

# PI Continuum — Trivy 이미지 점검 리포트

|        |                                                                                                |
|--------|------------------------------------------------------------------------------------------------|
| 저장소    | pi-continuum/pi-continuum                                                                      |
| 커밋     | 373bc2c3bd43ea0ddbd2d72e00a64d4d962316e2 · branch main · pi-continuum                          |
| 이미지    | pi-continuum:373bc2c · sha256:c0949c795dace8d302d8d8a9d2148bb264a2c7fd871796013703a7f981f6627b |
| 빌드 시각  | 2026-09-16 10:48:51 KST                                                                        |
| 리포트 생성 | 2026-09-16 10:52:43 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-373bc2c.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-373bc2c.tar (debian 13.6) (os-pkgs / debian)

| Severity | 취약점 ID                         | 패키지      | 설치 버전              | 수정 버전 | 상태       | 제목                                                                                            |
|----------|--------------------------------|----------|--------------------|-------|----------|-----------------------------------------------------------------------------------------------|
| HIGH     | <a href="#">CVE-2026-76642</a> | bsdutils | 1:2.41.5-0+deb13u1 |       | affected | util-linux: util-linux: failed external mount helper still runs privileged X-mount post-hooks |
| HIGH     | <a href="#">CVE-2026-78408</a> | 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     | <a href="#">CVE-2026-78409</a> | bsdutils      | 1:2.41.5-0+deb13u1 |       | affected | util-linux: util-linux: X-mount.subdir detached-tree resolution can escape via intermediate symlinks                |
| HIGH     | <a href="#">CVE-2026-78410</a> | 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     | <a href="#">CVE-2026-54369</a> | libacl1       | 2.3.2-2+b1         |       | affected | acl: Symlink traversal privilege escalation via libacl functions                                                    |
| HIGH     | <a href="#">CVE-2026-76642</a> | libblkid1     | 2.41.5-0+deb13u1   |       | affected | util-linux: util-linux: failed external mount helper still runs privileged X-mount post-hooks                       |
| HIGH     | <a href="#">CVE-2026-78408</a> | libblkid1     | 2.41.5-0+deb13u1   |       | affected | util-linux: util-linux: nsenter --join-cgroup leaks root cgroup migration authority                                 |
| HIGH     | <a href="#">CVE-2026-78409</a> | libblkid1     | 2.41.5-0+deb13u1   |       | affected | util-linux: util-linux: X-mount.subdir detached-tree resolution can escape via intermediate symlinks                |
| HIGH     | <a href="#">CVE-2026-78410</a> | 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     | <a href="#">CVE-2026-76642</a> | liblastlog2-2 | 2.41.5-0+deb13u1   |       | affected | util-linux: util-linux: failed external mount helper still runs privileged X-mount post-hooks                       |
| HIGH     | <a href="#">CVE-2026-78408</a> | liblastlog2-2 | 2.41.5-0+deb13u1   |       | affected | util-linux: util-linux: nsenter --join-cgroup leaks root cgroup migration authority                                 |
| HIGH     | <a href="#">CVE-2026-78409</a> | liblastlog2-2 | 2.41.5-0+deb13u1   |       | affected | util-linux: util-linux: X-mount.subdir detached-tree resolution can escape via intermediate symlinks                |
| HIGH     | <a href="#">CVE-2026-78410</a> | 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     | <a href="#">CVE-2026-76642</a> | libmount1     | 2.41.5-0+deb13u1   |       | affected | util-linux: util-linux: failed external mount helper still runs privileged X-mount post-hooks                       |
| HIGH     | <a href="#">CVE-2026-78408</a> | libmount1     | 2.41.5-0+deb13u1   |       | affected | util-linux: util-linux: nsenter --join-cgroup leaks root cgroup migration authority                                 |
| HIGH     | <a href="#">CVE-2026-78409</a> | libmount1     | 2.41.5-0+deb13u1   |       | affected | util-linux: util-linux: X-mount.subdir detached-tree resolution can escape via intermediate symlinks                |
| HIGH     | <a href="#">CVE-2026-78410</a> | 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     | <a href="#">CVE-2025-69720</a> | libncursesw6  | 6.5+20250216-2     |       | affected | ncurses: ncurses: Buffer overflow vulnerability may lead to arbitrary code execution.                               |
