|                   |               | OpenJDK: Incomplete bounds checks
in  |
2022-10-30T02:36:10.2919509Z |                   |                  |
|                   |               | Affine Transformations (2D,
8240119)  |
2022-10-30T02:36:10.2920295Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
14593 |
2022-10-30T02:36:10.2921120Z +                   +------------------+
+                   +---------------+-----------------------------------
---+
2022-10-30T02:36:10.2921984Z |                   | CVE-2020-2604    |
|                   | 8.242.08-r0   | OpenJDK: Serialization filter
|
2022-10-30T02:36:10.2922570Z |                   |                  |
|                   |               | changes via jdk.serialFilter
|
2022-10-30T02:36:10.2923309Z |                   |                  |
|                   |               | property modification
|
2022-10-30T02:36:10.2923985Z |                   |                  |
|                   |               | (Serialization, 8231422)
|
2022-10-30T02:36:10.2924791Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
2604  |
2022-10-30T02:36:10.2925617Z +                   +------------------+
+                   +---------------+-----------------------------------
---+
2022-10-30T02:36:10.2926485Z |                   | CVE-2020-2803    |
|                   | 8.252.09-r0   | OpenJDK: Incorrect bounds checks
|
2022-10-30T02:36:10.2927087Z |                   |                  |
|                   |               | in NIO Buffers (Libraries, 8234841)
|
```

```
2022-10-30T02:36:10.2927871Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
2803  |
2022-10-30T02:36:10.2928810Z +                   +------------------+
+                   +               +-----------------------------------
---+
2022-10-30T02:36:10.2929647Z |                   | CVE-2020-2805    |
|                   |               | OpenJDK: Incorrect type checks
|
2022-10-30T02:36:10.2930223Z |                   |                  |
|                   |               | in MethodType.readObject()
|
2022-10-30T02:36:10.2930748Z |                   |                  |
|                   |               | (Libraries, 8235274)
|
2022-10-30T02:36:10.2931508Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
2805  |
2022-10-30T02:36:10.2932359Z +-------------------+------------------+
+                   +---------------+-----------------------------------
---+
2022-10-30T02:36:10.2933284Z | openjdk8-jre-base | CVE-2020-14583   |
|                   | 8.272.10-r0   | OpenJDK: Bypass of boundary checks
|
2022-10-30T02:36:10.2933904Z |                   |                  |
|                   |               | in nio.Buffer via concurrent
|
2022-10-30T02:36:10.2934438Z |                   |                  |
|                   |               | access (Libraries, 8238920)...
|
2022-10-30T02:36:10.2935209Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
14583 |
2022-10-30T02:36:10.2936024Z +                   +------------------+
+                   +               +-----------------------------------
---+
2022-10-30T02:36:10.2936862Z |                   | CVE-2020-14593   |
|                   |               | OpenJDK: Incomplete bounds checks
in  |
2022-10-30T02:36:10.2937451Z |                   |                  |
|                   |               | Affine Transformations (2D,
8240119)  |
2022-10-30T02:36:10.2938242Z |                   |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
14593 |
2022-10-30T02:36:10.2939066Z +                   +------------------+
+                   +---------------+-----------------------------------
---+
2022-10-30T02:36:10.2939926Z |                   | CVE-2020-2604    |
|                   | 8.242.08-r0   | OpenJDK: Serialization filter
|
2022-10-30T02:36:10.2940512Z |                   |                  |
|                   |               | changes via jdk.serialFilter
|
2022-10-30T02:36:10.2941035Z |                   |                  |
|                   |               | property modification
|
```

```
2022-10-30T02:36:10.2941556Z |                    |                  |
|                    |               | (Serialization, 8231422)
|
2022-10-30T02:36:10.2942434Z |                    |                  |
|                    |               | -->avd.aquasec.com/nvd/cve-2020-
2604  |
2022-10-30T02:36:10.2943269Z +                    +------------------+
+                    +---------------+-----------------------------------
---+
2022-10-30T02:36:10.2944136Z |                    | CVE-2020-2803    |
|                    | 8.252.09-r0   | OpenJDK: Incorrect bounds checks
|
2022-10-30T02:36:10.2944724Z |                    |                  |
|                    |               | in NIO Buffers (Libraries, 8234841)
|
2022-10-30T02:36:10.2945503Z |                    |                  |
|                    |               | -->avd.aquasec.com/nvd/cve-2020-
2803  |
2022-10-30T02:36:10.2946315Z +                    +------------------+
+                    +               +-----------------------------------
