myproject\_web (debian 9.13)

===========================

Total: 70 (UNKNOWN: 1, LOW: 34, MEDIUM: 4, HIGH: 28, CRITICAL: 3)

┌───────────────┬──────────────────┬──────────┬───────────────────────┬────────────────┬──────────────────────────────────────────────────────────────┐

│ Library │ Vulnerability │ Severity │ Installed Version │ Fixed Version │ Title │

├───────────────┼──────────────────┼──────────┼───────────────────────┼────────────────┼──────────────────────────────────────────────────────────────┤

│ bsdutils │ CVE-2016-2779 │ HIGH │ 1:2.29.2-1+deb9u1 │ │ util-linux: runuser tty hijack via TIOCSTI ioctl │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2016-2779 │

│ ├──────────────────┼──────────┤ ├────────────────┼──────────────────────────────────────────────────────────────┤

│ │ CVE-2021-37600 │ LOW │ │ │ util-linux: integer overflow can lead to buffer overflow in │

│ │ │ │ │ │ get\_sem\_elements() in sys-utils/ipcutils.c... │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2021-37600 │

├───────────────┼──────────────────┤ ├───────────────────────┼────────────────┼──────────────────────────────────────────────────────────────┤

│ coreutils │ CVE-2016-2781 │ │ 8.26-3 │ │ coreutils: Non-privileged session can escape to the parent │

│ │ │ │ │ │ session in chroot │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2016-2781 │

├───────────────┼──────────────────┼──────────┼───────────────────────┼────────────────┼──────────────────────────────────────────────────────────────┤

│ dpkg │ CVE-2022-1664 │ CRITICAL │ 1.18.25 │ 1.18.26 │ Dpkg::Source::Archive in dpkg, the Debian package management │

│ │ │ │ │ │ system, b ... │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2022-1664 │

├───────────────┼──────────────────┼──────────┼───────────────────────┼────────────────┼──────────────────────────────────────────────────────────────┤

│ e2fslibs │ CVE-2022-1304 │ HIGH │ 1.43.4-2+deb9u2 │ │ e2fsprogs: out-of-bounds read/write via crafted filesystem │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2022-1304 │

├───────────────┤ │ │ ├────────────────┤ │

│ e2fsprogs │ │ │ │ │ │

│ │ │ │ │ │ │

├───────────────┼──────────────────┤ ├───────────────────────┼────────────────┼──────────────────────────────────────────────────────────────┤

│ gcc-6-base │ CVE-2018-12886 │ │ 6.3.0-18+deb9u1 │ │ gcc: spilling of stack protection address in cfgexpand.c and │

│ │ │ │ │ │ function.c leads to... │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2018-12886 │

├───────────────┼──────────────────┤ ├───────────────────────┼────────────────┼──────────────────────────────────────────────────────────────┤

│ gpgv │ CVE-2018-1000858 │ │ 2.1.18-8~deb9u4 │ │ gnupg2: Cross site request forgery in dirmngr resulting in │

│ │ │ │ │ │ an information disclosure... │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2018-1000858 │

│ ├──────────────────┼──────────┤ ├────────────────┼──────────────────────────────────────────────────────────────┤

│ │ CVE-2018-9234 │ LOW │ │ │ GnuPG: Unenforced configuration allows for apparently valid │

│ │ │ │ │ │ certifications actually signed by signing... │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2018-9234 │

│ ├──────────────────┤ │ ├────────────────┼──────────────────────────────────────────────────────────────┤

│ │ CVE-2019-14855 │ │ │ │ gnupg2: OpenPGP Key Certification Forgeries with SHA-1 │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2019-14855 │

├───────────────┼──────────────────┼──────────┼───────────────────────┼────────────────┼──────────────────────────────────────────────────────────────┤

│ libblkid1 │ CVE-2016-2779 │ HIGH │ 2.29.2-1+deb9u1 │ │ util-linux: runuser tty hijack via TIOCSTI ioctl │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2016-2779 │

