alpha-processing — Trivy 이미지 점검 리포트

저장소	pi-continuum/alpha-processing
커밋	`b11f26b8a73969c125bab541bd852d8aa055f9fd` · branch `main` · pi-continuum
이미지	`alpha-processing:b11f26b` · `sha256:4e78b2f21812bf6e22ae2ad086e08eaf64f3b9e33f3c6fbc7b863bf2de658fce`
빌드 시각	2026-09-13 23:20:25 KST
리포트 생성	2026-09-13 23:32:51 KST · Trivy 0.74.0

요약

Severity	취약점	비밀값	합계
CRITICAL	1	0	1
HIGH	52	0	52
MEDIUM	92	0	92
LOW	127	0	127
UNKNOWN	1	0	1
합계	273	0	273

대상

Target	Class	Type	취약점	비밀값
alpha-processing-b11f26b.tar (debian 13.7)	os-pkgs	debian	272	0
Node.js	lang-pkgs	node-pkg	0	0
Python	lang-pkgs	python-pkg	1	0

alpha-processing-b11f26b.tar (debian 13.7) (os-pkgs / debian)

Severity	취약점 ID	패키지	설치 버전	수정 버전	상태	제목
CRITICAL	CVE-2026-6653	libxml2	2.12.7+dfsg+really2.9.14-2.1+deb13u3		affected	libxml2: mingw-libxml2: libxml2: Denial of Service via crafted XML input due to use-after-free

Severity	취약점 ID	패키지	설치 버전	수정 버전	상태	제목
HIGH	CVE-2026-76642	bsdutils	1:2.41.5-0+deb13u1		affected	util-linux: util-linux: failed external mount helper still runs privileged X-mount post-hooks
HIGH	CVE-2026-78408	bsdutils	1:2.41.5-0+deb13u1		affected	util-linux: util-linux: nsenter --join-cgroup leaks root cgroup migration authority
HIGH	CVE-2026-78409	bsdutils	1:2.41.5-0+deb13u1		affected	util-linux: util-linux: X-mount.subdir detached-tree resolution can escape via intermediate symlinks
HIGH	CVE-2026-78410	bsdutils	1:2.41.5-0+deb13u1		affected	util-linux: util-linux: restricted bind mounts do not pin the source, allowing X-mount.owner/group/mode redirection
HIGH	CVE-2026-54369	libacl1	2.3.2-2+b1		affected	acl: Symlink traversal privilege escalation via libacl functions
HIGH	CVE-2026-76642	libblkid1	2.41.5-0+deb13u1		affected	util-linux: util-linux: failed external mount helper still runs privileged X-mount post-hooks
HIGH	CVE-2026-78408	libblkid1	2.41.5-0+deb13u1		affected	util-linux: util-linux: nsenter --join-cgroup leaks root cgroup migration authority
HIGH	CVE-2026-78409	libblkid1	2.41.5-0+deb13u1		affected	util-linux: util-linux: X-mount.subdir detached-tree resolution can escape via intermediate symlinks
HIGH	CVE-2026-78410	libblkid1	2.41.5-0+deb13u1		affected	util-linux: util-linux: restricted bind mounts do not pin the source, allowing X-mount.owner/group/mode redirection
HIGH	CVE-2026-34980	libcups2t64	2.4.10-3+deb13u2		affected	cups: OpenPrinting CUPS: Shared PostScript queue lets anonymous Print-Job requests reach `lp` code execution over the network
HIGH	CVE-2026-76956	libexpat1	2.8.3-1~deb13u1		affected	libexpat: libexpat: Denial of Service via hash flooding attack with crafted XML
HIGH	CVE-2026-76957	libexpat1	2.8.3-1~deb13u1		affected	libexpat: libexpat: Memory corruption vulnerability allows arbitrary code execution or denial of service
HIGH	CVE-2026-76642	liblastlog2-2	2.41.5-0+deb13u1		affected	util-linux: util-linux: failed external mount helper still runs privileged X-mount post-hooks
HIGH	CVE-2026-78408	liblastlog2-2	2.41.5-0+deb13u1		affected	util-linux: util-linux: nsenter --join-cgroup leaks root cgroup migration authority
HIGH	CVE-2026-78409	liblastlog2-2	2.41.5-0+deb13u1		affected	util-linux: util-linux: X-mount.subdir detached-tree resolution can escape via intermediate symlinks
HIGH	CVE-2026-78410	liblastlog2-2	2.41.5-0+deb13u1		affected	util-linux: util-linux: restricted bind mounts do not pin the source, allowing X-mount.owner/group/mode redirection
HIGH	CVE-2026-76642	libmount1	2.41.5-0+deb13u1		affected	util-linux: util-linux: failed external mount helper still runs privileged X-mount post-hooks
HIGH	CVE-2026-78408	libmount1	2.41.5-0+deb13u1		affected	util-linux: util-linux: nsenter --join-cgroup leaks root cgroup migration authority
HIGH	CVE-2026-78409	libmount1	2.41.5-0+deb13u1		affected	util-linux: util-linux: X-mount.subdir detached-tree resolution can escape via intermediate symlinks