---+
2022-10-30T02:36:10.2947146Z |                    | CVE-2020-2805    |
|                    |               | OpenJDK: Incorrect type checks
|
2022-10-30T02:36:10.2947833Z |                    |                  |
|                    |               | in MethodType.readObject()
|
2022-10-30T02:36:10.2948361Z |                    |                  |
|                    |               | (Libraries, 8235274)
|
2022-10-30T02:36:10.2949128Z |                    |                  |
|                    |               | -->avd.aquasec.com/nvd/cve-2020-
2805  |
2022-10-30T02:36:10.2949987Z +--------------------+------------------+
+                    +---------------+-----------------------------------
---+
2022-10-30T02:36:10.2950910Z | openjdk8-jre-lib   | CVE-2020-14583   |
|                    | 8.272.10-r0   | OpenJDK: Bypass of boundary checks
|
2022-10-30T02:36:10.2951529Z |                    |                  |
|                    |               | in nio.Buffer via concurrent
|
2022-10-30T02:36:10.2952074Z |                    |                  |
|                    |               | access (Libraries, 8238920)...
|
2022-10-30T02:36:10.2952846Z |                    |                  |
|                    |               | -->avd.aquasec.com/nvd/cve-2020-
14583 |
2022-10-30T02:36:10.2953662Z +                    +------------------+
+                    +               +-----------------------------------
---+
2022-10-30T02:36:10.2954497Z |                    | CVE-2020-14593   |
|                    |               | OpenJDK: Incomplete bounds checks
in  |
2022-10-30T02:36:10.2955087Z |                    |                  |
|                    |               | Affine Transformations (2D,
8240119)  |
```

```
2022-10-30T02:36:10.2955871Z |                    |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
14593 |
2022-10-30T02:36:10.2956702Z +                    +------------------+
+                   +---------------+-----------------------------------
---+
2022-10-30T02:36:10.2957580Z |                    | CVE-2020-2604    |
|                   | 8.242.08-r0   | OpenJDK: Serialization filter
|
2022-10-30T02:36:10.2958168Z |                    |                  |
|                   |               | changes via jdk.serialFilter
|
2022-10-30T02:36:10.2958695Z |                    |                  |
|                   |               | property modification
|
2022-10-30T02:36:10.2959216Z |                    |                  |
|                   |               | (Serialization, 8231422)
|
2022-10-30T02:36:10.2959988Z |                    |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
2604  |
2022-10-30T02:36:10.2960814Z +                    +------------------+
+                   +---------------+-----------------------------------
---+
2022-10-30T02:36:10.2961793Z |                    | CVE-2020-2803    |
|                   | 8.252.09-r0   | OpenJDK: Incorrect bounds checks
|
2022-10-30T02:36:10.2962398Z |                    |                  |
|                   |               | in NIO Buffers (Libraries, 8234841)
|
2022-10-30T02:36:10.2964272Z |                    |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
2803  |
2022-10-30T02:36:10.2965138Z +                    +------------------+
+                   +               +-----------------------------------
---+
2022-10-30T02:36:10.2965972Z |                    | CVE-2020-2805    |
|                   |               | OpenJDK: Incorrect type checks
|
2022-10-30T02:36:10.2966541Z |                    |                  |
|                   |               | in MethodType.readObject()
|
2022-10-30T02:36:10.2967065Z |                    |                  |
|                   |               | (Libraries, 8235274)
|
2022-10-30T02:36:10.2967967Z |                    |                  |
|                   |               | -->avd.aquasec.com/nvd/cve-2020-
2805  |
2022-10-30T02:36:10.2968852Z +-------------------+------------------+----
------+-------------------+---------------+-----------------------------
---------+
2022-10-30T02:36:10.2969816Z | sqlite-libs       | CVE-2019-8457    |
CRITICAL | 3.26.0-r3         | 3.28.0-r0     | sqlite: heap out-of-bound
|
2022-10-30T02:36:10.2970445Z |                    |                  |
|                   |               | read in function rtreenode()
|
```

```
2022-10-30T02:36:10.2971222Z |                   |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2019-
8457  |
2022-10-30T02:36:10.2972062Z +                   +------------------+----
------+                  +--------------+------------------------------
---------+
2022-10-30T02:36:10.2972939Z |                   | CVE-2019-19244   |
HIGH     |                  | 3.28.0-r2    | sqlite: allows a crash
|
2022-10-30T02:36:10.2973732Z |                   |                  |
|                   |              | if a sub-select uses both
|
2022-10-30T02:36:10.2974268Z |                   |                  |
|                   |              | DISTINCT and window...