│ ├──────────────────┼──────────┤ ├────────────────┼──────────────────────────────────────────────────────────────┤

│ │ CVE-2021-37600 │ LOW │ │ │ util-linux: integer overflow can lead to buffer overflow in │

│ │ │ │ │ │ get\_sem\_elements() in sys-utils/ipcutils.c... │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2021-37600 │

├───────────────┼──────────────────┼──────────┼───────────────────────┼────────────────┼──────────────────────────────────────────────────────────────┤

│ libbz2-1.0 │ CVE-2019-12900 │ CRITICAL │ 1.0.6-8.1 │ │ bzip2: out-of-bounds write in function BZ2\_decompress │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2019-12900 │

├───────────────┼──────────────────┼──────────┼───────────────────────┼────────────────┼──────────────────────────────────────────────────────────────┤

│ libcomerr2 │ CVE-2022-1304 │ HIGH │ 1.43.4-2+deb9u2 │ │ e2fsprogs: out-of-bounds read/write via crafted filesystem │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2022-1304 │

├───────────────┼──────────────────┼──────────┼───────────────────────┼────────────────┼──────────────────────────────────────────────────────────────┤

│ libdb5.3 │ CVE-2019-8457 │ CRITICAL │ 5.3.28-12+deb9u1 │ │ sqlite: heap out-of-bound read in function rtreenode() │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2019-8457 │

├───────────────┼──────────────────┼──────────┼───────────────────────┼────────────────┼──────────────────────────────────────────────────────────────┤

│ libfdisk1 │ CVE-2016-2779 │ HIGH │ 2.29.2-1+deb9u1 │ │ util-linux: runuser tty hijack via TIOCSTI ioctl │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2016-2779 │

│ ├──────────────────┼──────────┤ ├────────────────┼──────────────────────────────────────────────────────────────┤

│ │ CVE-2021-37600 │ LOW │ │ │ util-linux: integer overflow can lead to buffer overflow in │

│ │ │ │ │ │ get\_sem\_elements() in sys-utils/ipcutils.c... │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2021-37600 │

├───────────────┼──────────────────┼──────────┼───────────────────────┼────────────────┼──────────────────────────────────────────────────────────────┤

│ libgcc1 │ CVE-2018-12886 │ HIGH │ 1:6.3.0-18+deb9u1 │ │ gcc: spilling of stack protection address in cfgexpand.c and │

│ │ │ │ │ │ function.c leads to... │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2018-12886 │

├───────────────┼──────────────────┤ ├───────────────────────┼────────────────┼──────────────────────────────────────────────────────────────┤

│ libgcrypt20 │ CVE-2021-33560 │ │ 1.7.6-2+deb9u4 │ │ libgcrypt: mishandles ElGamal encryption because it lacks │

│ │ │ │ │ │ exponent blinding to address a... │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2021-33560 │

│ ├──────────────────┼──────────┤ ├────────────────┼──────────────────────────────────────────────────────────────┤

│ │ CVE-2019-13627 │ MEDIUM │ │ │ libgcrypt: ECDSA timing attack allowing private key leak │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2019-13627 │

├───────────────┼──────────────────┼──────────┼───────────────────────┼────────────────┼──────────────────────────────────────────────────────────────┤

│ liblz4-1 │ CVE-2019-17543 │ LOW │ 0.0~r131-2+deb9u1 │ │ lz4: heap-based buffer overflow in LZ4\_write32 │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2019-17543 │

├───────────────┼──────────────────┼──────────┼───────────────────────┼────────────────┼──────────────────────────────────────────────────────────────┤

│ libmount1 │ CVE-2016-2779 │ HIGH │ 2.29.2-1+deb9u1 │ │ util-linux: runuser tty hijack via TIOCSTI ioctl │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2016-2779 │

