

Registry 2.6.2

```
Activities Terminal Nov 1 01:30 osboxes@osboxes: /tmp
osboxes@osboxes:/tmp$ trivy image registry:2.6.2
2022-11-01T01:27:42.243-0400 INFO Detected OS: alpine
2022-11-01T01:27:42.244-0400 INFO Detecting Alpine vulnerabilities...
2022-11-01T01:27:42.275-0400 INFO Number of language-specific files: 0
2022-11-01T01:27:42.276-0400 WARN This OS version is no longer supported by the distribution: alpine 3.8.5
2022-11-01T01:27:42.276-0400 WARN The vulnerability detection may be insufficient because security updates are not provided

registry:2.6.2 (alpine 3.8.5)
=====
Total: 2 (UNKNOWN: 0, LOW: 0, MEDIUM: 2, HIGH: 0, CRITICAL: 0)

+-----+-----+-----+-----+-----+-----+
| LIBRARY | VULNERABILITY ID | SEVERITY | INSTALLED VERSION | FIXED VERSION | TITLE |
+-----+-----+-----+-----+-----+-----+
| apache2-utils | CVE-2020-1927 | MEDIUM | 2.4.41-r0 | 2.4.43-r0 | httpd: mod_rewrite configurations vulnerable to open redirect -->avd.aquasec.com/nvd/cve-2020-1927 |
+-----+-----+-----+-----+-----+-----+
| | CVE-2020-1934 | | | | httpd: mod_proxy_ftp use of uninitialized value -->avd.aquasec.com/nvd/cve-2020-1934 |
+-----+-----+-----+-----+-----+-----+

osboxes@osboxes:/tmp$
```

Registry 2.7.1

```
Activities Terminal Nov 1 01:34 osboxes@osboxes: /tmp
osboxes@osboxes:/tmp$ trivy image registry:2.7.1
2022-11-01T01:31:56.674-0400 INFO Detected OS: alpine
2022-11-01T01:31:56.675-0400 INFO Detecting Alpine vulnerabilities...
2022-11-01T01:31:56.727-0400 INFO Number of language-specific files: 0
2022-11-01T01:31:56.727-0400 WARN This OS version is no longer supported by the distribution: alpine 3.11.13
2022-11-01T01:31:56.727-0400 WARN The vulnerability detection may be insufficient because security updates are not provided

registry:2.7.1 (alpine 3.11.13)
=====
Total: 1 (UNKNOWN: 0, LOW: 0, MEDIUM: 0, HIGH: 0, CRITICAL: 1)

+-----+-----+-----+-----+-----+-----+
| LIBRARY | VULNERABILITY ID | SEVERITY | INSTALLED VERSION | FIXED VERSION | TITLE |
+-----+-----+-----+-----+-----+-----+
| zlib | CVE-2022-37434 | CRITICAL | 1.2.11-r3 | 1.2.11-r4 | zlib: heap-based buffer over-read and overflow in inflate() in inflate.c via a... -->avd.aquasec.com/nvd/cve-2022-37434 |
+-----+-----+-----+-----+-----+-----+

osboxes@osboxes:/tmp$
```