Severity	취약점 ID	패키지	설치 버전	수정 버전	상태	제목
HIGH	CVE-2026-78410	libmount1	2.41.5-0+deb13u1		affected	util-linux: util-linux: restricted bind mounts do not pin the source, allowing X-mount.owner/group/mode redirection
HIGH	CVE-2025-69720	libncursesw6	6.5+20250216-2		affected	ncurses: ncurses: Buffer overflow vulnerability may lead to arbitrary code execution.
HIGH	CVE-2026-76642	libsmartcols1	2.41.5-0+deb13u1		affected	util-linux: util-linux: failed external mount helper still runs privileged X-mount post-hooks
HIGH	CVE-2026-78408	libsmartcols1	2.41.5-0+deb13u1		affected	util-linux: util-linux: nsenter --join-cgroup leaks root cgroup migration authority
HIGH	CVE-2026-78409	libsmartcols1	2.41.5-0+deb13u1		affected	util-linux: util-linux: X-mount.subdir detached-tree resolution can escape via intermediate symlinks
HIGH	CVE-2026-78410	libsmartcols1	2.41.5-0+deb13u1		affected	util-linux: util-linux: restricted bind mounts do not pin the source, allowing X-mount.owner/group/mode redirection
HIGH	CVE-2026-16742	libsystemd0	257.13-1~deb13u1		affected	systemd: systemd-homed: Local privilege escalation via missing home-record signature verification
HIGH	CVE-2025-69720	libtinfo6	6.5+20250216-2		affected	ncurses: ncurses: Buffer overflow vulnerability may lead to arbitrary code execution.
HIGH	CVE-2026-16742	libudev1	257.13-1~deb13u1		affected	systemd: systemd-homed: Local privilege escalation via missing home-record signature verification
HIGH	CVE-2026-76642	libuuid1	2.41.5-0+deb13u1		affected	util-linux: util-linux: failed external mount helper still runs privileged X-mount post-hooks
HIGH	CVE-2026-78408	libuuid1	2.41.5-0+deb13u1		affected	util-linux: util-linux: nsenter --join-cgroup leaks root cgroup migration authority
HIGH	CVE-2026-78409	libuuid1	2.41.5-0+deb13u1		affected	util-linux: util-linux: X-mount.subdir detached-tree resolution can escape via intermediate symlinks
HIGH	CVE-2026-78410	libuuid1	2.41.5-0+deb13u1		affected	util-linux: util-linux: restricted bind mounts do not pin the source, allowing X-mount.owner/group/mode redirection
HIGH	CVE-2026-74860	libxml2	2.12.7+dfsg+really2.9.14-2.1+deb13u3		affected	libxml2: double-free/UAF in libxml2 Python bindings
HIGH	CVE-2026-86140	libxml2	2.12.7+dfsg+really2.9.14-2.1+deb13u3		affected	libxml2: libxml2: Arbitrary code execution via stack-based buffer overflow in xmlSnprintfElements
HIGH	CVE-2026-76642	login	1:4.16.0-2+really2.41.5-0+deb13u1		affected	util-linux: util-linux: failed external mount helper still runs privileged X-mount post-hooks
HIGH	CVE-2026-78408	login	1:4.16.0-2+really2.41.5-0+deb13u1		affected	util-linux: util-linux: nsenter --join-cgroup leaks root cgroup migration authority
HIGH	CVE-2026-78409	login	1:4.16.0-2+really2.41.5-0+deb13u1		affected	util-linux: util-linux: X-mount.subdir detached-tree resolution can escape via intermediate symlinks

Severity	취약점 ID	패키지	설치 버전	수정 버전	상태	제목
HIGH	CVE-2026-78410	login	1:4.16.0-2+really2.41.5-0+deb13u1		affected	util-linux: util-linux: restricted bind mounts do not pin the source, allowing X-mount.owner/group/mode redirection
HIGH	CVE-2026-76642	mount	2.41.5-0+deb13u1		affected	util-linux: util-linux: failed external mount helper still runs privileged X-mount post-hooks
HIGH	CVE-2026-78408	mount	2.41.5-0+deb13u1		affected	util-linux: util-linux: nsenter --join-cgroup leaks root cgroup migration authority
HIGH	CVE-2026-78409	mount	2.41.5-0+deb13u1		affected	util-linux: util-linux: X-mount.subdir detached-tree resolution can escape via intermediate symlinks
HIGH	CVE-2026-78410	mount	2.41.5-0+deb13u1		affected	util-linux: util-linux: restricted bind mounts do not pin the source, allowing X-mount.owner/group/mode redirection
HIGH	CVE-2025-69720	ncurses-base	6.5+20250216-2		affected	ncurses: ncurses: Buffer overflow vulnerability may lead to arbitrary code execution.
HIGH	CVE-2025-69720	ncurses-bin	6.5+20250216-2		affected	ncurses: ncurses: Buffer overflow vulnerability may lead to arbitrary code execution.
HIGH	CVE-2026-9538	perl-base	5.40.1-6+deb13u1		fix_deferred	perl-Archive-Tar: perl-Archive-Tar: Denial of Service via crafted tar header with large entry size
HIGH	CVE-2026-76642	util-linux	2.41.5-0+deb13u1		affected	util-linux: util-linux: failed external mount helper still runs privileged X-mount post-hooks
HIGH	CVE-2026-78408	util-linux	2.41.5-0+deb13u1		affected	util-linux: util-linux: nsenter --join-cgroup leaks root cgroup migration authority
HIGH	CVE-2026-78409	util-linux	2.41.5-0+deb13u1		affected	util-linux: util-linux: X-mount.subdir detached-tree resolution can escape via intermediate symlinks
HIGH	CVE-2026-78410	util-linux	2.41.5-0+deb13u1		affected	util-linux: util-linux: restricted bind mounts do not pin the source, allowing X-mount.owner/group/mode redirection
HIGH	CVE-2023-5574	xserver-common	2:21.1.16-1.3+deb13u4		fix_deferred	xorg-x11-server: Use-after-free bug in DamageDestroy
HIGH	CVE-2023-5574	xvfb	2:21.1.16-1.3+deb13u4		fix_deferred	xorg-x11-server: Use-after-free bug in DamageDestroy
MEDIUM	CVE-2026-3184	bsdutils	1:2.41.5-0+deb13u1		affected	util-linux: util-linux: Access control bypass due to improper hostname canonicalization
MEDIUM	CVE-2026-54370	libacl1	2.3.2-2+b1		affected	acl: TOCTOU Symlink Traversal via getfacl/setfacl
MEDIUM	CVE-2026-54371	libattr1	1:2.5.2-3		affected	attr: attr: Symlink Traversal Privilege Escalation via getfattr and setfattr
MEDIUM	CVE-2024-52615	libavahi-client3	0.8-16		affected	avahi: Avahi Wide-Area DNS Uses Constant Source Port