│ ├──────────────────┼──────────┤ ├────────────────┼──────────────────────────────────────────────────────────────┤

│ │ CVE-2021-37600 │ LOW │ │ │ util-linux: integer overflow can lead to buffer overflow in │

│ │ │ │ │ │ get\_sem\_elements() in sys-utils/ipcutils.c... │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2021-37600 │

├───────────────┼──────────────────┼──────────┼───────────────────────┼────────────────┼──────────────────────────────────────────────────────────────┤

│ libncursesw5 │ CVE-2022-29458 │ HIGH │ 6.0+20161126-1+deb9u2 │ │ ncurses: segfaulting OOB read │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2022-29458 │

│ ├──────────────────┼──────────┤ ├────────────────┼──────────────────────────────────────────────────────────────┤

│ │ CVE-2018-19211 │ LOW │ │ │ ncurses: Null pointer dereference at function │

│ │ │ │ │ │ \_nc\_parse\_entry in parse\_entry.c │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2018-19211 │

│ ├──────────────────┤ │ ├────────────────┼──────────────────────────────────────────────────────────────┤

│ │ CVE-2019-17594 │ │ │ │ ncurses: heap-based buffer overflow in the \_nc\_find\_entry │

│ │ │ │ │ │ function in tinfo/comp\_hash.c │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2019-17594 │

│ ├──────────────────┤ │ ├────────────────┼──────────────────────────────────────────────────────────────┤

│ │ CVE-2019-17595 │ │ │ │ ncurses: heap-based buffer overflow in the fmt\_entry │

│ │ │ │ │ │ function in tinfo/comp\_hash.c │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2019-17595 │

├───────────────┼──────────────────┼──────────┼───────────────────────┼────────────────┼──────────────────────────────────────────────────────────────┤

│ libpcre3 │ CVE-2020-14155 │ MEDIUM │ 2:8.39-3 │ │ pcre: Integer overflow when parsing callout numeric │

│ │ │ │ │ │ arguments │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2020-14155 │

├───────────────┼──────────────────┼──────────┼───────────────────────┼────────────────┼──────────────────────────────────────────────────────────────┤

│ libsepol1 │ CVE-2021-36084 │ LOW │ 2.6-2 │ │ libsepol: use-after-free in \_\_cil\_verify\_classperms() │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2021-36084 │

│ ├──────────────────┤ │ ├────────────────┼──────────────────────────────────────────────────────────────┤

│ │ CVE-2021-36085 │ │ │ │ libsepol: use-after-free in \_\_cil\_verify\_classperms() │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2021-36085 │

│ ├──────────────────┤ │ ├────────────────┼──────────────────────────────────────────────────────────────┤

│ │ CVE-2021-36086 │ │ │ │ use-after-free in cil\_reset\_classpermission() │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2021-36086 │

│ ├──────────────────┤ │ ├────────────────┼──────────────────────────────────────────────────────────────┤

│ │ CVE-2021-36087 │ │ │ │ libsepol: heap-based buffer overflow in ebitmap\_match\_any() │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2021-36087 │

├───────────────┼──────────────────┼──────────┼───────────────────────┼────────────────┼──────────────────────────────────────────────────────────────┤

│ libsmartcols1 │ CVE-2016-2779 │ HIGH │ 2.29.2-1+deb9u1 │ │ util-linux: runuser tty hijack via TIOCSTI ioctl │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2016-2779 │

│ ├──────────────────┼──────────┤ ├────────────────┼──────────────────────────────────────────────────────────────┤

│ │ CVE-2021-37600 │ LOW │ │ │ util-linux: integer overflow can lead to buffer overflow in │

│ │ │ │ │ │ get\_sem\_elements() in sys-utils/ipcutils.c... │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2021-37600 │

├───────────────┼──────────────────┼──────────┼───────────────────────┼────────────────┼──────────────────────────────────────────────────────────────┤

