registry.cn-hangzhou.aliyuncs.com/acs/k8s-gpushare-plugin:v2-1.11-aff8a23 (debian 9.5) - Trivy Report - 2022-11-01 07:48:44.607420722 +0000 UTC m=+15.229094843

debian

Package	Vulnerability ID	Severity	Installed Version	Fixed Version	Links
apt	CVE-2019-3462	HIGH	1.4.8	1.4.9	http://www.securityfocus.com/bid/106690 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-3462 https://lists.apache.org/thread.html/8338a0f605bdbb3a6098bb76f666a95fc2b2f53f37fa1ecc89f1146f@%3Cdevnull.infra.apache.org%3E Toggle more links
bsdutils	CVE-2016-2779	HIGH	2.29.2-1+deb9u1		http://www.openwall.com/lists/oss-security/2016/02/27/1 http://www.openwall.com/lists/oss-security/2016/02/27/2 https://access.redhat.com/security/cve/CVE-2016-2779 Toggle more links
dpkg	CVE-2022-1664	CRITICAL	1.18.25	1.18.26	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1664 https://git.dpkg.org/cgit/dpkg/dpkg.git/commit/?id=1f23dddc17f69c9598477098c7fb9936e15fa495 https://git.dpkg.org/cgit/dpkg/dpkg.git/commit/?id=58814cacee39c4ce9e2cd0e3a3b9b57ad437eff5 Toggle more links
e2fslibs	CVE-2022-1304	HIGH	1.43.4-2		https://access.redhat.com/security/cve/CVE-2022-1304 https://bugzilla.redhat.com/show_bug.cgi?id=2069726 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1304 Toggle more links
e2fsprogs	CVE-2022-1304	HIGH	1.43.4-2		https://access.redhat.com/security/cve/CVE-2022-1304 https://bugzilla.redhat.com/show_bug.cgi?id=2069726 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1304 Toggle more links
gcc-6-base	CVE-2018-12886	HIGH	6.3.0-18+deb9u1		https://access.redhat.com/security/cve/CVE-2018-12886 https://gcc.gnu.org/viewcvs/gcc/trunk/gcc/config/arm/arm-protos.h?revision=266379&view=markup https://www.gnu.org/software/gcc/gcc-8/changes.html
gpgv	CVE-2018-1000858	HIGH	2.1.18-8~deb9u2		https://access.redhat.com/hydra/rest/securitydata/cve/CVE-2018-1000858.json https://access.redhat.com/hydra/rest/securitydata/cve/CVE-2019-13050.json https://access.redhat.com/security/cve/CVE-2018-1000858 Toggle more links
gzip	CVE-2022-1271	HIGH	1.6-5	1.6-5+deb9u1	https://access.redhat.com/hydra/rest/securitydata/cve/CVE-2022-1271.json https://access.redhat.com/security/cve/CVE-2022-1271 https://bugzilla.redhat.com/show_bug.cgi?id=2073310 Toggle more links
libapt-pkg5.0	CVE-2019-3462	HIGH	1.4.8	1.4.9	http://www.securityfocus.com/bid/106690 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-3462 https://lists.apache.org/thread.html/8338a0f605bdbb3a6098bb76f666a95fc2b2f53f37fa1ecc89f1146f@%3Cdevnull.infra.apache.org%3E Toggle more links
libblkid1	CVE-2016-2779	HIGH	2.29.2-1+deb9u1		http://www.openwall.com/lists/oss-security/2016/02/27/1 http://www.openwall.com/lists/oss-security/2016/02/27/2 https://access.redhat.com/security/cve/CVE-2016-2779 Toggle more links
libbz2-1.0	CVE-2019-12900	CRITICAL	1.0.6-8.1		http://lists.opensuse.org/opensuse-security-announce/2019-07/msg00040.html http://lists.opensuse.org/opensuse-security-announce/2019-08/msg00050.html http://lists.opensuse.org/opensuse-security-announce/2019-11/msg00078.html Toggle more links
libc-bin	CVE-2017-18269	CRITICAL	2.24-11+deb9u3	2.24-11+deb9u4	https://access.redhat.com/security/cve/CVE-2017-18269 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-18269 https://github.com/fingolfin/memmove-bug Toggle more links
libc-bin	CVE-2018-6485	CRITICAL	2.24-11+deb9u3		http://bugs.debian.org/878159 http://www.securityfocus.com/bid/102912 https://access.redhat.com/errata/RHBA-2019:0327 Toggle more links