Severity	취약점 ID	패키지	설치 버전	수정 버전	상태	제목
MEDIUM	CVE-2024-52616	libavahi-client3	0.8-16		affected	avahi: Avahi Wide-Area DNS Predictable Transaction IDs
MEDIUM	CVE-2025-59529	libavahi-client3	0.8-16		fix_deferred	avahi: simple clients denial-of-service
MEDIUM	CVE-2025-68276	libavahi-client3	0.8-16		affected	avahi: Avahi: Denial of Service via D-Bus record browsers with AVAHI_LOOKUP_USE_WIDE_AREA flag
MEDIUM	CVE-2025-68468	libavahi-client3	0.8-16		affected	avahi: Avahi: Denial of Service via crafted mDNS/DNS-SD announcements
MEDIUM	CVE-2025-68471	libavahi-client3	0.8-16		affected	avahi: Avahi: Denial of Service via unsolicited CNAME announcements
MEDIUM	CVE-2026-24401	libavahi-client3	0.8-16		affected	avahi: Avahi: Denial of Service via recursive CNAME record in mDNS response
MEDIUM	CVE-2026-34933	libavahi-client3	0.8-16		affected	avahi: avahi-daemon: Avahi: Denial of Service via D-Bus method call
MEDIUM	CVE-2024-52615	libavahi-common-data	0.8-16		affected	avahi: Avahi Wide-Area DNS Uses Constant Source Port
MEDIUM	CVE-2024-52616	libavahi-common-data	0.8-16		affected	avahi: Avahi Wide-Area DNS Predictable Transaction IDs
MEDIUM	CVE-2025-59529	libavahi-common-data	0.8-16		fix_deferred	avahi: simple clients denial-of-service
MEDIUM	CVE-2025-68276	libavahi-common-data	0.8-16		affected	avahi: Avahi: Denial of Service via D-Bus record browsers with AVAHI_LOOKUP_USE_WIDE_AREA flag
MEDIUM	CVE-2025-68468	libavahi-common-data	0.8-16		affected	avahi: Avahi: Denial of Service via crafted mDNS/DNS-SD announcements
MEDIUM	CVE-2025-68471	libavahi-common-data	0.8-16		affected	avahi: Avahi: Denial of Service via unsolicited CNAME announcements
MEDIUM	CVE-2026-24401	libavahi-common-data	0.8-16		affected	avahi: Avahi: Denial of Service via recursive CNAME record in mDNS response
MEDIUM	CVE-2026-34933	libavahi-common-data	0.8-16		affected	avahi: avahi-daemon: Avahi: Denial of Service via D-Bus method call
MEDIUM	CVE-2024-52615	libavahi-common3	0.8-16		affected	avahi: Avahi Wide-Area DNS Uses Constant Source Port

Severity	취약점 ID	패키지	설치 버전	수정 버전	상태	제목
MEDIUM	CVE-2024-52616	libavahi-common3	0.8-16		affected	avahi: Avahi Wide-Area DNS Predictable Transaction IDs
MEDIUM	CVE-2025-59529	libavahi-common3	0.8-16		fix_deferred	avahi: simple clients denial-of-service
MEDIUM	CVE-2025-68276	libavahi-common3	0.8-16		affected	avahi: Avahi: Denial of Service via D-Bus record browsers with AVAHI_LOOKUP_USE_WIDE_AREA flag
MEDIUM	CVE-2025-68468	libavahi-common3	0.8-16		affected	avahi: Avahi: Denial of Service via crafted mDNS/DNS-SD announcements
MEDIUM	CVE-2025-68471	libavahi-common3	0.8-16		affected	avahi: Avahi: Denial of Service via unsolicited CNAME announcements
MEDIUM	CVE-2026-24401	libavahi-common3	0.8-16		affected	avahi: Avahi: Denial of Service via recursive CNAME record in mDNS response
MEDIUM	CVE-2026-34933	libavahi-common3	0.8-16		affected	avahi: avahi-daemon: Avahi: Denial of Service via D-Bus method call
MEDIUM	CVE-2026-3184	libblkid1	2.41.5-0+deb13u1		affected	util-linux: util-linux: Access control bypass due to improper hostname canonicalization
MEDIUM	CVE-2026-42250	libbz2-1.0	1.0.8-6		affected	bzip2: bzip2: Denial of Service in bzip2recover via a specially crafted file
MEDIUM	CVE-2026-18374	libc-bin	2.41-12+deb13u4		affected	glibc: glibc: Heap buffer overflow via attacker-controlled fopen mode string
MEDIUM	CVE-2026-19499	libc-bin	2.41-12+deb13u4		affected	glibc: Buffer Overflow in strfmon right-justification padding
MEDIUM	CVE-2026-19542	libc-bin	2.41-12+deb13u4		affected	glibc: Fix out-of-bounds array write in tdelete
MEDIUM	CVE-2026-5435	libc-bin	2.41-12+deb13u4		affected	glibc: glibc: Out-of-bounds write via TSIG record processing
MEDIUM	CVE-2026-6238	libc-bin	2.41-12+deb13u4		affected	glibc: glibc: Application crash or uninitialized memory read via crafted DNS response
MEDIUM	CVE-2026-6368	libc-bin	2.41-12+deb13u4		affected	glibc: glibc: Process abort due to invalid memory in wordexp
MEDIUM	CVE-2026-6791	libc-bin	2.41-12+deb13u4		affected	glibc: Glibc: Denial of Service via stack exhaustion during tilde expansion
MEDIUM	CVE-2026-77117	libc-bin	2.41-12+deb13u4		affected	glibc: Non-progress DoS in SHIFT_JISX0213 -&gt
MEDIUM	CVE-2026-80489	libc-bin	2.41-12+deb13u4		affected	glibc: Non-progress DoS in EUC_JISX0213 -> UCS-4 conversion state
MEDIUM	CVE-2026-89092	libc-bin	2.41-12+deb13u4		affected	glibc: glibc: nscd stack overflow leads to degraded DNS resolution
MEDIUM	CVE-2026-18374	libc6	2.41-12+deb13u4		affected	glibc: glibc: Heap buffer overflow via attacker-controlled fopen mode string
MEDIUM	CVE-2026-19499	libc6	2.41-12+deb13u4		affected	glibc: Buffer Overflow in strfmon right-justification padding