│ libss2 │ CVE-2022-1304 │ HIGH │ 1.43.4-2+deb9u2 │ │ e2fsprogs: out-of-bounds read/write via crafted filesystem │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2022-1304 │

├───────────────┼──────────────────┤ ├───────────────────────┼────────────────┼──────────────────────────────────────────────────────────────┤

│ libstdc++6 │ CVE-2018-12886 │ │ 6.3.0-18+deb9u1 │ │ gcc: spilling of stack protection address in cfgexpand.c and │

│ │ │ │ │ │ function.c leads to... │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2018-12886 │

├───────────────┼──────────────────┤ ├───────────────────────┼────────────────┼──────────────────────────────────────────────────────────────┤

│ libsystemd0 │ CVE-2019-3843 │ │ 232-25+deb9u13 │ │ systemd: services with DynamicUser can create SUID/SGID │

│ │ │ │ │ │ binaries │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2019-3843 │

│ ├──────────────────┤ │ ├────────────────┼──────────────────────────────────────────────────────────────┤

│ │ CVE-2019-3844 │ │ │ │ systemd: services with DynamicUser can get new privileges │

│ │ │ │ │ │ and create SGID binaries... │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2019-3844 │

│ ├──────────────────┤ │ ├────────────────┼──────────────────────────────────────────────────────────────┤

│ │ CVE-2020-1712 │ │ │ 232-25+deb9u14 │ systemd: use-after-free when asynchronous polkit queries are │

│ │ │ │ │ │ performed │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2020-1712 │

│ ├──────────────────┼──────────┤ ├────────────────┼──────────────────────────────────────────────────────────────┤

│ │ CVE-2021-3997 │ MEDIUM │ │ │ systemd: Uncontrolled recursion in systemd-tmpfiles when │

│ │ │ │ │ │ removing files │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2021-3997 │

│ ├──────────────────┼──────────┤ ├────────────────┼──────────────────────────────────────────────────────────────┤

│ │ CVE-2018-16888 │ LOW │ │ │ systemd: kills privileged process if unprivileged PIDFile │

│ │ │ │ │ │ was tampered │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2018-16888 │

│ ├──────────────────┤ │ ├────────────────┼──────────────────────────────────────────────────────────────┤

│ │ CVE-2018-6954 │ │ │ │ systemd: Mishandled symlinks in systemd-tmpfiles allows │

│ │ │ │ │ │ local users to obtain ownership of... │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2018-6954 │

├───────────────┼──────────────────┼──────────┼───────────────────────┼────────────────┼──────────────────────────────────────────────────────────────┤

│ libtinfo5 │ CVE-2022-29458 │ HIGH │ 6.0+20161126-1+deb9u2 │ │ ncurses: segfaulting OOB read │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2022-29458 │

│ ├──────────────────┼──────────┤ ├────────────────┼──────────────────────────────────────────────────────────────┤

│ │ CVE-2018-19211 │ LOW │ │ │ ncurses: Null pointer dereference at function │

│ │ │ │ │ │ \_nc\_parse\_entry in parse\_entry.c │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2018-19211 │

│ ├──────────────────┤ │ ├────────────────┼──────────────────────────────────────────────────────────────┤

│ │ CVE-2019-17594 │ │ │ │ ncurses: heap-based buffer overflow in the \_nc\_find\_entry │

│ │ │ │ │ │ function in tinfo/comp\_hash.c │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2019-17594 │

│ ├──────────────────┤ │ ├────────────────┼──────────────────────────────────────────────────────────────┤

│ │ CVE-2019-17595 │ │ │ │ ncurses: heap-based buffer overflow in the fmt\_entry │

│ │ │ │ │ │ function in tinfo/comp\_hash.c │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2019-17595 │

├───────────────┼──────────────────┼──────────┼───────────────────────┼────────────────┼──────────────────────────────────────────────────────────────┤

│ libudev1 │ CVE-2019-3843 │ HIGH │ 232-25+deb9u13 │ │ systemd: services with DynamicUser can create SUID/SGID │