| HIGH     | <a href="#">CVE-2026-76642</a> | libsmartcols1 | 2.41.5-0+deb13u1   |       | affected | util-linux: util-linux: failed external mount helper still runs privileged X-mount post-hooks                       |
| HIGH     | <a href="#">CVE-2026-78408</a> | 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     | <a href="#">CVE-2026-78409</a> | libsmartcols1 | 2.41.5-0+deb13u1                  |       | affected | util-linux: util-linux: X-mount.subdir detached-tree resolution can escape via intermediate symlinks                |
| HIGH     | <a href="#">CVE-2026-78410</a> | 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     | <a href="#">CVE-2026-16742</a> | libsystemd0   | 257.13-1~deb13u1                  |       | affected | systemd: systemd-homed: Local privilege escalation via missing home-record signature verification                   |
| HIGH     | <a href="#">CVE-2025-69720</a> | libtinfo6     | 6.5+20250216-2                    |       | affected | ncurses: ncurses: Buffer overflow vulnerability may lead to arbitrary code execution.                               |
| HIGH     | <a href="#">CVE-2026-16742</a> | libudev1      | 257.13-1~deb13u1                  |       | affected | systemd: systemd-homed: Local privilege escalation via missing home-record signature verification                   |
| HIGH     | <a href="#">CVE-2026-76642</a> | libuuid1      | 2.41.5-0+deb13u1                  |       | affected | util-linux: util-linux: failed external mount helper still runs privileged X-mount post-hooks                       |
| HIGH     | <a href="#">CVE-2026-78408</a> | libuuid1      | 2.41.5-0+deb13u1                  |       | affected | util-linux: util-linux: nsenter --join-cgroup leaks root cgroup migration authority                                 |
| HIGH     | <a href="#">CVE-2026-78409</a> | libuuid1      | 2.41.5-0+deb13u1                  |       | affected | util-linux: util-linux: X-mount.subdir detached-tree resolution can escape via intermediate symlinks                |
| HIGH     | <a href="#">CVE-2026-78410</a> | 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     | <a href="#">CVE-2026-76642</a> | 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     | <a href="#">CVE-2026-78408</a> | 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     | <a href="#">CVE-2026-78409</a> | 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     | <a href="#">CVE-2026-78410</a> | 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     | <a href="#">CVE-2026-76642</a> | mount         | 2.41.5-0+deb13u1                  |       | affected | util-linux: util-linux: failed external mount helper still runs privileged X-mount post-hooks                       |
| HIGH     | <a href="#">CVE-2026-78408</a> | mount         | 2.41.5-0+deb13u1                  |       | affected | util-linux: util-linux: nsenter --join-cgroup leaks root cgroup migration authority                                 |
| HIGH     | <a href="#">CVE-2026-78409</a> | mount         | 2.41.5-0+deb13u1                  |       | affected | util-linux: util-linux: X-mount.subdir detached-tree resolution can escape via intermediate symlinks                |
| HIGH     | <a href="#">CVE-2026-78410</a> | 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     | <a href="#">CVE-2025-69720</a> | ncurses-base | 6.5+20250216-2     |       | affected     | ncurses: ncurses: Buffer overflow vulnerability may lead to arbitrary code execution.                               |
| HIGH     | <a href="#">CVE-2025-69720</a> | ncurses-bin  | 6.5+20250216-2     |       | affected     | ncurses: ncurses: Buffer overflow vulnerability may lead to arbitrary code execution.                               |
| HIGH     | <a href="#">CVE-2026-9538</a>  | 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     | <a href="#">CVE-2026-76642</a> | util-linux   | 2.41.5-0+deb13u1   |       | affected     | util-linux: util-linux: failed external mount helper still runs privileged X-mount post-hooks                       |
| HIGH     | <a href="#">CVE-2026-78408</a> | util-linux   | 2.41.5-0+deb13u1   |       | affected     | util-linux: util-linux: nsenter --join-cgroup leaks root cgroup migration authority                                 |