Severity	취약점 ID	패키지	설치 버전	수정 버전	상태	제목
MEDIUM	CVE-2026-19542	libc6	2.41-12+deb13u4		affected	glibc: Fix out-of-bounds array write in tdelete
MEDIUM	CVE-2026-5435	libc6	2.41-12+deb13u4		affected	glibc: glibc: Out-of-bounds write via TSIG record processing
MEDIUM	CVE-2026-6238	libc6	2.41-12+deb13u4		affected	glibc: glibc: Application crash or uninitialized memory read via crafted DNS response
MEDIUM	CVE-2026-6368	libc6	2.41-12+deb13u4		affected	glibc: glibc: Process abort due to invalid memory in wordexp
MEDIUM	CVE-2026-6791	libc6	2.41-12+deb13u4		affected	glibc: Glibc: Denial of Service via stack exhaustion during tilde expansion
MEDIUM	CVE-2026-77117	libc6	2.41-12+deb13u4		affected	glibc: Non-progress DoS in SHIFT_JISX0213 -&gt
MEDIUM	CVE-2026-80489	libc6	2.41-12+deb13u4		affected	glibc: Non-progress DoS in EUC_JISX0213 -> UCS-4 conversion state
MEDIUM	CVE-2026-89092	libc6	2.41-12+deb13u4		affected	glibc: glibc: nscd stack overflow leads to degraded DNS resolution
MEDIUM	CVE-2025-58436	libcups2t64	2.4.10-3+deb13u2		affected	cups: Slow client communication leads to a possible DoS attack
MEDIUM	CVE-2025-61915	libcups2t64	2.4.10-3+deb13u2		affected	CUPS: Local denial-of-service via cupsd.conf update and related issues
MEDIUM	CVE-2026-27447	libcups2t64	2.4.10-3+deb13u2		affected	cups: OpenPrinting CUPS: Authorization bypass via case-insensitive username comparison
MEDIUM	CVE-2026-34978	libcups2t64	2.4.10-3+deb13u2		affected	cups: OpenPrinting CUPS: Denial of Service via path traversal in RSS notifier
MEDIUM	CVE-2026-34979	libcups2t64	2.4.10-3+deb13u2		affected	cups: OpenPrinting CUPS: Denial of Service via heap-based buffer overflow in job attribute processing
MEDIUM	CVE-2026-34990	libcups2t64	2.4.10-3+deb13u2		affected	cups: OpenPrinting CUPS: Privilege escalation via arbitrary file overwrite due to coerced authentication
MEDIUM	CVE-2026-39314	libcups2t64	2.4.10-3+deb13u2		affected	cups: CUPS: Denial of Service via integer underflow in IPP attribute handling
MEDIUM	CVE-2026-39316	libcups2t64	2.4.10-3+deb13u2		affected	cups: CUPS: Denial of Service and potential arbitrary code execution via use-after-free vulnerability when deleting temporary printers.
MEDIUM	CVE-2026-41079	libcups2t64	2.4.10-3+deb13u2		affected	cups: CUPS: Information disclosure via crafted SNMP response
MEDIUM	CVE-2026-87875	libcups2t64	2.4.10-3+deb13u2		affected	cups: OpenPrinting CUPS: Heap out-of-bounds read in cupsUTF32ToUTF8() via missing source-length bound
MEDIUM	CVE-2025-66382	libexpat1	2.8.3-1~deb13u1		fix_deferred	libexpat: libexpat: Denial of service via crafted file processing
MEDIUM	CVE-2026-66046	libexpat1	2.8.3-1~deb13u1		affected	Expat through 2.8.3 contains a denial of service vulnerability caused ...
MEDIUM	CVE-2026-86469	libglib2.0-0t64	2.84.4-3~deb13u5		affected	glib2: TOCTOU Symlink Race in `G_FILE_CREATE_REPLACE_DESTINATION` Fallback Path
MEDIUM	CVE-2026-3184	liblastlog2-2	2.41.5-0+deb13u1		affected	util-linux: util-linux: Access control bypass due to improper hostname canonicalization

Severity	취약점 ID	패키지	설치 버전	수정 버전	상태	제목
MEDIUM	CVE-2026-3184	libmount1	2.41.5-0+deb13u1		affected	util-linux: util-linux: Access control bypass due to improper hostname canonicalization
MEDIUM	CVE-2026-13757	libp11-kit0	0.25.5-3		affected	p11-kit: Stack exhaustion via unbounded recursion in RPC attribute parsing
MEDIUM	CVE-2026-18938	libp11-kit0	0.25.5-3		affected	p11-kit: Integer overflow in RPC attribute-array length calculation can under-allocate nested attribute storage on 32 bit systems
MEDIUM	CVE-2026-54411	libpam-modules	1.7.0-5		affected	linux-pam: Plaintext password recovery via timing discrepancy in pam_userdb module
MEDIUM	CVE-2026-54411	libpam-modules-bin	1.7.0-5		affected	linux-pam: Plaintext password recovery via timing discrepancy in pam_userdb module
MEDIUM	CVE-2026-54411	libpam-runtime	1.7.0-5		affected	linux-pam: Plaintext password recovery via timing discrepancy in pam_userdb module
MEDIUM	CVE-2026-54411	libpam0g	1.7.0-5		affected	linux-pam: Plaintext password recovery via timing discrepancy in pam_userdb module
MEDIUM	CVE-2026-3184	libsmartcols1	2.41.5-0+deb13u1		affected	util-linux: util-linux: Access control bypass due to improper hostname canonicalization
MEDIUM	CVE-2026-39113	libsqlite3-0	3.46.1-7+deb13u2		affected	Buffer Overflow vulnerability in SQLite affected version source snapsh ...
MEDIUM	CVE-2026-50812	libsqlite3-0	3.46.1-7+deb13u2		affected	sqlite: SQLite: Denial of Service via malformed changeset in Session Extension
MEDIUM	CVE-2026-50813	libsqlite3-0	3.46.1-7+deb13u2		affected	sqlite: SQLite: Information disclosure via Session Extension changeset merge path
MEDIUM	CVE-2026-15059	libsystemd0	257.13-1~deb13u1		affected	systemd: systemd-oomd: Unprivileged users can terminate arbitrary processes via IPC API
MEDIUM	CVE-2026-15059	libudev1	257.13-1~deb13u1		affected	systemd: systemd-oomd: Unprivileged users can terminate arbitrary processes via IPC API
MEDIUM	CVE-2026-3184	libuuid1	2.41.5-0+deb13u1		affected	util-linux: util-linux: Access control bypass due to improper hostname canonicalization
MEDIUM	CVE-2026-86138	libxml2	2.12.7+dfsg+really2.9.14-2.1+deb13u3		affected	libxml2: libxml2: Arbitrary code execution via heap-based buffer overflow
MEDIUM	CVE-2026-86139	libxml2	2.12.7+dfsg+really2.9.14-2.1+deb13u3		affected	libxml2: libxml2: Integer overflow in xmlURIEscapeStr may lead to arbitrary code execution
MEDIUM	CVE-2026-86142	libxml2	2.12.7+dfsg+really2.9.14-2.1+deb13u3		affected	libxml2: libxml2: Heap-based buffer overflow in xmlXPtrEval due to xpointer length saturation
MEDIUM	CVE-2026-86143	libxml2	2.12.7+dfsg+really2.9.14-2.1+deb13u3		affected	libxml2: libxml2: Data integrity issues due to integer overflow in write callbacks