│ │ │ │ │ │ binaries │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2019-3843 │

│ ├──────────────────┤ │ ├────────────────┼──────────────────────────────────────────────────────────────┤

│ │ CVE-2019-3844 │ │ │ │ systemd: services with DynamicUser can get new privileges │

│ │ │ │ │ │ and create SGID binaries... │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2019-3844 │

│ ├──────────────────┤ │ ├────────────────┼──────────────────────────────────────────────────────────────┤

│ │ CVE-2020-1712 │ │ │ 232-25+deb9u14 │ systemd: use-after-free when asynchronous polkit queries are │

│ │ │ │ │ │ performed │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2020-1712 │

│ ├──────────────────┼──────────┤ ├────────────────┼──────────────────────────────────────────────────────────────┤

│ │ CVE-2021-3997 │ MEDIUM │ │ │ systemd: Uncontrolled recursion in systemd-tmpfiles when │

│ │ │ │ │ │ removing files │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2021-3997 │

│ ├──────────────────┼──────────┤ ├────────────────┼──────────────────────────────────────────────────────────────┤

│ │ CVE-2018-16888 │ LOW │ │ │ systemd: kills privileged process if unprivileged PIDFile │

│ │ │ │ │ │ was tampered │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2018-16888 │

│ ├──────────────────┤ │ ├────────────────┼──────────────────────────────────────────────────────────────┤

│ │ CVE-2018-6954 │ │ │ │ systemd: Mishandled symlinks in systemd-tmpfiles allows │

│ │ │ │ │ │ local users to obtain ownership of... │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2018-6954 │

├───────────────┼──────────────────┼──────────┼───────────────────────┼────────────────┼──────────────────────────────────────────────────────────────┤

│ libuuid1 │ CVE-2016-2779 │ HIGH │ 2.29.2-1+deb9u1 │ │ util-linux: runuser tty hijack via TIOCSTI ioctl │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2016-2779 │

│ ├──────────────────┼──────────┤ ├────────────────┼──────────────────────────────────────────────────────────────┤

│ │ CVE-2021-37600 │ LOW │ │ │ util-linux: integer overflow can lead to buffer overflow in │

│ │ │ │ │ │ get\_sem\_elements() in sys-utils/ipcutils.c... │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2021-37600 │

├───────────────┼──────────────────┤ ├───────────────────────┼────────────────┼──────────────────────────────────────────────────────────────┤

│ login │ CVE-2018-7169 │ │ 1:4.4-4.1+deb9u1 │ │ shadow-utils: newgidmap allows unprivileged user to drop │

│ │ │ │ │ │ supplementary groups potentially allowing privilege... │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2018-7169 │

├───────────────┼──────────────────┼──────────┼───────────────────────┼────────────────┼──────────────────────────────────────────────────────────────┤

│ mount │ CVE-2016-2779 │ HIGH │ 2.29.2-1+deb9u1 │ │ util-linux: runuser tty hijack via TIOCSTI ioctl │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2016-2779 │

│ ├──────────────────┼──────────┤ ├────────────────┼──────────────────────────────────────────────────────────────┤

│ │ CVE-2021-37600 │ LOW │ │ │ util-linux: integer overflow can lead to buffer overflow in │

│ │ │ │ │ │ get\_sem\_elements() in sys-utils/ipcutils.c... │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2021-37600 │

├───────────────┼──────────────────┼──────────┼───────────────────────┼────────────────┼──────────────────────────────────────────────────────────────┤

│ ncurses-base │ CVE-2022-29458 │ HIGH │ 6.0+20161126-1+deb9u2 │ │ ncurses: segfaulting OOB read │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2022-29458 │

│ ├──────────────────┼──────────┤ ├────────────────┼──────────────────────────────────────────────────────────────┤