| HIGH     | <a href="#">CVE-2026-78409</a> | util-linux   | 2.41.5-0+deb13u1   |       | affected     | util-linux: util-linux: X-mount.subdir detached-tree resolution can escape via intermediate symlinks                |
| HIGH     | <a href="#">CVE-2026-78410</a> | 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   | <a href="#">CVE-2026-3184</a>  | bsdutils     | 1:2.41.5-0+deb13u1 |       | affected     | util-linux: util-linux: Access control bypass due to improper hostname canonicalization                             |
| MEDIUM   | <a href="#">CVE-2026-54370</a> | libacl1      | 2.3.2-2+b1         |       | affected     | acl: TOCTOU Symlink Traversal via getfacl/setfacl                                                                   |
| MEDIUM   | <a href="#">CVE-2026-54371</a> | libattr1     | 1:2.5.2-3          |       | affected     | attr: attr: Symlink Traversal Privilege Escalation via getfattr and setfattr                                        |
| MEDIUM   | <a href="#">CVE-2026-3184</a>  | libblkid1    | 2.41.5-0+deb13u1   |       | affected     | util-linux: util-linux: Access control bypass due to improper hostname canonicalization                             |
| MEDIUM   | <a href="#">CVE-2026-42250</a> | libbz2-1.0   | 1.0.8-6            |       | affected     | bzip2: bzip2: Denial of Service in bzip2recover via a specially crafted file                                        |
| MEDIUM   | <a href="#">CVE-2026-18374</a> | libc-bin     | 2.41-12+deb13u4    |       | affected     | glibc: glibc: Heap buffer overflow via attacker-controlled fopen mode string                                        |
| MEDIUM   | <a href="#">CVE-2026-19499</a> | libc-bin     | 2.41-12+deb13u4    |       | affected     | glibc: Buffer Overflow in strfmon right-justification padding                                                       |
| MEDIUM   | <a href="#">CVE-2026-19542</a> | libc-bin     | 2.41-12+deb13u4    |       | affected     | glibc: Fix out-of-bounds array write in tdelete                                                                     |
| MEDIUM   | <a href="#">CVE-2026-5435</a>  | libc-bin     | 2.41-12+deb13u4    |       | affected     | glibc: glibc: Out-of-bounds write via TSIG record processing                                                        |
| MEDIUM   | <a href="#">CVE-2026-6238</a>  | libc-bin     | 2.41-12+deb13u4    |       | affected     | glibc: glibc: Application crash or uninitialized memory read via crafted DNS response                               |
| MEDIUM   | <a href="#">CVE-2026-6368</a>  | libc-bin     | 2.41-12+deb13u4    |       | affected     | glibc: glibc: Process abort due to invalid memory in wordexp                                                        |
| MEDIUM   | <a href="#">CVE-2026-6791</a>  | libc-bin     | 2.41-12+deb13u4    |       | affected     | glibc: Glibc: Denial of Service via stack exhaustion during tilde expansion                                         |
| MEDIUM   | <a href="#">CVE-2026-77117</a> | libc-bin     | 2.41-12+deb13u4    |       | affected     | glibc: Non-progress DoS in SHIFT_JISX0213 -&gt;                                                                     |
| MEDIUM   | <a href="#">CVE-2026-80489</a> | 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   | <a href="#">CVE-2026-89092</a> | libc-bin           | 2.41-12+deb13u4  |       | affected | glibc: glibc: nscd stack overflow leads to degraded DNS resolution                      |
| MEDIUM   | <a href="#">CVE-2026-18374</a> | libc6              | 2.41-12+deb13u4  |       | affected | glibc: glibc: Heap buffer overflow via attacker-controlled fopen mode string            |
| MEDIUM   | <a href="#">CVE-2026-19499</a> | libc6              | 2.41-12+deb13u4  |       | affected | glibc: Buffer Overflow in strfmon right-justification padding                           |
| MEDIUM   | <a href="#">CVE-2026-19542</a> | libc6              | 2.41-12+deb13u4  |       | affected | glibc: Fix out-of-bounds array write in tdelete                                         |
| MEDIUM   | <a href="#">CVE-2026-5435</a>  | libc6              | 2.41-12+deb13u4  |       | affected | glibc: glibc: Out-of-bounds write via TSIG record processing                            |
| MEDIUM   | <a href="#">CVE-2026-6238</a>  | libc6              | 2.41-12+deb13u4  |       | affected | glibc: glibc: Application crash or uninitialized memory read via crafted DNS response   |