Severity	취약점 ID	패키지	설치 버전	수정 버전	상태	제목
MEDIUM	CVE-2026-86144	libxml2	2.12.7+dfsg+really2.9.14-2.1+deb13u3		affected	libxml2: libxml2: Information disclosure, SSRF, or denial of service due to improper parseFlags propagation.
MEDIUM	CVE-2026-3184	login	1:4.16.0-2+really2.41.5-0+deb13u1		affected	util-linux: util-linux: Access control bypass due to improper hostname canonicalization
MEDIUM	CVE-2026-3184	mount	2.41.5-0+deb13u1		affected	util-linux: util-linux: Access control bypass due to improper hostname canonicalization
MEDIUM	CVE-2026-15534	perl-base	5.40.1-6+deb13u1		fix_deferred	perl: Perl: Arbitrary code execution via out-of-bounds memory access in regular expression engine.
MEDIUM	CVE-2026-19487	perl-base	5.40.1-6+deb13u1		affected	perl: Perl: Incorrect regular expression matching can lead to wrong access or filtering decisions.
MEDIUM	CVE-2026-18477	tar	1.35+dfsg-3.1		affected	tar: tar: TOCTOU in incremental dumpdir 'X' rename handling allows restore path escape
MEDIUM	CVE-2026-18508	tar	1.35+dfsg-3.1		affected	tar: tar: --one-top-level hardlink targets not confined to top-level directory enabling arbitrary file overwrite
MEDIUM	CVE-2026-5704	tar	1.35+dfsg-3.1		affected	tar: tar: Hidden file injection via crafted archives
MEDIUM	CVE-2026-3184	util-linux	2.41.5-0+deb13u1		affected	util-linux: util-linux: Access control bypass due to improper hostname canonicalization
MEDIUM	CVE-2026-27171	zlib1g	1:1.3.dfsg+really1.3.1-1+b1		affected	zlib: zlib: Denial of Service via infinite loop in CRC32 combine functions
MEDIUM	CVE-2026-85091	zlib1g	1:1.3.dfsg+really1.3.1-1+b1		affected	zlib versions 1.3.1.2 through 1.3.2 contain a heap buffer overflow vul ...
LOW	CVE-2011-3374	apt	3.0.3		affected	It was found that apt-key in apt, all versions, do not correctly valid ...
LOW	TEMP-0841856-B18BAF	bash	5.2.37-2+b10		affected	[Privilege escalation possible to other user than root]
LOW	CVE-2022-0563	bsdutils	1:2.41.5-0+deb13u1		affected	util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled with libreadline
LOW	CVE-2017-18018	coreutils	9.7-3		affected	coreutils: race condition vulnerability in chown and chgrp
LOW	CVE-2025-5278	coreutils	9.7-3		affected	coreutils: Heap Buffer Under-Read in GNU Coreutils sort via Key Specification
LOW	CVE-2026-56391	coreutils	9.7-3		affected	coreutils: GNU coreutils uniq: Denial of Service and information disclosure via out-of-bounds read with multibyte input
LOW	CVE-2026-56392	coreutils	9.7-3		affected	coreutils: GNU coreutils unexpand: Denial of Service via crafted tab stop values
LOW	CVE-2026-53910	diffutils	1:3.10-4		affected	diffutils: heap-based buffer overflow due to multiple signed integer overflows in line-mapping calculations
LOW	CVE-2011-3374	libapt-pkg7.0	3.0.3		affected	It was found that apt-key in apt, all versions, do not correctly valid ...

Severity	취약점 ID	패키지	설치 버전	수정 버전	상태	제목
LOW	CVE-2026-56109	libasound2-data	1.2.14-1+deb13u1		affected	alsa-lib: ALSA library: Double-free vulnerability leading to memory corruption
LOW	CVE-2026-56109	libasound2t64	1.2.14-1+deb13u1		affected	alsa-lib: ALSA library: Double-free vulnerability leading to memory corruption
LOW	CVE-2022-0563	libblkid1	2.41.5-0+deb13u1		affected	util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled with libreadline
LOW	CVE-2010-4756	libc-bin	2.41-12+deb13u4		affected	glibc: glob implementation can cause excessive CPU and memory consumption due to crafted glob expressions
LOW	CVE-2018-20796	libc-bin	2.41-12+deb13u4		affected	glibc: uncontrolled recursion in function check_dst_limits_calc_pos_1 in posix/regexec.c
LOW	CVE-2019-1010022	libc-bin	2.41-12+deb13u4		affected	glibc: stack guard protection bypass
LOW	CVE-2019-1010023	libc-bin	2.41-12+deb13u4		affected	glibc: running ldd on malicious ELF leads to code execution because of wrong size computation
LOW	CVE-2019-1010024	libc-bin	2.41-12+deb13u4		affected	glibc: ASLR bypass using cache of thread stack and heap
LOW	CVE-2019-1010025	libc-bin	2.41-12+deb13u4		affected	glibc: information disclosure of heap addresses of pthread_created thread
LOW	CVE-2019-9192	libc-bin	2.41-12+deb13u4		affected	glibc: uncontrolled recursion in function check_dst_limits_calc_pos_1 in posix/regexec.c
LOW	CVE-2010-4756	libc6	2.41-12+deb13u4		affected	glibc: glob implementation can cause excessive CPU and memory consumption due to crafted glob expressions
LOW	CVE-2018-20796	libc6	2.41-12+deb13u4		affected	glibc: uncontrolled recursion in function check_dst_limits_calc_pos_1 in posix/regexec.c
LOW	CVE-2019-1010022	libc6	2.41-12+deb13u4		affected	glibc: stack guard protection bypass
LOW	CVE-2019-1010023	libc6	2.41-12+deb13u4		affected	glibc: running ldd on malicious ELF leads to code execution because of wrong size computation
LOW	CVE-2019-1010024	libc6	2.41-12+deb13u4		affected	glibc: ASLR bypass using cache of thread stack and heap
LOW	CVE-2019-1010025	libc6	2.41-12+deb13u4		affected	glibc: information disclosure of heap addresses of pthread_created thread
LOW	CVE-2019-9192	libc6	2.41-12+deb13u4		affected	glibc: uncontrolled recursion in function check_dst_limits_calc_pos_1 in posix/regexec.c
LOW	CVE-2017-7475	libcairo2	1.18.4-1+b1		will_not_fix	cairo: NULL pointer dereference with a crafted font file
LOW	CVE-2018-18064	libcairo2	1.18.4-1+b1		affected	cairo: Stack-based buffer overflow via parsing of crafted WebKitGTK+ document
LOW	CVE-2025-50422	libcairo2	1.18.4-1+b1		fix_deferred	poppler: Poppler crash on malformed input