|
2022-10-30T02:36:10.2975028Z |                   |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2019-
19244 |
2022-10-30T02:36:10.2975852Z +                   +------------------+
+                  +--------------+-----------------------------------
---+
2022-10-30T02:36:10.2976701Z |                   | CVE-2019-5018    |
|                   | 3.28.0-r0    | sqlite: Use-after-free in
|
2022-10-30T02:36:10.2977273Z |                   |                  |
|                   |              | window function leading
|
2022-10-30T02:36:10.2977799Z |                   |                  |
|                   |              | to remote code execution
|
2022-10-30T02:36:10.2978564Z |                   |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2019-
5018  |
2022-10-30T02:36:10.2979393Z +                   +------------------+
+                  +--------------+-----------------------------------
---+
2022-10-30T02:36:10.2980264Z |                   | CVE-2020-11655   |
|                   | 3.28.0-r3    | sqlite: malformed window-function
|
2022-10-30T02:36:10.2980843Z |                   |                  |
|                   |              | query leads to DoS
|
2022-10-30T02:36:10.2981602Z |                   |                  |
|                   |              | -->avd.aquasec.com/nvd/cve-2020-
11655 |
2022-10-30T02:36:10.2982613Z +-------------------+------------------+----
------+-------------------+--------------+------------------------------
---------+
2022-10-30T02:36:10.2983716Z 2022-10-30T02:36:10.269Z  [34mINFO [0m
       Table result includes only package filenames. Use '--format json'
option to get the full path to the package file.
2022-10-30T02:36:10.2984234Z
2022-10-30T02:36:10.2984529Z Java (jar)
2022-10-30T02:36:10.2984895Z ==========
2022-10-30T02:36:10.2985301Z Total: 14 (HIGH: 11, CRITICAL: 3)
2022-10-30T02:36:10.2985546Z
```

```
2022-10-30T02:36:10.2986369Z +----------------------------------------
-------+------------------+----------+-------------------+---------------
-----------------+----------------------------------------+
2022-10-30T02:36:10.2987187Z |                      LIBRARY
| VULNERABILITY ID | SEVERITY | INSTALLED VERSION |         FIXED VERSION
|                TITLE                |
2022-10-30T02:36:10.2988240Z +----------------------------------------
-------+------------------+----------+-------------------+---------------
-----------------+----------------------------------------+
2022-10-30T02:36:10.2989611Z | com.fasterxml.jackson.core:jackson-
databind      | CVE-2020-36518   | HIGH     | 2.11.0            |
2.12.6.1, 2.13.2.1            | jackson-databind: denial of service   |
2022-10-30T02:36:10.2990388Z | (app.jar)
|                  |          |                   |
| via a large depth of nested objects   |
2022-10-30T02:36:10.2991261Z |
|                  |          |                   |
| -->avd.aquasec.com/nvd/cve-2020-36518 |
2022-10-30T02:36:10.2992199Z +
+------------------+          +                   +----------------------
----------+----------------------------------------+
2022-10-30T02:36:10.2993170Z |
| CVE-2022-42003   |          |                   | 2.13.4.1
| jackson-databind: deep                |
2022-10-30T02:36:10.2993800Z |
|                  |          |                   |
| wrapper array nesting wrt             |
2022-10-30T02:36:10.2994384Z |
|                  |          |                   |
| UNWRAP_SINGLE_VALUE_ARRAYS            |
2022-10-30T02:36:10.2995242Z |
|                  |          |                   |
| -->avd.aquasec.com/nvd/cve-2022-42003 |
2022-10-30T02:36:10.2996181Z +
+------------------+          +                   +----------------------
----------+----------------------------------------+
2022-10-30T02:36:10.2997139Z |
| CVE-2022-42004   |          |                   | 2.13.4
| jackson-databind: use                 |
2022-10-30T02:36:10.2997757Z |
|                  |          |                   |
| of deeply nested arrays               |