libc-bin	CVE-2018-6551	**CRITICAL**	2.24-11+deb9u3		https://access.redhat.com/security/cve/CVE-2018-6551 https://security.netapp.com/advisory/ntap-20190404-0003/ https://sourceware.org/bugzilla/show_bug.cgi?id=22774 Toggle more links
libc-bin	CVE-2019-9169	**CRITICAL**	2.24-11+deb9u3		http://www.securityfocus.com/bid/107160 https://access.redhat.com/security/cve/CVE-2019-9169 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9169 Toggle more links
libc-bin	CVE-2021-33574	**CRITICAL**	2.24-11+deb9u3		https://access.redhat.com/security/cve/CVE-2021-33574 https://linux.oracle.com/cve/CVE-2021-33574.html https://linux.oracle.com/errata/ELSA-2021-9560.html Toggle more links
libc-bin	CVE-2021-35942	**CRITICAL**	2.24-11+deb9u3		https://access.redhat.com/hydra/rest/securitydata/cve/CVE-2021-35942.json https://access.redhat.com/security/cve/CVE-2021-35942 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35942 Toggle more links
libc-bin	CVE-2022-23218	**CRITICAL**	2.24-11+deb9u3		https://access.redhat.com/security/cve/CVE-2022-23218 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23218 https://linux.oracle.com/cve/CVE-2022-23218.html Toggle more links
libc-bin	CVE-2022-23219	**CRITICAL**	2.24-11+deb9u3		https://access.redhat.com/security/cve/CVE-2022-23219 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23219 https://linux.oracle.com/cve/CVE-2022-23219.html Toggle more links
libc-bin	CVE-2009-5155	**HIGH**	2.24-11+deb9u3		http://git.savannah.gnu.org/cgit/gnulib.git/commit/?id=5513b40999149090987a0341c018d05d3eea1272 https://access.redhat.com/security/cve/CVE-2009-5155 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-5155 Toggle more links
libc-bin	CVE-2017-1000408	**HIGH**	2.24-11+deb9u3	2.24-11+deb9u4	http://seclists.org/oss-sec/2017/q4/385 http://www.openwall.com/lists/oss-security/2017/12/11/4 http://www.openwall.com/lists/oss-security/2019/06/27/7 Toggle more links
libc-bin	CVE-2017-1000409	**HIGH**	2.24-11+deb9u3	2.24-11+deb9u4	http://seclists.org/oss-sec/2017/q4/385 http://www.openwall.com/lists/oss-security/2017/12/11/4 https://access.redhat.com/security/cve/CVE-2017-1000409 Toggle more links
libc-bin	CVE-2017-16997	**HIGH**	2.24-11+deb9u3	2.24-11+deb9u4	http://www.securityfocus.com/bid/102228 https://access.redhat.com/errata/RHBA-2019:0327 https://access.redhat.com/errata/RHSA-2018:3092 Toggle more links
libc-bin	CVE-2018-1000001	**HIGH**	2.24-11+deb9u3		http://seclists.org/oss-sec/2018/q1/38 http://www.openwall.com/lists/oss-security/2018/01/11/5 http://www.securityfocus.com/bid/102525 Toggle more links
libc-bin	CVE-2020-1751	**HIGH**	2.24-11+deb9u3		https://access.redhat.com/security/cve/CVE-2020-1751 https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1751 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1751 Toggle more links
libc-bin	CVE-2020-1752	**HIGH**	2.24-11+deb9u3		https://access.redhat.com/security/cve/CVE-2020-1752 https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1752 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1752 Toggle more links
libc-bin	CVE-2021-3326	**HIGH**	2.24-11+deb9u3		http://www.openwall.com/lists/oss-security/2021/01/28/2 https://access.redhat.com/security/cve/CVE-2021-3326 https://bugs.chromium.org/p/project-zero/issues/detail?id=2146 Toggle more links
libc-bin	CVE-2021-3999	**HIGH**	2.24-11+deb9u3		https://access.redhat.com/hydra/rest/securitydata/cve/CVE-2021-3999.json https://access.redhat.com/security/cve/CVE-2021-3999 https://bugzilla.redhat.com/show_bug.cgi?id=2024637 Toggle more links
libc6	CVE-2017-18269	**CRITICAL**	2.24-11+deb9u3	2.24-11+deb9u4	https://access.redhat.com/security/cve/CVE-2017-18269