Registry 2.8.0-beta.1

```
osboxes@osboxes:/tmp$ trivy image registry:2.8.0-beta.1
2022-11-01T01:37:05.203-0400 INFO Detected OS: alpine
2022-11-01T01:37:05.212-0400 WARN This OS version is not on the EOL list: alpine 3.15
2022-11-01T01:37:05.212-0400 INFO Detecting Alpine vulnerabilities...
2022-11-01T01:37:05.292-0400 INFO Number of language-specific files: 0
2022-11-01T01:37:05.292-0400 WARN This OS version is no longer supported by the distribution: alpine 3.15.0
2022-11-01T01:37:05.292-0400 WARN The vulnerability detection may be insufficient because security updates are not provided

registry:2.8.0-beta.1 (alpine 3.15.0)
=====
Total: 9 (UNKNOWN: 0, LOW: 0, MEDIUM: 2, HIGH: 6, CRITICAL: 1)

+-----+-----+-----+-----+-----+-----+
| LIBRARY | VULNERABILITY ID | SEVERITY | INSTALLED VERSION | FIXED VERSION | TITLE |
+-----+-----+-----+-----+-----+-----+
| busybox | CVE-2022-28391 | HIGH | 1.34.1-r3 | 1.34.1-r5 | busybox: remote attackers may execute arbitrary code if netstat is used -->avd.aquasec.com/nvd/cve-2022-28391 |
+-----+-----+-----+-----+-----+-----+
| libcrypto1.1 | CVE-2022-0778 | | 1.1.1l-r7 | 1.1.1n-r0 | openssl: Infinite loop in BN_mod_sqrt() reachable when parsing certificates -->avd.aquasec.com/nvd/cve-2022-0778 |
+-----+-----+-----+-----+-----+-----+
| | CVE-2022-2097 | MEDIUM | | 1.1.1q-r0 | openssl: AES OCB fails to encrypt some bytes -->avd.aquasec.com/nvd/cve-2022-2097 |
+-----+-----+-----+-----+-----+-----+
| libretls | CVE-2022-0778 | HIGH | 3.3.4-r2 | 3.3.4-r3 | openssl: Infinite loop in BN_mod_sqrt() reachable when parsing certificates -->avd.aquasec.com/nvd/cve-2022-0778 |
+-----+-----+-----+-----+-----+-----+
| libssl1.1 | | | 1.1.1l-r7 | 1.1.1n-r0 | |
+-----+-----+-----+-----+-----+-----+
```

```
osboxes@osboxes:/tmp$ trivy image registry:2.8.0-beta.1
2022-11-01T01:37:05.203-0400 INFO Detected OS: alpine
2022-11-01T01:37:05.212-0400 WARN This OS version is not on the EOL list: alpine 3.15
2022-11-01T01:37:05.212-0400 INFO Detecting Alpine vulnerabilities...
2022-11-01T01:37:05.292-0400 INFO Number of language-specific files: 0
2022-11-01T01:37:05.292-0400 WARN This OS version is no longer supported by the distribution: alpine 3.15.0
2022-11-01T01:37:05.292-0400 WARN The vulnerability detection may be insufficient because security updates are not provided

registry:2.8.0-beta.1 (alpine 3.15.0)
=====
Total: 9 (UNKNOWN: 0, LOW: 0, MEDIUM: 2, HIGH: 6, CRITICAL: 1)

+-----+-----+-----+-----+-----+-----+
| LIBRARY | VULNERABILITY ID | SEVERITY | INSTALLED VERSION | FIXED VERSION | TITLE |
+-----+-----+-----+-----+-----+-----+
| busybox | CVE-2022-28391 | HIGH | 1.34.1-r3 | 1.34.1-r5 | busybox: remote attackers may execute arbitrary code if netstat is used -->avd.aquasec.com/nvd/cve-2022-28391 |
+-----+-----+-----+-----+-----+-----+
| libcrypto1.1 | CVE-2022-0778 | | 1.1.1l-r7 | 1.1.1n-r0 | openssl: Infinite loop in BN_mod_sqrt() reachable when parsing certificates -->avd.aquasec.com/nvd/cve-2022-0778 |
+-----+-----+-----+-----+-----+-----+
| | CVE-2022-2097 | MEDIUM | | 1.1.1q-r0 | openssl: AES OCB fails to encrypt some bytes -->avd.aquasec.com/nvd/cve-2022-2097 |
+-----+-----+-----+-----+-----+-----+
| libretls | CVE-2022-0778 | HIGH | 3.3.4-r2 | 3.3.4-r3 | openssl: Infinite loop in BN_mod_sqrt() reachable when parsing certificates -->avd.aquasec.com/nvd/cve-2022-0778 |
+-----+-----+-----+-----+-----+-----+
| libssl1.1 | | | 1.1.1l-r7 | 1.1.1n-r0 | |
+-----+-----+-----+-----+-----+-----+
| ssl_client | CVE-2022-28391 | HIGH | 1.34.1-r3 | 1.34.1-r5 | busybox: remote attackers may execute arbitrary code if netstat is used -->avd.aquasec.com/nvd/cve-2022-28391 |
+-----+-----+-----+-----+-----+-----+
| zlib | CVE-2022-37434 | CRITICAL | 1.2.11-r3 | 1.2.12-r2 | zlib: heap-based buffer over-read and overflow in inflate() in inflate.c via a... -->avd.aquasec.com/nvd/cve-2022-37434 |
+-----+-----+-----+-----+-----+-----+
| | CVE-2018-25032 | HIGH | | 1.2.12-r0 | zlib: A flaw found in zlib when compressing (not decompressing) certain inputs... -->avd.aquasec.com/nvd/cve-2018-25032 |
+-----+-----+-----+-----+-----+-----+
```