Severity	취약점 ID	패키지	설치 버전	수정 버전	상태	제목
LOW	CVE-2014-8166	libcups2t64	2.4.10-3+deb13u2		affected	cups: code execution via unescape ANSI escape sequences
LOW	CVE-2026-87876	libcups2t64	2.4.10-3+deb13u2		affected	cups: OpenPrinting CUPS: Remaining case-insensitive username matching in scheduler side paths (CVE-2026-27447 follow-up)
LOW	CVE-2024-25260	libelf1t64	0.192-4		affected	elfutils: global-buffer-overflow exists in the function ebl_machine_flag_name in eblmachineflagname.c
LOW	CVE-2025-1352	libelf1t64	0.192-4		affected	elfutils: GNU elfutils eu-readelf libdw_alloc.c __libdw_thread_tail memory corruption
LOW	CVE-2025-1365	libelf1t64	0.192-4		affected	elfutils: GNU elfutils eu-readelf readelf.c process_symtab buffer overflow
LOW	CVE-2025-1371	libelf1t64	0.192-4		affected	elfutils: GNU elfutils eu-read readelf.c handle_dynamic_symtab null pointer dereference
LOW	CVE-2025-1372	libelf1t64	0.192-4		affected	elfutils: GNU elfutils eu-readelf readelf.c print_string_section buffer overflow
LOW	CVE-2025-1376	libelf1t64	0.192-4		affected	elfutils: GNU elfutils eu-strip elf_strptr.c elf_strptr denial of service
LOW	CVE-2025-1377	libelf1t64	0.192-4		affected	elfutils: GNU elfutils eu-strip strip.c gelf_getsymshndx denial of service
LOW	CVE-2023-45913	libgbm1	25.0.7-2+deb13u1		affected	Mesa v23.0.4 was discovered to contain a NULL pointer dereference via ...
LOW	CVE-2023-45919	libgbm1	25.0.7-2+deb13u1		affected	Mesa 23.0.4 was discovered to contain a buffer over-read in glXQuerySe ...
LOW	CVE-2023-45922	libgbm1	25.0.7-2+deb13u1		affected	glx_pbuffer.c in Mesa 23.0.4 was discovered to contain a segmentation ...
LOW	CVE-2023-45931	libgbm1	25.0.7-2+deb13u1		affected	Mesa 23.0.4 was discovered to contain a NULL pointer dereference in ch ...
LOW	CVE-2023-45924	libgl1	1.7.0-1+b2		affected	libglxproto.c in OpenGL libglvnd bb06db5a was discovered to contain a ...
LOW	CVE-2023-45913	libgl1-mesa-dri	25.0.7-2+deb13u1		affected	Mesa v23.0.4 was discovered to contain a NULL pointer dereference via ...
LOW	CVE-2023-45919	libgl1-mesa-dri	25.0.7-2+deb13u1		affected	Mesa 23.0.4 was discovered to contain a buffer over-read in glXQuerySe ...
LOW	CVE-2023-45922	libgl1-mesa-dri	25.0.7-2+deb13u1		affected	glx_pbuffer.c in Mesa 23.0.4 was discovered to contain a segmentation ...
LOW	CVE-2023-45931	libgl1-mesa-dri	25.0.7-2+deb13u1		affected	Mesa 23.0.4 was discovered to contain a NULL pointer dereference in ch ...
LOW	CVE-2012-0039	libglib2.0-0t64	2.84.4-3~deb13u5		affected	glib2: hash table collisions CPU usage DoS
LOW	CVE-2023-45924	libglvnd0	1.7.0-1+b2		affected	libglxproto.c in OpenGL libglvnd bb06db5a was discovered to contain a ...
LOW	CVE-2023-45913	libglx-mesa0	25.0.7-2+deb13u1		affected	Mesa v23.0.4 was discovered to contain a NULL pointer dereference via ...