					https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-18269 https://github.com/fingolfin/memmove-bug Toggle more links
libc6	CVE-2018-6485	**CRITICAL**	2.24-11+deb9u3		http://bugs.debian.org/878159 http://www.securityfocus.com/bid/102912 https://access.redhat.com/errata/RHBA-2019:0327 Toggle more links
libc6	CVE-2018-6551	**CRITICAL**	2.24-11+deb9u3		https://access.redhat.com/security/cve/CVE-2018-6551 https://security.netapp.com/advisory/ntap-20190404-0003/ https://sourceware.org/bugzilla/show_bug.cgi?id=22774 Toggle more links
libc6	CVE-2019-9169	**CRITICAL**	2.24-11+deb9u3		http://www.securityfocus.com/bid/107160 https://access.redhat.com/security/cve/CVE-2019-9169 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9169 Toggle more links
libc6	CVE-2021-33574	**CRITICAL**	2.24-11+deb9u3		https://access.redhat.com/security/cve/CVE-2021-33574 https://linux.oracle.com/cve/CVE-2021-33574.html https://linux.oracle.com/errata/ELSA-2021-9560.html Toggle more links
libc6	CVE-2021-35942	**CRITICAL**	2.24-11+deb9u3		https://access.redhat.com/hydra/rest/securitydata/cve/CVE-2021-35942.json https://access.redhat.com/security/cve/CVE-2021-35942 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35942 Toggle more links
libc6	CVE-2022-23218	**CRITICAL**	2.24-11+deb9u3		https://access.redhat.com/security/cve/CVE-2022-23218 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23218 https://linux.oracle.com/cve/CVE-2022-23218.html Toggle more links
libc6	CVE-2022-23219	**CRITICAL**	2.24-11+deb9u3		https://access.redhat.com/security/cve/CVE-2022-23219 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23219 https://linux.oracle.com/cve/CVE-2022-23219.html Toggle more links
libc6	CVE-2009-5155	**HIGH**	2.24-11+deb9u3		http://git.savannah.gnu.org/cgit/gnulib.git/commit/?id=5513b40999149090987a0341c018d05d3eea1272 https://access.redhat.com/security/cve/CVE-2009-5155 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-5155 Toggle more links
libc6	CVE-2017-1000408	**HIGH**	2.24-11+deb9u3	2.24-11+deb9u4	http://seclists.org/oss-sec/2017/q4/385 http://www.openwall.com/lists/oss-security/2017/12/11/4 http://www.openwall.com/lists/oss-security/2019/06/27/7 Toggle more links
libc6	CVE-2017-1000409	**HIGH**	2.24-11+deb9u3	2.24-11+deb9u4	http://seclists.org/oss-sec/2017/q4/385 http://www.openwall.com/lists/oss-security/2017/12/11/4 https://access.redhat.com/security/cve/CVE-2017-1000409 Toggle more links
libc6	CVE-2017-16997	**HIGH**	2.24-11+deb9u3	2.24-11+deb9u4	http://www.securityfocus.com/bid/102228 https://access.redhat.com/errata/RHBA-2019:0327 https://access.redhat.com/errata/RHSA-2018:3092 Toggle more links
libc6	CVE-2018-1000001	**HIGH**	2.24-11+deb9u3		http://seclists.org/oss-sec/2018/q1/38 http://www.openwall.com/lists/oss-security/2018/01/11/5 http://www.securityfocus.com/bid/102525 Toggle more links
libc6	CVE-2020-1751	**HIGH**	2.24-11+deb9u3		https://access.redhat.com/security/cve/CVE-2020-1751 https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1751 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1751 Toggle more links
libc6	CVE-2020-1752	**HIGH**	2.24-11+deb9u3		https://access.redhat.com/security/cve/CVE-2020-1752 https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1752 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1752 Toggle more links
libc6	CVE-2021-3326	**HIGH**	2.24-11+deb9u3		http://www.openwall.com/lists/oss-security/2021/01/28/2 https://access.redhat.com/security/cve/CVE-2021-3326 https://bugs.chromium.org/p/project-zero/issues/detail?id=2146