│ │ CVE-2018-19211 │ LOW │ │ │ ncurses: Null pointer dereference at function │

│ │ │ │ │ │ \_nc\_parse\_entry in parse\_entry.c │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2018-19211 │

│ ├──────────────────┤ │ ├────────────────┼──────────────────────────────────────────────────────────────┤

│ │ CVE-2019-17594 │ │ │ │ ncurses: heap-based buffer overflow in the \_nc\_find\_entry │

│ │ │ │ │ │ function in tinfo/comp\_hash.c │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2019-17594 │

│ ├──────────────────┤ │ ├────────────────┼──────────────────────────────────────────────────────────────┤

│ │ CVE-2019-17595 │ │ │ │ ncurses: heap-based buffer overflow in the fmt\_entry │

│ │ │ │ │ │ function in tinfo/comp\_hash.c │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2019-17595 │

├───────────────┼──────────────────┼──────────┤ ├────────────────┼──────────────────────────────────────────────────────────────┤

│ ncurses-bin │ CVE-2022-29458 │ HIGH │ │ │ ncurses: segfaulting OOB read │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2022-29458 │

│ ├──────────────────┼──────────┤ ├────────────────┼──────────────────────────────────────────────────────────────┤

│ │ CVE-2018-19211 │ LOW │ │ │ ncurses: Null pointer dereference at function │

│ │ │ │ │ │ \_nc\_parse\_entry in parse\_entry.c │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2018-19211 │

│ ├──────────────────┤ │ ├────────────────┼──────────────────────────────────────────────────────────────┤

│ │ CVE-2019-17594 │ │ │ │ ncurses: heap-based buffer overflow in the \_nc\_find\_entry │

│ │ │ │ │ │ function in tinfo/comp\_hash.c │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2019-17594 │

│ ├──────────────────┤ │ ├────────────────┼──────────────────────────────────────────────────────────────┤

│ │ CVE-2019-17595 │ │ │ │ ncurses: heap-based buffer overflow in the fmt\_entry │

│ │ │ │ │ │ function in tinfo/comp\_hash.c │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2019-17595 │

├───────────────┼──────────────────┤ ├───────────────────────┼────────────────┼──────────────────────────────────────────────────────────────┤

│ passwd │ CVE-2018-7169 │ │ 1:4.4-4.1+deb9u1 │ │ shadow-utils: newgidmap allows unprivileged user to drop │

│ │ │ │ │ │ supplementary groups potentially allowing privilege... │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2018-7169 │

├───────────────┼──────────────────┼──────────┼───────────────────────┼────────────────┼──────────────────────────────────────────────────────────────┤

│ perl-base │ CVE-2020-16156 │ HIGH │ 5.24.1-3+deb9u7 │ │ perl-CPAN: Bypass of verification of signatures in CHECKSUMS │

│ │ │ │ │ │ files │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2020-16156 │

├───────────────┼──────────────────┼──────────┼───────────────────────┼────────────────┼──────────────────────────────────────────────────────────────┤

│ tzdata │ DLA-3051-1 │ UNKNOWN │ 2021a-0+deb9u3 │ 2021a-0+deb9u4 │ tzdata - new timezone database │

├───────────────┼──────────────────┼──────────┼───────────────────────┼────────────────┼──────────────────────────────────────────────────────────────┤

│ util-linux │ CVE-2016-2779 │ HIGH │ 2.29.2-1+deb9u1 │ │ util-linux: runuser tty hijack via TIOCSTI ioctl │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2016-2779 │

│ ├──────────────────┼──────────┤ ├────────────────┼──────────────────────────────────────────────────────────────┤

│ │ CVE-2021-37600 │ LOW │ │ │ util-linux: integer overflow can lead to buffer overflow in │

│ │ │ │ │ │ get\_sem\_elements() in sys-utils/ipcutils.c... │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2021-37600 │

└───────────────┴──────────────────┴──────────┴───────────────────────┴────────────────┴──────────────────────────────────────────────────────────────┘