| MEDIUM   | <a href="#">CVE-2026-6368</a>  | libc6              | 2.41-12+deb13u4  |       | affected | glibc: glibc: Process abort due to invalid memory in wordexp                            |
| MEDIUM   | <a href="#">CVE-2026-6791</a>  | libc6              | 2.41-12+deb13u4  |       | affected | glibc: Glibc: Denial of Service via stack exhaustion during tilde expansion             |
| MEDIUM   | <a href="#">CVE-2026-77117</a> | libc6              | 2.41-12+deb13u4  |       | affected | glibc: Non-progress DoS in SHIFT_JISX0213 -&gt;                                         |
| MEDIUM   | <a href="#">CVE-2026-80489</a> | libc6              | 2.41-12+deb13u4  |       | affected | glibc: Non-progress DoS in EUC_JISX0213 -> UCS-4 conversion state                       |
| MEDIUM   | <a href="#">CVE-2026-89092</a> | libc6              | 2.41-12+deb13u4  |       | affected | glibc: glibc: nscd stack overflow leads to degraded DNS resolution                      |
| MEDIUM   | <a href="#">CVE-2026-3184</a>  | libblastlog2-2     | 2.41.5-0+deb13u1 |       | affected | util-linux: util-linux: Access control bypass due to improper hostname canonicalization |
| MEDIUM   | <a href="#">CVE-2026-3184</a>  | libmount1          | 2.41.5-0+deb13u1 |       | affected | util-linux: util-linux: Access control bypass due to improper hostname canonicalization |
| MEDIUM   | <a href="#">CVE-2026-54411</a> | libpam-modules     | 1.7.0-5          |       | affected | linux-pam: Plaintext password recovery via timing discrepancy in pam_userdb module      |
| MEDIUM   | <a href="#">CVE-2026-54411</a> | libpam-modules-bin | 1.7.0-5          |       | affected | linux-pam: Plaintext password recovery via timing discrepancy in pam_userdb module      |
| MEDIUM   | <a href="#">CVE-2026-54411</a> | libpam-runtime     | 1.7.0-5          |       | affected | linux-pam: Plaintext password recovery via timing discrepancy in pam_userdb module      |
| MEDIUM   | <a href="#">CVE-2026-54411</a> | libpam0g           | 1.7.0-5          |       | affected | linux-pam: Plaintext password recovery via timing discrepancy in pam_userdb module      |
| MEDIUM   | <a href="#">CVE-2026-3184</a>  | libsmartcols1      | 2.41.5-0+deb13u1 |       | affected | util-linux: util-linux: Access control bypass due to improper hostname canonicalization |
| MEDIUM   | <a href="#">CVE-2026-50812</a> | sqlite3-0          | 3.46.1-7+deb13u2 |       | affected | sqlite: SQLite: Denial of Service via malformed changeset in Session Extension          |
| MEDIUM   | <a href="#">CVE-2026-50813</a> | sqlite3-0          | 3.46.1-7+deb13u2 |       | affected | sqlite: SQLite: Information disclosure via Session Extension changeset merge path       |
| MEDIUM   | <a href="#">CVE-2026-15059</a> | 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   | <a href="#">CVE-2026-15059</a>      | libudev1   | 257.13-1~deb13u1                  |       | affected     | systemd: systemd-oomd: Unprivileged users can terminate arbitrary processes via IPC API                                 |
| MEDIUM   | <a href="#">CVE-2026-3184</a>       | libuuid1   | 2.41.5-0+deb13u1                  |       | affected     | util-linux: util-linux: Access control bypass due to improper hostname canonicalization                                 |
| MEDIUM   | <a href="#">CVE-2026-3184</a>       | 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   | <a href="#">CVE-2026-3184</a>       | mount      | 2.41.5-0+deb13u1                  |       | affected     | util-linux: util-linux: Access control bypass due to improper hostname canonicalization                                 |
| MEDIUM   | <a href="#">CVE-2026-15534</a>      | 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   | <a href="#">CVE-2026-19487</a>      | perl-base  | 5.40.1-6+deb13u1                  |       | affected     | perl: Perl: Incorrect regular expression matching can lead to wrong access or filtering decisions.                      |
| MEDIUM   | <a href="#">CVE-2026-18477</a>      | tar        | 1.35+dfsg-3.1                     |       | affected     | tar: tar: TOCTOU in incremental dumpdir 'X' rename handling allows restore path escape                                  |