					Toggle more links
libc6	CVE-2021-3999	**HIGH**	2.24-11+deb9u3		https://access.redhat.com/hydra/rest/securitydata/cve/CVE-2021-3999.json https://access.redhat.com/security/cve/CVE-2021-3999 https://bugzilla.redhat.com/show_bug.cgi?id=2024637 Toggle more links
libcomerr2	CVE-2022-1304	**HIGH**	1.43.4-2		https://access.redhat.com/security/cve/CVE-2022-1304 https://bugzilla.redhat.com/show_bug.cgi?id=2069726 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1304 Toggle more links
libdb5.3	CVE-2019-8457	**CRITICAL**	5.3.28-12+deb9u1		http://lists.opensuse.org/opensuse-security-announce/2019-06/msg00074.html https://access.redhat.com/security/cve/CVE-2019-8457 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8457 Toggle more links
libfdisk1	CVE-2016-2779	**HIGH**	2.29.2-1+deb9u1		http://www.openwall.com/lists/oss-security/2016/02/27/1 http://www.openwall.com/lists/oss-security/2016/02/27/2 https://access.redhat.com/security/cve/CVE-2016-2779 Toggle more links
libgcc1	CVE-2018-12886	**HIGH**	6.3.0-18+deb9u1		https://access.redhat.com/security/cve/CVE-2018-12886 https://gcc.gnu.org/viewcvs/gcc/trunk/gcc/config/arm/arm-protos.h?revision=266379&view=markup https://www.gnu.org/software/gcc/gcc-8/changes.html
libgcrypt20	CVE-2021-33560	**HIGH**	1.7.6-2+deb9u3		https://access.redhat.com/hydra/rest/securitydata/cve/CVE-2021-33560.json https://access.redhat.com/security/cve/CVE-2021-33560 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33560 Toggle more links
liblz4-1	CVE-2021-3520	**CRITICAL**	0.0~r131-2	0.0~r131-2+deb9u1	https://access.redhat.com/hydra/rest/securitydata/cve/CVE-2021-3520.json https://access.redhat.com/security/cve/CVE-2021-3520 https://bugzilla.redhat.com/show_bug.cgi?id=1954559 Toggle more links
liblzma5	CVE-2022-1271	**HIGH**	5.2.2-1.2	5.2.2-1.2+deb9u1	https://access.redhat.com/hydra/rest/securitydata/cve/CVE-2022-1271.json https://access.redhat.com/security/cve/CVE-2022-1271 https://bugzilla.redhat.com/show_bug.cgi?id=2073310 Toggle more links
libmount1	CVE-2016-2779	**HIGH**	2.29.2-1+deb9u1		http://www.openwall.com/lists/oss-security/2016/02/27/1 http://www.openwall.com/lists/oss-security/2016/02/27/2 https://access.redhat.com/security/cve/CVE-2016-2779 Toggle more links
libncursesw5	CVE-2022-29458	**HIGH**	6.0+20161126-1+deb9u2		http://seclists.org/fulldisclosure/2022/Oct/41 https://access.redhat.com/security/cve/CVE-2022-29458 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29458 Toggle more links
libsmartcols1	CVE-2016-2779	**HIGH**	2.29.2-1+deb9u1		http://www.openwall.com/lists/oss-security/2016/02/27/1 http://www.openwall.com/lists/oss-security/2016/02/27/2 https://access.redhat.com/security/cve/CVE-2016-2779 Toggle more links
libss2	CVE-2022-1304	**HIGH**	1.43.4-2		https://access.redhat.com/security/cve/CVE-2022-1304 https://bugzilla.redhat.com/show_bug.cgi?id=2069726 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1304 Toggle more links
libstdc++6	CVE-2018-12886	**HIGH**	6.3.0-18+deb9u1		https://access.redhat.com/security/cve/CVE-2018-12886 https://gcc.gnu.org/viewcvs/gcc/trunk/gcc/config/arm/arm-protos.h?revision=266379&view=markup https://www.gnu.org/software/gcc/gcc-8/changes.html
libsystemd0	CVE-2022-2526	**CRITICAL**	232-25+deb9u4		https://access.redhat.com/errata/RHSA-2022:6206 https://access.redhat.com/hydra/rest/securitydata/cve/CVE-2022-2526.json https://access.redhat.com/security/cve/CVE-2022-2526 Toggle more links
libsystemd0	CVE-2018-15686	**HIGH**	232-25+deb9u4	232-25+deb9u10	http://www.securityfocus.com/bid/105747 https://access.redhat.com/errata/RHSA-2019:2091 https://access.redhat.com/errata/RHSA-2019:3222 Toggle more links
libsystemd0	CVE-2018-15688	**HIGH**	232-25+deb9u4	232-25+deb9u6	http://www.securityfocus.com/bid/105745 https://access.redhat.com/errata/RHBA-2019:0327

					https://access.redhat.com/errata/RHSA-2018:3665 Toggle more links
libsystemd0	CVE-2018-16864	**HIGH**	232-25+deb9u4	232-25+deb9u7	http://www.openwall.com/lists/oss-security/2021/07/20/2 http://www.securityfocus.com/bid/106523 https://access.redhat.com/errata/RHBA-2019:0327 Toggle more links
libsystemd0	CVE-2018-16865	**HIGH**	232-25+deb9u4	232-25+deb9u7	http://packetstormsecurity.com/files/152841/System-Down-A-systemd-journald-Exploit.html http://seclists.org/fulldisclosure/2019/May/21 http://www.openwall.com/lists/oss-security/2019/05/10/4 Toggle more links
libsystemd0	CVE-2019-3842	**HIGH**	232-25+deb9u4	232-25+deb9u11	http://lists.opensuse.org/opensuse-security-announce/2019-05/msg00062.html http://packetstormsecurity.com/files/152610/systemd-Seat-Verification-Active-Session-Spoofing.html https://access.redhat.com/security/cve/CVE-2019-3842 Toggle more links
libsystemd0	CVE-2019-3843	**HIGH**	232-25+deb9u4		http://www.securityfocus.com/bid/108116 https://access.redhat.com/security/cve/CVE-2019-3843 https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-3843 Toggle more links
libsystemd0	CVE-2019-3844	**HIGH**	232-25+deb9u4		http://www.securityfocus.com/bid/108096 https://access.redhat.com/security/cve/CVE-2019-3844 https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-3844 Toggle more links
libsystemd0	CVE-2020-1712	**HIGH**	232-25+deb9u4	232-25+deb9u14	https://access.redhat.com/security/cve/CVE-2020-1712 https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1712 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1712 Toggle more links
libtinfo5	CVE-2022-29458	**HIGH**	6.0+20161126-1+deb9u2		http://seclists.org/fulldisclosure/2022/Oct/41 https://access.redhat.com/security/cve/CVE-2022-29458 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29458 Toggle more links
libudev1	CVE-2022-2526	**CRITICAL**	232-25+deb9u4		https://access.redhat.com/errata/RHSA-2022:6206 https://access.redhat.com/hydra/rest/securitydata/cve/CVE-2022-2526.json https://access.redhat.com/security/cve/CVE-2022-2526 Toggle more links
libudev1	CVE-2018-15686	**HIGH**	232-25+deb9u4	232-25+deb9u10	http://www.securityfocus.com/bid/105747 https://access.redhat.com/errata/RHSA-2019:2091 https://access.redhat.com/errata/RHSA-2019:3222 Toggle more links
libudev1	CVE-2018-15688	**HIGH**	232-25+deb9u4	232-25+deb9u6	http://www.securityfocus.com/bid/105745 https://access.redhat.com/errata/RHBA-2019:0327 https://access.redhat.com/errata/RHSA-2018:3665 Toggle more links
libudev1	CVE-2018-16864	**HIGH**	232-25+deb9u4	232-25+deb9u7	http://www.openwall.com/lists/oss-security/2021/07/20/2 http://www.securityfocus.com/bid/106523 https://access.redhat.com/errata/RHBA-2019:0327 Toggle more links
libudev1	CVE-2018-16865	**HIGH**	232-25+deb9u4	232-25+deb9u7	http://packetstormsecurity.com/files/152841/System-Down-A-systemd-journald-Exploit.html http://seclists.org/fulldisclosure/2019/May/21 http://www.openwall.com/lists/oss-security/2019/05/10/4 Toggle more links
libudev1	CVE-2019-3842	**HIGH**	232-25+deb9u4	232-25+deb9u11	http://lists.opensuse.org/opensuse-security-announce/2019-05/msg00062.html http://packetstormsecurity.com/files/152610/systemd-Seat-Verification-Active-Session-Spoofing.html https://access.redhat.com/security/cve/CVE-2019-3842 Toggle more links
libudev1	CVE-2019-3843	**HIGH**	232-25+deb9u4		http://www.securityfocus.com/bid/108116 https://access.redhat.com/security/cve/CVE-2019-3843 https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-3843 Toggle more links
libudev1	CVE-2019-3844	**HIGH**	232-25+deb9u4		http://www.securityfocus.com/bid/108096 https://access.redhat.com/security/cve/CVE-2019-3844 https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-3844 Toggle more links

