PI Continuum — Trivy 이미지 점검 리포트

저장소	pi-continuum/pi-continuum
커밋	`133bfa633f663306e3a5264af3209137f8378e4c` · branch `main` · pi-continuum
이미지	`pi-continuum:133bfa6` · `sha256:4f87e2a9e101616638de9adf5826f13103634884cbf632af6e7c5b742c781e14`
빌드 시각	2026-09-15 23:03:07 KST
리포트 생성	2026-09-15 23:07:42 KST · Trivy 0.74.0

요약

Severity	취약점	비밀값	합계
CRITICAL	0	0	0
HIGH	44	0	44
MEDIUM	47	0	47
LOW	57	0	57
UNKNOWN	1	0	1
합계	149	0	149

대상

Target	Class	Type	취약점	비밀값
pi-continuum-133bfa6.tar (debian 13.6)	os-pkgs	debian	149	0
Node.js	lang-pkgs	node-pkg	0	0
Python	lang-pkgs	python-pkg	0	0

pi-continuum-133bfa6.tar (debian 13.6) (os-pkgs / debian)

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

Severity	취약점 ID	패키지	설치 버전	수정 버전	상태	제목
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-2026-76642	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
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

Severity	취약점 ID	패키지	설치 버전	수정 버전	상태	제목
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-2026-76642	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
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

Severity	취약점 ID	패키지	설치 버전	수정 버전	상태	제목
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
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-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

Severity	취약점 ID	패키지	설치 버전	수정 버전	상태	제목
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
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-2026-3184	liblastlog2-2	2.41.5-0+deb13u1		affected	util-linux: util-linux: Access control bypass due to improper hostname canonicalization
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-2026-54411	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-2026-50812	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

Severity	취약점 ID	패키지	설치 버전	수정 버전	상태	제목
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-2026-3184	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+b9		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

Severity	취약점 ID	패키지	설치 버전	수정 버전	상태	제목
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 ...
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-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-2022-0563	libmount1	2.41.5-0+deb13u1		affected	util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled with libreadline

Severity	취약점 ID	패키지	설치 버전	수정 버전	상태	제목
LOW	CVE-2025-6141	libncursesw6	6.5+20250216-2		affected	gnu-ncurses: ncurses Stack Buffer Overflow
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 ...
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-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-2022-0563	mount	2.41.5-0+deb13u1		affected	util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled with libreadline

Severity	취약점 ID	패키지	설치 버전	수정 버전	상태	제목
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
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]