2022-10-30T02:36:10.2998607Z |
|                  |          |                   |
| -->avd.aquasec.com/nvd/cve-2022-42004 |
2022-10-30T02:36:10.2999623Z +----------------------------------------
-------+------------------+          +-------------------+---------------
-----------------+----------------------------------------+
2022-10-30T02:36:10.3000758Z | io.fabric8:kubernetes-client
| CVE-2021-20218   |          | 4.4.1             | 4.7.2, 4.11.2,
4.13.2, 5.0.2   | fabric8-kubernetes-client:            |
2022-10-30T02:36:10.3001503Z | (app.jar)
|                  |          |                   |
| vulnerable to a path traversal        |
2022-10-30T02:36:10.3002190Z |
|                  |          |                   |
| leading to integrity and              |
```

```
2022-10-30T02:36:10.3002762Z |
|                  |          |                    |
| availability compromise...            |
2022-10-30T02:36:10.3003809Z |
|                  |          |                    |
| -->avd.aquasec.com/nvd/cve-2021-20218 |
2022-10-30T02:36:10.3004855Z +----------------------------------------
-------+------------------+          +--------------------+---------------
-----------------+---------------------------------------+
2022-10-30T02:36:10.3006012Z | org.apache.tomcat.embed:tomcat-embed-core
| CVE-2020-13934   |          | 9.0.35             | 8.5.57, 9.0.37
| tomcat: OutOfMemoryException          |
2022-10-30T02:36:10.3006866Z | (app.jar)
|                  |          |                    |
| caused by HTTP/2 connection           |
2022-10-30T02:36:10.3007451Z |
|                  |          |                    |
| leak could lead to DoS                |
2022-10-30T02:36:10.3008306Z |
|                  |          |                    |
| -->avd.aquasec.com/nvd/cve-2020-13934 |
2022-10-30T02:36:10.3009241Z +
+------------------+          +                    +----------------------
----------+---------------------------------------+
2022-10-30T02:36:10.3010236Z |
| CVE-2020-17527   |          |                    | 8.5.60, 9.0.40,
10.0.2         | tomcat: HTTP/2 request header mix-up  |
2022-10-30T02:36:10.3011175Z |
|                  |          |                    |
| -->avd.aquasec.com/nvd/cve-2020-17527 |
2022-10-30T02:36:10.3012119Z +
+------------------+          +                    +----------------------
----------+---------------------------------------+
2022-10-30T02:36:10.3013109Z |
| CVE-2021-25122   |          |                    | 8.5.62, 9.0.42,
10.0.2         | tomcat: Request mix-up with h2c       |
2022-10-30T02:36:10.3014031Z |
|                  |          |                    |
| -->avd.aquasec.com/nvd/cve-2021-25122 |
2022-10-30T02:36:10.3014969Z +
+------------------+          +                    +----------------------
----------+---------------------------------------+
2022-10-30T02:36:10.3015962Z |
| CVE-2021-25329   |          |                    | 7.0.107, 8.5.61,
9.0.41        | tomcat: Incomplete fix                |
2022-10-30T02:36:10.3016863Z |
|                  |          |                    |
| for CVE-2020-9484 (RCE                |
2022-10-30T02:36:10.3017445Z |
|                  |          |                    |
| via session persistence)              |
2022-10-30T02:36:10.3018292Z |
|                  |          |                    |
| -->avd.aquasec.com/nvd/cve-2021-25329 |
2022-10-30T02:36:10.3019292Z +----------------------------------------
-------+------------------+          +                    +--------------
-----------------+---------------------------------------+
```

```
2022-10-30T02:36:10.3020541Z | org.apache.tomcat.embed:tomcat-embed-
websocket   | CVE-2020-13935   |          |                   | 7.0.105,
8.5.57, 9.0.37,       | tomcat: multiple requests             |
2022-10-30T02:36:10.3021300Z | (app.jar)
|                  |          |                   | 10.0.2
| with invalid payload length           |
2022-10-30T02:36:10.3021906Z |