libudev1	CVE-2020-1712	**HIGH**	232-25+deb9u4	232-25+deb9u14	https://access.redhat.com/security/cve/CVE-2020-1712 https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1712 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1712 Toggle more links
libuuid1	CVE-2016-2779	**HIGH**	2.29.2-1+deb9u1		http://www.openwall.com/lists/oss-security/2016/02/27/1 http://www.openwall.com/lists/oss-security/2016/02/27/2 https://access.redhat.com/security/cve/CVE-2016-2779 Toggle more links
login	CVE-2017-12424	**CRITICAL**	1:4.4-4.1	1:4.4-4.1+deb9u1	https://access.redhat.com/security/cve/CVE-2017-12424 https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=756630 https://bugs.launchpad.net/ubuntu/+source/shadow/+bug/1266675 Toggle more links
login	CVE-2017-20002	**HIGH**	1:4.4-4.1	1:4.4-4.1+deb9u1	https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=877374 https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=914957 https://lists.debian.org/debian-lts-announce/2021/03/msg00020.html
mount	CVE-2016-2779	**HIGH**	2.29.2-1+deb9u1		http://www.openwall.com/lists/oss-security/2016/02/27/1 http://www.openwall.com/lists/oss-security/2016/02/27/2 https://access.redhat.com/security/cve/CVE-2016-2779 Toggle more links
multiarch-support	CVE-2017-18269	**CRITICAL**	2.24-11+deb9u3	2.24-11+deb9u4	https://access.redhat.com/security/cve/CVE-2017-18269 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-18269 https://github.com/fingolfin/memmove-bug Toggle more links
multiarch-support	CVE-2018-6485	**CRITICAL**	2.24-11+deb9u3		http://bugs.debian.org/878159 http://www.securityfocus.com/bid/102912 https://access.redhat.com/errata/RHBA-2019:0327 Toggle more links
multiarch-support	CVE-2018-6551	**CRITICAL**	2.24-11+deb9u3		https://access.redhat.com/security/cve/CVE-2018-6551 https://security.netapp.com/advisory/ntap-20190404-0003/ https://sourceware.org/bugzilla/show_bug.cgi?id=22774 Toggle more links
multiarch-support	CVE-2019-9169	**CRITICAL**	2.24-11+deb9u3		http://www.securityfocus.com/bid/107160 https://access.redhat.com/security/cve/CVE-2019-9169 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9169 Toggle more links
multiarch-support	CVE-2021-33574	**CRITICAL**	2.24-11+deb9u3		https://access.redhat.com/security/cve/CVE-2021-33574 https://linux.oracle.com/cve/CVE-2021-33574.html https://linux.oracle.com/errata/ELSA-2021-9560.html Toggle more links
multiarch-support	CVE-2021-35942	**CRITICAL**	2.24-11+deb9u3		https://access.redhat.com/hydra/rest/securitydata/cve/CVE-2021-35942.json https://access.redhat.com/security/cve/CVE-2021-35942 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35942 Toggle more links
multiarch-support	CVE-2022-23218	**CRITICAL**	2.24-11+deb9u3		https://access.redhat.com/security/cve/CVE-2022-23218 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23218 https://linux.oracle.com/cve/CVE-2022-23218.html Toggle more links
multiarch-support	CVE-2022-23219	**CRITICAL**	2.24-11+deb9u3		https://access.redhat.com/security/cve/CVE-2022-23219 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23219 https://linux.oracle.com/cve/CVE-2022-23219.html Toggle more links
multiarch-support	CVE-2009-5155	**HIGH**	2.24-11+deb9u3		http://git.savannah.gnu.org/cgit/gnulib.git/commit/?id=5513b40999149090987a0341c018d05d3eea1272 https://access.redhat.com/security/cve/CVE-2009-5155 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-5155 Toggle more links
multiarch-support	CVE-2017-1000408	**HIGH**	2.24-11+deb9u3	2.24-11+deb9u4	http://seclists.org/oss-sec/2017/q4/385 http://www.openwall.com/lists/oss-security/2017/12/11/4 http://www.openwall.com/lists/oss-security/2019/06/27/7 Toggle more links
multiarch-support	CVE-2017-1000409	**HIGH**	2.24-11+deb9u3	2.24-11+deb9u4	http://seclists.org/oss-sec/2017/q4/385 http://www.openwall.com/lists/oss-security/2017/12/11/4