Node.js (node-pkg)

==================

Total: 22 (UNKNOWN: 0, LOW: 0, MEDIUM: 10, HIGH: 9, CRITICAL: 3)

┌─────────────────────────────────────┬────────────────┬──────────┬───────────────────┬─────────────────────────────────────────────────────────┬──────────────────────────────────────────────────────────────┐

│ Library │ Vulnerability │ Severity │ Installed Version │ Fixed Version │ Title │

├─────────────────────────────────────┼────────────────┼──────────┼───────────────────┼─────────────────────────────────────────────────────────┼──────────────────────────────────────────────────────────────┤

│ ansi-regex (package.json) │ CVE-2021-3807 │ HIGH │ 3.0.0 │ 3.0.1, 4.1.1, 5.0.1, 6.0.1 │ nodejs-ansi-regex: Regular expression denial of service │

│ │ │ │ │ │ (ReDoS) matching ANSI escape codes │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2021-3807 │

│ │ │ ├───────────────────┤ │ │

│ │ │ │ 4.1.0 │ │ │

│ │ │ │ │ │ │

│ │ │ │ │ │ │

│ │ │ │ │ │ │

│ │ │ │ │ │ │

│ │ │ │ │ │ │

│ │ │ │ │ │ │

│ │ │ │ │ │ │

│ │ │ │ │ │ │

│ │ │ │ │ │ │

│ │ │ │ │ │ │

├─────────────────────────────────────┼────────────────┤ ├───────────────────┼─────────────────────────────────────────────────────────┼──────────────────────────────────────────────────────────────┤

│ decode-uri-component (package.json) │ CVE-2022-38900 │ │ 0.2.0 │ 0.2.1 │ improper input validation resulting in DoS │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2022-38900 │

├─────────────────────────────────────┼────────────────┤ ├───────────────────┼─────────────────────────────────────────────────────────┼──────────────────────────────────────────────────────────────┤

│ dicer (package.json) │ CVE-2022-24434 │ │ 0.2.5 │ │ nodejs service crash by sending a crafted payload │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2022-24434 │

├─────────────────────────────────────┼────────────────┼──────────┼───────────────────┼─────────────────────────────────────────────────────────┼──────────────────────────────────────────────────────────────┤

│ got (package.json) │ CVE-2022-33987 │ MEDIUM │ 6.7.1 │ 11.8.5, 12.1.0 │ nodejs-got: missing verification of requested URLs allows │

│ │ │ │ │ │ redirects to UNIX sockets │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2022-33987 │

├─────────────────────────────────────┼────────────────┼──────────┼───────────────────┼─────────────────────────────────────────────────────────┼──────────────────────────────────────────────────────────────┤

│ http-cache-semantics (package.json) │ CVE-2022-25881 │ HIGH │ 3.8.1 │ 4.1.1 │ Regular Expression Denial of Service (ReDoS) vulnerability │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2022-25881 │

├─────────────────────────────────────┼────────────────┼──────────┼───────────────────┼─────────────────────────────────────────────────────────┼──────────────────────────────────────────────────────────────┤

│ jsonwebtoken (package.json) │ CVE-2022-23539 │ MEDIUM │ 8.5.1 │ 9.0.0 │ jsonwebtoken: Unrestricted key type could lead to legacy │

│ │ │ │ │ │ keys usagen │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2022-23539 │

│ ├────────────────┤ │ │ ├──────────────────────────────────────────────────────────────┤

│ │ CVE-2022-23540 │ │ │ │ jsonwebtoken: Insecure default algorithm in jwt.verify() │

│ │ │ │ │ │ could lead to signature validation bypass... │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2022-23540 │

│ ├────────────────┤ │ │ ├──────────────────────────────────────────────────────────────┤

│ │ CVE-2022-23541 │ │ │ │ jsonwebtoken: Insecure implementation of key retrieval │

