脆弱性レポート - ツール: trivy

2025-09-26 08:40:17

対象: ubuntu:latest (ubuntu 24.04)

ID	PkgName	InstalledVersion	Severity	Title
CVE-2016-2781	coreutils	9.4-3ubuntu6	LOW	coreutils: Non-privileged session can escape to the parent session in chroot
CVE-2025-6297	dpkg	1.22.6ubuntu6.1	LOW	It was discovered that dpkg-deb does not properly sanitize directory p ...
CVE-2025-30258	gpgv	2.4.4-2ubuntu17	MEDIUM	gnupg: verification DoS due to a malicious subkey in the keyring
CVE-2022-3219	gpgv	2.4.4-2ubuntu17	LOW	gnupg: denial of service issue (resource consumption) using compressed packets
CVE-2025-0395	libc-bin	2.39-0ubuntu8.3	MEDIUM	glibc: buffer overflow in the GNU C Library's assert()
CVE-2025-5702	libc-bin	2.39-0ubuntu8.3	MEDIUM	glibc: Vector register overwrite bug in glibc
CVE-2025-8058	libc-bin	2.39-0ubuntu8.3	MEDIUM	glibc: Double free in glibc
CVE-2025-0395	libc6	2.39-0ubuntu8.3	MEDIUM	glibc: buffer overflow in the GNU C Library's assert()
CVE-2025-5702	libc6	2.39-0ubuntu8.3	MEDIUM	glibc: Vector register overwrite bug in glibc
CVE-2025-8058	libc6	2.39-0ubuntu8.3	MEDIUM	glibc: Double free in glibc
CVE-2025-1390	libcap2	1:2.66-5ubuntu2	MEDIUM	libcap: pam_cap: Fix potential configuration parsing error
CVE-2024-2236	libgcrypt20	1.10.3-2build1	LOW	libgcrypt: vulnerable to Marvin Attack
CVE-2024-12243	libgnutls30t64	3.8.3-1.1ubuntu3.2	MEDIUM	gnutls: GnuTLS Impacted by Inefficient DER Decoding in libtasn1 Leading to Remote DoS
CVE-2025-32988	libgnutls30t64	3.8.3-1.1ubuntu3.2	MEDIUM	gnutls: Vulnerability in GnuTLS otherName SAN export
CVE-2025-32989	libgnutls30t64	3.8.3-1.1ubuntu3.2	MEDIUM	gnutls: Vulnerability in GnuTLS SCT extension parsing
CVE-2025-32990	libgnutls30t64	3.8.3-1.1ubuntu3.2	MEDIUM	gnutls: Vulnerability in GnuTLS certtool template parsing
CVE-2025-6395	libgnutls30t64	3.8.3-1.1ubuntu3.2	MEDIUM	gnutls: NULL pointer dereference in _gnutls_figure_common_ciphersuite()
CVE-2025-31115	liblzma5	5.6.1+really5.4.5-1build0.1	MEDIUM	xz: XZ has a heap-use-after-free bug in threaded .xz decoder

ID	PkgName	InstalledVersion	Severity	Title
CVE-2024-10963	libpam-modules	1.5.3-5ubuntu5.1	MEDIUM	pam: Improper Hostname Interpretation in pam_access Leads to Access Control Bypass
CVE-2025-6020	libpam-modules	1.5.3-5ubuntu5.1	MEDIUM	linux-pam: Linux-pam directory Traversal
CVE-2025-8941	libpam-modules	1.5.3-5ubuntu5.1	MEDIUM	linux-pam: Incomplete fix for CVE-2025-6020
CVE-2024-10963	libpam-modules-bin	1.5.3-5ubuntu5.1	MEDIUM	pam: Improper Hostname Interpretation in pam_access Leads to Access Control Bypass
CVE-2025-6020	libpam-modules-bin	1.5.3-5ubuntu5.1	MEDIUM	linux-pam: Linux-pam directory Traversal
CVE-2025-8941	libpam-modules-bin	1.5.3-5ubuntu5.1	MEDIUM	linux-pam: Incomplete fix for CVE-2025-6020
CVE-2024-10963	libpam-runtime	1.5.3-5ubuntu5.1	MEDIUM	pam: Improper Hostname Interpretation in pam_access Leads to Access Control Bypass
CVE-2025-6020	libpam-runtime	1.5.3-5ubuntu5.1	MEDIUM	linux-pam: Linux-pam directory Traversal
CVE-2025-8941	libpam-runtime	1.5.3-5ubuntu5.1	MEDIUM	linux-pam: Incomplete fix for CVE-2025-6020
CVE-2024-10963	libpam0g	1.5.3-5ubuntu5.1	MEDIUM	pam: Improper Hostname Interpretation in pam_access Leads to Access Control Bypass
CVE-2025-6020	libpam0g	1.5.3-5ubuntu5.1	MEDIUM	linux-pam: Linux-pam directory Traversal
CVE-2025-8941	libpam0g	1.5.3-5ubuntu5.1	MEDIUM	linux-pam: Incomplete fix for CVE-2025-6020
CVE-2024-13176	libssl3t64	3.0.13-0ubuntu3.4	LOW	openssl: Timing side-channel in ECDSA signature computation
CVE-2024-41996	libssl3t64	3.0.13-0ubuntu3.4	LOW	openssl: remote attackers (from the client side) to trigger unnecessarily expensive server-side DHE modular-exponentiation calculations
CVE-2024-9143	libssl3t64	3.0.13-0ubuntu3.4	LOW	openssl: Low-level invalid GF(2^m) parameters lead to OOB memory access
CVE-2025-4598	libsystemd0	255.4-1ubuntu8.4	MEDIUM	systemd-coredump: race condition that allows a local attacker to crash a SUID program and gain read access to the resulting core dump
CVE-2024-12133	libtasn1-6	4.19.0-3build1	MEDIUM	libtasn1: Inefficient DER Decoding in libtasn1 Leading to Potential Remote DoS

ID	PkgName	InstalledVersion	Severity	Title
CVE-2025-4598	libudev1	255.4-1ubuntu8.4	MEDIUM	systemd-coredump: race condition that allows a local attacker to crash a SUID program and gain read access to the resulting core dump
CVE-2024-56433	login	1:4.13+dfsg1-4ubuntu3.2	LOW	shadow-utils: Default subordinate ID configuration in /etc/login.defs could lead to compromise
CVE-2024-56433	passwd	1:4.13+dfsg1-4ubuntu3.2	LOW	shadow-utils: Default subordinate ID configuration in /etc/login.defs could lead to compromise
CVE-2024-56406	perl-base	5.38.2-3.2build2	MEDIUM	perl: Perl 5.34, 5.36, 5.38 and 5.40 are vulnerable to a heap buffer overflow when transliterating non-ASCII bytes
CVE-2025-40909	perl-base	5.38.2-3.2build2	MEDIUM	perl: Perl threads have a working directory race condition where file operations may target unintended paths
CVE-2025-45582	tar	1.35+dfsg-3build1	MEDIUM	tar: Tar path traversal