					https://access.redhat.com/security/cve/CVE-2017-1000409 Toggle more links
multiarch-support	CVE-2017-16997	**HIGH**	2.24-11+deb9u3	2.24-11+deb9u4	http://www.securityfocus.com/bid/102228 https://access.redhat.com/errata/RHBA-2019:0327 https://access.redhat.com/errata/RHSA-2018:3092 Toggle more links
multiarch-support	CVE-2018-1000001	**HIGH**	2.24-11+deb9u3		http://seclists.org/oss-sec/2018/q1/38 http://www.openwall.com/lists/oss-security/2018/01/11/5 http://www.securityfocus.com/bid/102525 Toggle more links
multiarch-support	CVE-2020-1751	**HIGH**	2.24-11+deb9u3		https://access.redhat.com/security/cve/CVE-2020-1751 https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1751 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1751 Toggle more links
multiarch-support	CVE-2020-1752	**HIGH**	2.24-11+deb9u3		https://access.redhat.com/security/cve/CVE-2020-1752 https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1752 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1752 Toggle more links
multiarch-support	CVE-2021-3326	**HIGH**	2.24-11+deb9u3		http://www.openwall.com/lists/oss-security/2021/01/28/2 https://access.redhat.com/security/cve/CVE-2021-3326 https://bugs.chromium.org/p/project-zero/issues/detail?id=2146 Toggle more links
multiarch-support	CVE-2021-3999	**HIGH**	2.24-11+deb9u3		https://access.redhat.com/hydra/rest/securitydata/cve/CVE-2021-3999.json https://access.redhat.com/security/cve/CVE-2021-3999 https://bugzilla.redhat.com/show_bug.cgi?id=2024637 Toggle more links
ncurses-base	CVE-2022-29458	**HIGH**	6.0+20161126-1+deb9u2		http://seclists.org/fulldisclosure/2022/Oct/41 https://access.redhat.com/security/cve/CVE-2022-29458 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29458 Toggle more links
ncurses-bin	CVE-2022-29458	**HIGH**	6.0+20161126-1+deb9u2		http://seclists.org/fulldisclosure/2022/Oct/41 https://access.redhat.com/security/cve/CVE-2022-29458 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29458 Toggle more links
passwd	CVE-2017-12424	**CRITICAL**	1:4.4-4.1	1:4.4-4.1+deb9u1	https://access.redhat.com/security/cve/CVE-2017-12424 https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=756630 https://bugs.launchpad.net/ubuntu/+source/shadow/+bug/1266675 Toggle more links
passwd	CVE-2017-20002	**HIGH**	1:4.4-4.1	1:4.4-4.1+deb9u1	https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=877374 https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=914957 https://lists.debian.org/debian-lts-announce/2021/03/msg00020.html
perl-base	CVE-2018-18311	**CRITICAL**	5.24.1-3+deb9u4	5.24.1-3+deb9u5	http://seclists.org/fulldisclosure/2019/Mar/49 http://www.securityfocus.com/bid/106145 http://www.securitytracker.com/id/1042181 Toggle more links
perl-base	CVE-2018-18312	**CRITICAL**	5.24.1-3+deb9u4	5.24.1-3+deb9u5	http://www.securityfocus.com/bid/106179 http://www.securitytracker.com/id/1042181 https://access.redhat.com/errata/RHSA-2019:0001 Toggle more links
perl-base	CVE-2018-18313	**CRITICAL**	5.24.1-3+deb9u4	5.24.1-3+deb9u5	http://seclists.org/fulldisclosure/2019/Mar/49 http://www.securitytracker.com/id/1042181 https://access.redhat.com/errata/RHSA-2019:0001 Toggle more links
perl-base	CVE-2018-18314	**CRITICAL**	5.24.1-3+deb9u4	5.24.1-3+deb9u5	http://www.securityfocus.com/bid/106145 http://www.securitytracker.com/id/1042181 https://access.redhat.com/errata/RHSA-2019:0001 Toggle more links
perl-base	CVE-2020-10543	**HIGH**	5.24.1-3+deb9u4	5.24.1-3+deb9u7	http://lists.opensuse.org/opensuse-security-announce/2020-06/msg00044.html https://access.redhat.com/security/cve/CVE-2020-10543 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10543 Toggle more links