|                  |          |                   |
| in a WebSocket frame could...         |
2022-10-30T02:36:10.3022758Z |
|                  |          |                   |
| -->avd.aquasec.com/nvd/cve-2020-13935 |
2022-10-30T02:36:10.3023789Z +-----------------------------------------
-------+-----------------+----------+-------------------+---------------
-----------------+-----------------------------------------+
2022-10-30T02:36:10.3025073Z | org.springframework.boot:spring-boot-
starter-web | CVE-2022-22965   | CRITICAL | 2.3.0.RELEASE     | 2.6.6,
2.5.12                  | spring-framework: RCE via             |
2022-10-30T02:36:10.3025833Z | (app.jar)
|                  |          |                   |
| Data Binding on JDK 9+                |
2022-10-30T02:36:10.3026695Z |
|                  |          |                   |
| -->avd.aquasec.com/nvd/cve-2022-22965 |
2022-10-30T02:36:10.3027643Z +-----------------------------------------
-------+                 +          +-------------------+---------------
-----------------+                                       +
2022-10-30T02:36:10.3028649Z | org.springframework:spring-beans
|                  |          | 5.2.6.RELEASE     | 5.3.18, 5.2.20
|                                     |
2022-10-30T02:36:10.3029294Z | (app.jar)
|                  |          |                   |
|                                     |
2022-10-30T02:36:10.3029823Z |
|                  |          |                   |
|                                     |
2022-10-30T02:36:10.3030766Z +-----------------------------------------
-------+-----------------+----------+                   +---------------
-----------------+-----------------------------------------+
2022-10-30T02:36:10.3031871Z | org.springframework:spring-core
| CVE-2021-22118   | HIGH     |                   | 5.2.15, 5.3.7
| spring-web: (re)creating the          |
2022-10-30T02:36:10.3032595Z | (app.jar)
|                  |          |                   |
| temporary storage directory           |
2022-10-30T02:36:10.3033197Z |
|                  |          |                   |
| could result in  a privilege...       |
2022-10-30T02:36:10.3034054Z |
|                  |          |                   |
| -->avd.aquasec.com/nvd/cve-2021-22118 |
2022-10-30T02:36:10.3035063Z +-----------------------------------------
-------+-----------------+----------+                   +---------------
-----------------+-----------------------------------------+
2022-10-30T02:36:10.3036189Z | org.springframework:spring-webmvc
| CVE-2022-22965   | CRITICAL |                   | 5.2.20, 5.3.18
| spring-framework: RCE via             |
```

```
2022-10-30T02:36:10.3036902Z | (app.jar)
|                  |          |                    |
| Data Binding on JDK 9+               |
2022-10-30T02:36:10.3037872Z |
|                  |          |                    |
| -->avd.aquasec.com/nvd/cve-2022-22965 |
2022-10-30T02:36:10.3038904Z +-----------------------------------------
-------+------------------+----------+-------------------+---------------
-----------------+---------------------------------------+
2022-10-30T02:36:10.3040014Z | org.yaml:snakeyaml (app.jar)
| CVE-2022-25857   | HIGH     |              1.26 |
1.31 | snakeyaml: Denial of Service          |
2022-10-30T02:36:10.3040694Z |
|                  |          |                    |
| due to missing nested depth           |
2022-10-30T02:36:10.3041273Z |
|                  |          |                    |
| limitation for collections...         |
2022-10-30T02:36:10.3042224Z |
|                  |          |                    |
| -->avd.aquasec.com/nvd/cve-2022-25857 |
2022-10-30T02:36:10.3043365Z +-----------------------------------------
-------+------------------+----------+-------------------+---------------
-----------------+---------------------------------------+
2022-10-30T02:36:10.3074215Z ##[error]Bash exited with code '1'.
2022-10-30T02:36:10.3090869Z ##[section]Finishing: Ejecutando análisis de
imagen con Trivy
```