│ │ │ │ │ │ function could lead to Forgeable Public/Private... │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2022-23541 │

├─────────────────────────────────────┼────────────────┼──────────┼───────────────────┼─────────────────────────────────────────────────────────┼──────────────────────────────────────────────────────────────┤

│ minimatch (package.json) │ CVE-2022-3517 │ HIGH │ 3.0.4 │ 3.0.5 │ ReDoS via the braceExpand function │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2022-3517 │

├─────────────────────────────────────┼────────────────┼──────────┼───────────────────┼─────────────────────────────────────────────────────────┼──────────────────────────────────────────────────────────────┤

│ minimist (package.json) │ CVE-2021-44906 │ CRITICAL │ 1.2.5 │ 0.2.4, 1.2.6 │ prototype pollution │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2021-44906 │

│ │ │ │ │ │ │

│ │ │ │ │ │ │

│ │ │ │ │ │ │

├─────────────────────────────────────┼────────────────┼──────────┼───────────────────┼─────────────────────────────────────────────────────────┼──────────────────────────────────────────────────────────────┤

│ passport (package.json) │ CVE-2022-25896 │ MEDIUM │ 0.5.3 │ 0.6.0 │ passport: incorrect session regeneration │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2022-25896 │

├─────────────────────────────────────┼────────────────┼──────────┼───────────────────┼─────────────────────────────────────────────────────────┼──────────────────────────────────────────────────────────────┤

│ qs (package.json) │ CVE-2022-24999 │ HIGH │ 6.5.2 │ 6.2.4, 6.3.3, 6.4.1, 6.5.3, 6.6.1, 6.7.3, 6.8.3, 6.9.7, │ "qs" prototype poisoning causes the hang of the node process │

│ │ │ │ │ 6.10.3 │ https://avd.aquasec.com/nvd/cve-2022-24999 │

├─────────────────────────────────────┼────────────────┼──────────┼───────────────────┼─────────────────────────────────────────────────────────┼──────────────────────────────────────────────────────────────┤

│ request (package.json) │ CVE-2023-28155 │ MEDIUM │ 2.88.0 │ │ The Request package through 2.88.1 for Node.js allows a │

│ │ │ │ │ │ bypass of SSRF... │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2023-28155 │

│ │ │ │ ├─────────────────────────────────────────────────────────┤ │

│ │ │ │ │ │ │

│ │ │ │ │ │ │

│ │ │ │ │ │ │

│ │ │ ├───────────────────┼─────────────────────────────────────────────────────────┤ │

│ │ │ │ 2.88.2 │ │ │

│ │ │ │ │ │ │

│ │ │ │ │ │ │

├─────────────────────────────────────┼────────────────┼──────────┼───────────────────┼─────────────────────────────────────────────────────────┼──────────────────────────────────────────────────────────────┤

│ xmldom (package.json) │ CVE-2022-39353 │ CRITICAL │ 0.1.31 │ │ xmldom: Allows multiple root elements in a DOM tree │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2022-39353 │

│ ├────────────────┼──────────┤ ├─────────────────────────────────────────────────────────┼──────────────────────────────────────────────────────────────┤

│ │ CVE-2021-21366 │ MEDIUM │ │ 0.5.0 │ xmldom is a pure JavaScript W3C standard-based (XML DOM │

│ │ │ │ │ │ Level 2 Core)... │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2021-21366 │

│ ├────────────────┤ │ ├─────────────────────────────────────────────────────────┼──────────────────────────────────────────────────────────────┤

│ │ CVE-2021-32796 │ │ │ 0.7.0 │ nodejs-xmldom: misinterpretation of malicious XML input │

│ │ │ │ │ │ https://avd.aquasec.com/nvd/cve-2021-32796 │

└─────────────────────────────────────┴────────────────┴──────────┴───────────────────┴─────────────────────────────────────────────────────────┴──────────────────────────────────────────────────────────────┘