perl-base	CVE-2020-10878	**HIGH**	5.24.1-3+deb9u4	5.24.1-3+deb9u7	http://lists.opensuse.org/opensuse-security-announce/2020-06/msg00044.html https://access.redhat.com/security/cve/CVE-2020-10878 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10878 Toggle more links
perl-base	CVE-2020-12723	**HIGH**	5.24.1-3+deb9u4	5.24.1-3+deb9u7	http://lists.opensuse.org/opensuse-security-announce/2020-06/msg00044.html https://access.redhat.com/security/cve/CVE-2020-12723 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12723 Toggle more links
perl-base	CVE-2020-16156	**HIGH**	5.24.1-3+deb9u4		http://blogs.perl.org/users/neilb/2021/11/addressing-cpan-vulnerabilities-related-to-checksums.html https://access.redhat.com/security/cve/CVE-2020-16156 https://blog.hackeriet.no/cpan-signature-verification-vulnerabilities/ Toggle more links
util-linux	CVE-2016-2779	**HIGH**	2.29.2-1+deb9u1		http://www.openwall.com/lists/oss-security/2016/02/27/1 http://www.openwall.com/lists/oss-security/2016/02/27/2 https://access.redhat.com/security/cve/CVE-2016-2779 Toggle more links
zlib1g	CVE-2022-37434	**CRITICAL**	1:1.2.8.dfsg-5		http://seclists.org/fulldisclosure/2022/Oct/41 http://www.openwall.com/lists/oss-security/2022/08/05/2 http://www.openwall.com/lists/oss-security/2022/08/09/1 Toggle more links
zlib1g	CVE-2018-25032	**HIGH**	1:1.2.8.dfsg-5	1:1.2.8.dfsg-5+deb9u1	http://seclists.org/fulldisclosure/2022/May/33 http://seclists.org/fulldisclosure/2022/May/35 http://seclists.org/fulldisclosure/2022/May/38 Toggle more links

No Misconfigurations found

No Vulnerabilities found

No Misconfigurations found

No Vulnerabilities found

No Misconfigurations found

No Vulnerabilities found

No Misconfigurations found

OS Packages

Package	Licenses	Classification	Severity
adduser	GPL-2.0	restricted	**HIGH**
apt	GPL-2.0	restricted	**HIGH**
base-files	GPL-3.0	restricted	**HIGH**
base-passwd	GPL-2.0	restricted	**HIGH**
bash	GPL-3.0	restricted	**HIGH**
bsdutils	GPL-2.0	restricted	**HIGH**
bsdutils	LGPL-2.0	restricted	**HIGH**
bsdutils	LGPL-2.1	restricted	**HIGH**
bsdutils	GPL-3.0	restricted	**HIGH**
bsdutils	LGPL-3.0	restricted	**HIGH**
coreutils	GPL-3.0	restricted	**HIGH**
dash	GPL-3.0	restricted	**HIGH**
debian-archive-keyring	GPL-3.0	restricted	**HIGH**
debianutils	GPL-3.0	restricted	**HIGH**
diffutils	GPL-3.0	restricted	**HIGH**
dpkg	GPL-2.0	restricted	**HIGH**
e2fslibs	GPL-2.0	restricted	**HIGH**
e2fslibs	LGPL-2.0	restricted	**HIGH**

e2fsprogs	GPL-2.0	restricted	HIGH
e2fsprogs	LGPL-2.0	restricted	HIGH
findutils	GPL-3.0	restricted	HIGH
gcc-6-base	GPL-3.0	restricted	HIGH
gcc-6-base	GPL-2.0	restricted	HIGH
gpgv	GPL-3.0	restricted	HIGH
gpgv	LGPL-2.1	restricted	HIGH
gpgv	LGPL-3.0	restricted	HIGH
grep	GPL-3.0	restricted	HIGH
gzip	GPL-3.0	restricted	HIGH
hostname	GPL-2.0	restricted	HIGH
init-system-helpers	GPL-2.0	restricted	HIGH
libacl1	LGPL-2.1	restricted	HIGH
libacl1	GPL-3.0	restricted	HIGH
libapt-pkg5.0	GPL-2.0	restricted	HIGH
libattr1	LGPL-2.1	restricted	HIGH
libattr1	GPL-2.0	restricted	HIGH
libaudit-common	GPL-2.0	restricted	HIGH
libaudit-common	LGPL-2.1	restricted	HIGH
libaudit-common	GPL-1.0	restricted	HIGH
libaudit1	GPL-2.0	restricted	HIGH
libaudit1	LGPL-2.1	restricted	HIGH
libaudit1	GPL-1.0	restricted	HIGH
libblkid1	GPL-2.0	restricted	HIGH
libblkid1	LGPL-2.0	restricted	HIGH
libblkid1	LGPL-2.1	restricted	HIGH
libblkid1	GPL-3.0	restricted	HIGH
libblkid1	LGPL-3.0	restricted	HIGH
libbz2-1.0	GPL-2.0	restricted	HIGH
libc-bin	LGPL-2.1	restricted	HIGH
libc-bin	GPL-2.0	restricted	HIGH
libc6	LGPL-2.1	restricted	HIGH
libc6	GPL-2.0	restricted	HIGH
libcap-ng0	LGPL-2.1	restricted	HIGH
libcap-ng0	GPL-2.0	restricted	HIGH
libcap-ng0	GPL-3.0	restricted	HIGH
libdb5.3	Sleepycat	restricted	HIGH
libfdisk1	GPL-2.0	restricted	HIGH
libfdisk1	LGPL-2.0	restricted	HIGH
libfdisk1	LGPL-2.1	restricted	HIGH
libfdisk1	GPL-3.0	restricted	HIGH
libfdisk1	LGPL-3.0	restricted	HIGH
libgcrypt20	LGPL-3.0	restricted	HIGH
libgcrypt20	GPL-2.0	restricted	HIGH
libgpg-error0	LGPL-2.1	restricted	HIGH
liblz4-1	GPL-2.0	restricted	HIGH