Severity	취약점 ID	패키지	설치 버전	수정 버전	상태	제목
LOW	CVE-2023-45919	libglx-mesa0	25.0.7-2+deb13u1		affected	Mesa 23.0.4 was discovered to contain a buffer over-read in glXQuerySe ...
LOW	CVE-2023-45922	libglx-mesa0	25.0.7-2+deb13u1		affected	glx_pbuffer.c in Mesa 23.0.4 was discovered to contain a segmentation ...
LOW	CVE-2023-45931	libglx-mesa0	25.0.7-2+deb13u1		affected	Mesa 23.0.4 was discovered to contain a NULL pointer dereference in ch ...
LOW	CVE-2023-45924	libglx0	1.7.0-1+b2		affected	libglxproto.c in OpenGL libglvnd bb06db5a was discovered to contain a ...
LOW	CVE-2011-3389	libgnutls30t64	3.8.9-3+deb13u4		affected	HTTPS: block-wise chosen-plaintext attack against SSL/TLS (BEAST)
LOW	CVE-2018-5709	libgssapi-krb5-2	1.21.3-5+deb13u1		affected	krb5: integer overflow in dbentry->n_key_data in kadmin/dbutil/dump.c
LOW	CVE-2024-26458	libgssapi-krb5-2	1.21.3-5+deb13u1		affected	krb5: Memory leak at /krb5/src/lib/rpc/pmap_rmt.c
LOW	CVE-2024-26461	libgssapi-krb5-2	1.21.3-5+deb13u1		affected	krb5: Memory leak at /krb5/src/lib/gssapi/krb5/k5sealv3.c
LOW	CVE-2026-11850	libgssapi-krb5-2	1.21.3-5+deb13u1		affected	krb5: krb5: integer underflow in berval2tl_data() leads to heap out-of-bounds read
LOW	CVE-2018-5709	libk5crypto3	1.21.3-5+deb13u1		affected	krb5: integer overflow in dbentry->n_key_data in kadmin/dbutil/dump.c
LOW	CVE-2024-26458	libk5crypto3	1.21.3-5+deb13u1		affected	krb5: Memory leak at /krb5/src/lib/rpc/pmap_rmt.c
LOW	CVE-2024-26461	libk5crypto3	1.21.3-5+deb13u1		affected	krb5: Memory leak at /krb5/src/lib/gssapi/krb5/k5sealv3.c
LOW	CVE-2026-11850	libk5crypto3	1.21.3-5+deb13u1		affected	krb5: krb5: integer underflow in berval2tl_data() leads to heap out-of-bounds read
LOW	CVE-2018-5709	libkrb5-3	1.21.3-5+deb13u1		affected	krb5: integer overflow in dbentry->n_key_data in kadmin/dbutil/dump.c
LOW	CVE-2024-26458	libkrb5-3	1.21.3-5+deb13u1		affected	krb5: Memory leak at /krb5/src/lib/rpc/pmap_rmt.c
LOW	CVE-2024-26461	libkrb5-3	1.21.3-5+deb13u1		affected	krb5: Memory leak at /krb5/src/lib/gssapi/krb5/k5sealv3.c
LOW	CVE-2026-11850	libkrb5-3	1.21.3-5+deb13u1		affected	krb5: krb5: integer underflow in berval2tl_data() leads to heap out-of-bounds read
LOW	CVE-2018-5709	libkrb5support0	1.21.3-5+deb13u1		affected	krb5: integer overflow in dbentry->n_key_data in kadmin/dbutil/dump.c
LOW	CVE-2024-26458	libkrb5support0	1.21.3-5+deb13u1		affected	krb5: Memory leak at /krb5/src/lib/rpc/pmap_rmt.c
LOW	CVE-2024-26461	libkrb5support0	1.21.3-5+deb13u1		affected	krb5: Memory leak at /krb5/src/lib/gssapi/krb5/k5sealv3.c

Severity	취약점 ID	패키지	설치 버전	수정 버전	상태	제목
LOW	CVE-2026-11850	libkrb5support0	1.21.3-5+deb13u1		affected	krb5: krb5: integer underflow in berval2tl_data() leads to heap out-of-bounds read
LOW	CVE-2022-0563	liblastlog2-2	2.41.5-0+deb13u1		affected	util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled with libreadline
LOW	CVE-2024-7883	libllvm19	1:19.1.7-3+b1		will_not_fix	clang: CMSE secure state may leak from stack to floating-point registers
LOW	CVE-2026-13573	libllvm19	1:19.1.7-3+b1		affected	llvm: llvm: Denial of Service via stack-based buffer overflow in StringMap::insert
LOW	CVE-2026-13574	libllvm19	1:19.1.7-3+b1		affected	llvm: llvm-project: LLVM: Denial of service via heap-based buffer overflow in Bitcode File Handler
LOW	CVE-2022-0563	libmount1	2.41.5-0+deb13u1		affected	util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled with libreadline
LOW	CVE-2025-6141	libncursesw6	6.5+20250216-2		affected	gnu-ncurses: ncurses Stack Buffer Overflow
LOW	CVE-2017-11695	libnss3	2:3.110-1+deb13u4		affected	nss: Heap-buffer-overflow in alloc_segs
LOW	CVE-2017-11696	libnss3	2:3.110-1+deb13u4		affected	nss: Heap-buffer-overflow in __hash_open
LOW	CVE-2017-11697	libnss3	2:3.110-1+deb13u4		affected	nss: Floating Point Exception in __hash_open
LOW	CVE-2017-11698	libnss3	2:3.110-1+deb13u4		affected	nss: Heap-buffer-overflow in __get_page
LOW	CVE-2023-37769	libpixman-1-0	0.44.0-3		affected	stress-test master commit e4c878 was discovered to contain a FPE vulne ...
LOW	CVE-2021-4214	libpng16-16t64	1.6.48-1+deb13u5		affected	libpng: hardcoded value leads to heap-overflow
LOW	CVE-2026-3713	libpng16-16t64	1.6.48-1+deb13u5		affected	libpng: libpng: Heap-based buffer overflow in pnm2png allows information disclosure and denial of service
LOW	CVE-2022-0563	libsmartcols1	2.41.5-0+deb13u1		affected	util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled with libreadline
LOW	CVE-2021-45346	libsqlite3-0	3.46.1-7+deb13u2		affected	sqlite: crafted SQL query allows a malicious user to obtain sensitive information
LOW	CVE-2025-70873	libsqlite3-0	3.46.1-7+deb13u2		affected	sqlite: SQLite: Information Disclosure via Crafted ZIP File
LOW	CVE-2013-4392	libsystemd0	257.13-1~deb13u1		affected	systemd: TOCTOU race condition when updating file permissions and SELinux security contexts
LOW	CVE-2023-31437	libsystemd0	257.13-1~deb13u1		affected	An issue was discovered in systemd 253. An attacker can modify a seale ...
LOW	CVE-2023-31438	libsystemd0	257.13-1~deb13u1		affected	An issue was discovered in systemd 253. An attacker can truncate a sea ...
LOW	CVE-2023-31439	libsystemd0	257.13-1~deb13u1		affected	An issue was discovered in systemd 253. An attacker can modify the con ...