liblzma5	GPL-2.0	restricted	**HIGH**
liblzma5	LGPL-2.1	restricted	**HIGH**
liblzma5	LGPL-2.0	restricted	**HIGH**
liblzma5	GPL-3.0	restricted	**HIGH**
libmount1	GPL-2.0	restricted	**HIGH**
libmount1	LGPL-2.0	restricted	**HIGH**
libmount1	LGPL-2.1	restricted	**HIGH**
libmount1	GPL-3.0	restricted	**HIGH**
libmount1	LGPL-3.0	restricted	**HIGH**
libpam-modules	GPL-3.0	restricted	**HIGH**
libpam-modules-bin	GPL-3.0	restricted	**HIGH**
libpam-runtime	GPL-3.0	restricted	**HIGH**
libpam0g	GPL-3.0	restricted	**HIGH**
libselinux1	LGPL-2.1	restricted	**HIGH**
libselinux1	GPL-2.0	restricted	**HIGH**
libsemanage-common	LGPL-3.0	restricted	**HIGH**
libsemanage-common	GPL-3.0	restricted	**HIGH**
libsemanage1	LGPL-3.0	restricted	**HIGH**
libsemanage1	GPL-3.0	restricted	**HIGH**
libsepol1	LGPL-3.0	restricted	**HIGH**
libsepol1	GPL-3.0	restricted	**HIGH**
libsmartcols1	GPL-2.0	restricted	**HIGH**
libsmartcols1	LGPL-2.0	restricted	**HIGH**
libsmartcols1	LGPL-2.1	restricted	**HIGH**
libsmartcols1	GPL-3.0	restricted	**HIGH**
libsmartcols1	LGPL-3.0	restricted	**HIGH**
libsystemd0	LGPL-2.1	restricted	**HIGH**
libsystemd0	GPL-2.0	restricted	**HIGH**
libudev1	LGPL-2.1	restricted	**HIGH**
libudev1	GPL-2.0	restricted	**HIGH**
libustr-1.0-1	LGPL-2.0	restricted	**HIGH**
libustr-1.0-1	GPL-2.0	restricted	**HIGH**
libustr-1.0-1	LGPL-2.1	restricted	**HIGH**
libuuid1	GPL-2.0	restricted	**HIGH**
libuuid1	LGPL-2.0	restricted	**HIGH**
libuuid1	LGPL-2.1	restricted	**HIGH**
libuuid1	GPL-3.0	restricted	**HIGH**
libuuid1	LGPL-3.0	restricted	**HIGH**
login	GPL-2.0	restricted	**HIGH**
lsb-base	GPL-2.0	restricted	**HIGH**
mawk	GPL-2.0	restricted	**HIGH**
mount	GPL-2.0	restricted	**HIGH**
mount	LGPL-2.0	restricted	**HIGH**
mount	LGPL-2.1	restricted	**HIGH**
mount	GPL-3.0	restricted	**HIGH**
mount	LGPL-3.0	restricted	**HIGH**

multiarch-support	LGPL-2.1	restricted	**HIGH**
multiarch-support	GPL-2.0	restricted	**HIGH**
passwd	GPL-2.0	restricted	**HIGH**
sed	GPL-3.0	restricted	**HIGH**
sensible-utils	GPL-2.0	restricted	**HIGH**
sysvinit-utils	GPL-2.0	restricted	**HIGH**
tar	GPL-3.0	restricted	**HIGH**
tar	GPL-2.0	restricted	**HIGH**
util-linux	GPL-2.0	restricted	**HIGH**
util-linux	LGPL-2.0	restricted	**HIGH**
util-linux	LGPL-2.1	restricted	**HIGH**
util-linux	GPL-3.0	restricted	**HIGH**
util-linux	LGPL-3.0	restricted	**HIGH**