Severity	취약점 ID	패키지	설치 버전	수정 버전	상태	제목
LOW	CVE-2026-40228	libsystemd0	257.13-1~deb13u1		affected	systemd: systemd-journald: Unintended output to user terminals via logger command
LOW	CVE-2025-6141	libtinfo6	6.5+20250216-2		affected	gnu-ncurses: ncurses Stack Buffer Overflow
LOW	CVE-2013-4392	libudev1	257.13-1~deb13u1		affected	systemd: TOCTOU race condition when updating file permissions and SELinux security contexts
LOW	CVE-2023-31437	libudev1	257.13-1~deb13u1		affected	An issue was discovered in systemd 253. An attacker can modify a seale ...
LOW	CVE-2023-31438	libudev1	257.13-1~deb13u1		affected	An issue was discovered in systemd 253. An attacker can truncate a sea ...
LOW	CVE-2023-31439	libudev1	257.13-1~deb13u1		affected	An issue was discovered in systemd 253. An attacker can modify the con ...
LOW	CVE-2026-40228	libudev1	257.13-1~deb13u1		affected	systemd: systemd-journald: Unintended output to user terminals via logger command
LOW	CVE-2022-0563	libuuid1	2.41.5-0+deb13u1		affected	util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled with libreadline
LOW	CVE-2026-44950	libxfont2	1:2.0.6-1+deb13u1		affected	libxfonts2: libXfont2: Privilege Escalation via Heap Buffer Overflow in Font Server Client
LOW	CVE-2026-59679	libxfont2	1:2.0.6-1+deb13u1		affected	libxfont2: Font Server Client encoding[] Out-Of-Bounds Read/Write
LOW	CVE-2026-11979	libxml2	2.12.7+dfsg+really2.9.14-2.1+deb13u3		affected	libxml2: libxml2: Arbitrary code execution in xmlcatalog utility via buffer overflow
LOW	CVE-2026-86137	libxml2	2.12.7+dfsg+really2.9.14-2.1+deb13u3		affected	libxml2: libxml2: Denial of Service via out-of-bounds read in xmlFAParsePosCharGroup
LOW	CVE-2026-86141	libxml2	2.12.7+dfsg+really2.9.14-2.1+deb13u3		affected	libxml2: libxml2: Denial of Service due to NULL pointer dereference in xmlRegNewParserCtxt
LOW	CVE-2022-0563	login	1:4.16.0-2+really2.41.5-0+deb13u1		affected	util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled with libreadline
LOW	CVE-2007-5686	login.defs	1:4.17.4-2		affected	initscripts in rPath Linux 1 sets insecure permissions for the /var/lo ...
LOW	CVE-2024-56433	login.defs	1:4.17.4-2		affected	shadow-utils: Default subordinate ID configuration in /etc/login.defs could lead to compromise
LOW	TEMP-0628843-DBAD28	login.defs	1:4.17.4-2		affected	[more related to CVE-2005-4890]
LOW	CVE-2023-45913	mesa-libgallium	25.0.7-2+deb13u1		affected	Mesa v23.0.4 was discovered to contain a NULL pointer dereference via ...
LOW	CVE-2023-45919	mesa-libgallium	25.0.7-2+deb13u1		affected	Mesa 23.0.4 was discovered to contain a buffer over-read in glXQuerySe ...

Severity	취약점 ID	패키지	설치 버전	수정 버전	상태	제목
LOW	CVE-2023-45922	mesa-libgallium	25.0.7-2+deb13u1		affected	glx_pbuffer.c in Mesa 23.0.4 was discovered to contain a segmentation ...
LOW	CVE-2023-45931	mesa-libgallium	25.0.7-2+deb13u1		affected	Mesa 23.0.4 was discovered to contain a NULL pointer dereference in ch ...
LOW	CVE-2022-0563	mount	2.41.5-0+deb13u1		affected	util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled with libreadline
LOW	CVE-2025-6141	ncurses-base	6.5+20250216-2		affected	gnu-ncurses: ncurses Stack Buffer Overflow
LOW	CVE-2025-6141	ncurses-bin	6.5+20250216-2		affected	gnu-ncurses: ncurses Stack Buffer Overflow
LOW	CVE-2007-5686	passwd	1:4.17.4-2		affected	initscripts in rPath Linux 1 sets insecure permissions for the /var/lo ...
LOW	CVE-2024-56433	passwd	1:4.17.4-2		affected	shadow-utils: Default subordinate ID configuration in /etc/login.defs could lead to compromise
LOW	TEMP-0628843-DBAD28	passwd	1:4.17.4-2		affected	[more related to CVE-2005-4890]
LOW	CVE-2011-4116	perl-base	5.40.1-6+deb13u1		affected	perl: File:: Temp insecure temporary file handling
LOW	TEMP-0517018-A83CE6	sysvinit-utils	3.14-4		affected	[sysvinit: no-root option in expert installer exposes locally exploitable security flaw]
LOW	CVE-2005-2541	tar	1.35+dfsg-3.1		affected	tar: does not properly warn the user when extracting setuid or setgid files
LOW	TEMP-0290435-0B57B5	tar	1.35+dfsg-3.1		affected	[tar's rmt command may have undesired side effects]
LOW	CVE-2022-0563	util-linux	2.41.5-0+deb13u1		affected	util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled with libreadline
LOW	CVE-2018-15853	x11-xkb-utils	7.7+9		affected	libxkbcommon: xkbcomp: Endless recursion in xkbcomp/expr.c resulting in a crash
LOW	CVE-2018-15859	x11-xkb-utils	7.7+9		affected	libxkbcommon: xkbcomp: NULL pointer dereference when parsing invalid atoms in ExprResolveLhs resulting in a crash
LOW	CVE-2018-15861	x11-xkb-utils	7.7+9		affected	libxkbcommon: xkbcomp: NULL pointer dereference in ExprResolveLhs resulting in a crash
LOW	CVE-2018-15863	x11-xkb-utils	7.7+9		affected	libxkbcommon: xkbcomp: NULL pointer dereference in ResolveStateAndPredicate resulting in a crash
UNKNOWN	TEMP-1147318-639065	liblzma5	5.8.1-1+deb13u1		affected	[GHSA-5qpq-xqfv-j9pg: Invalid write if a decoder is reinitialized after allocation failure]

Python (lang-pkgs / python-pkg)

Severity	취약점 ID	패키지	설치 버전	수정 버전	상태	제목
HIGH	CVE-2026-81726	nltk	3.10.3		affected	nltk: NLTK: Unauthorized file access via path traversal in model-artifact APIs