| MEDIUM   | <a href="#">CVE-2026-18508</a>      | 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   | <a href="#">CVE-2026-5704</a>       | tar        | 1.35+dfsg-3.1                     |       | affected     | tar: tar: Hidden file injection via crafted archives                                                                    |
| MEDIUM   | <a href="#">CVE-2026-3184</a>       | util-linux | 2.41.5-0+deb13u1                  |       | affected     | util-linux: util-linux: Access control bypass due to improper hostname canonicalization                                 |
| MEDIUM   | <a href="#">CVE-2026-27171</a>      | zlib1g     | 1:1.3.dfsg+really1.3.1-1+b1       |       | affected     | zlib: zlib: Denial of Service via infinite loop in CRC32 combine functions                                              |
| MEDIUM   | <a href="#">CVE-2026-85091</a>      | 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      | <a href="#">CVE-2011-3374</a>       | apt        | 3.0.3                             |       | affected     | It was found that apt-key in apt, all versions, do not correctly valid ...                                              |
| LOW      | <a href="#">TEMP-0841856-B18BAF</a> | bash       | 5.2.37-2+b9                       |       | affected     | [Privilege escalation possible to other user than root]                                                                 |
| LOW      | <a href="#">CVE-2022-0563</a>       | bsdutils   | 1:2.41.5-0+deb13u1                |       | affected     | util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled with libreadline                       |
| LOW      | <a href="#">CVE-2017-18018</a>      | coreutils  | 9.7-3                             |       | affected     | coreutils: race condition vulnerability in chown and chgrp                                                              |
| LOW      | <a href="#">CVE-2025-5278</a>       | coreutils  | 9.7-3                             |       | affected     | coreutils: Heap Buffer Under-Read in GNU Coreutils sort via Key Specification                                           |
| LOW      | <a href="#">CVE-2026-56391</a>      | coreutils  | 9.7-3                             |       | affected     | coreutils: GNU coreutils uniq: Denial of Service and information disclosure via out-of-bounds read with multibyte input |
| LOW      | <a href="#">CVE-2026-56392</a>      | 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      | <a href="#">CVE-2026-53910</a>   | diffutils      | 1:3.10-4         |       | affected | diffutils: heap-based buffer overflow due to multiple signed integer overflows in line-mapping calculations |
| LOW      | <a href="#">CVE-2011-3374</a>    | libapt-pkg7.0  | 3.0.3            |       | affected | It was found that apt-key in apt, all versions, do not correctly valid ...                                  |
| LOW      | <a href="#">CVE-2022-0563</a>    | libblkid1      | 2.41.5-0+deb13u1 |       | affected | util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled with libreadline           |
| LOW      | <a href="#">CVE-2010-4756</a>    | libc-bin       | 2.41-12+deb13u4  |       | affected | glibc: glob implementation can cause excessive CPU and memory consumption due to crafted glob expressions   |
| LOW      | <a href="#">CVE-2018-20796</a>   | libc-bin       | 2.41-12+deb13u4  |       | affected | glibc: uncontrolled recursion in function check_dst_limits_calc_pos_1 in posix/regexec.c                    |
| LOW      | <a href="#">CVE-2019-1010022</a> | libc-bin       | 2.41-12+deb13u4  |       | affected | glibc: stack guard protection bypass                                                                        |
| LOW      | <a href="#">CVE-2019-1010023</a> | libc-bin       | 2.41-12+deb13u4  |       | affected | glibc: running ldd on malicious ELF leads to code execution because of wrong size computation               |
| LOW      | <a href="#">CVE-2019-1010024</a> | libc-bin       | 2.41-12+deb13u4  |       | affected | glibc: ASLR bypass using cache of thread stack and heap                                                     |
| LOW      | <a href="#">CVE-2019-1010025</a> | libc-bin       | 2.41-12+deb13u4  |       | affected | glibc: information disclosure of heap addresses of pthread_created thread                                   |
| LOW      | <a href="#">CVE-2019-9192</a>    | libc-bin       | 2.41-12+deb13u4  |       | affected | glibc: uncontrolled recursion in function check_dst_limits_calc_pos_1 in posix/regexec.c                    |
| LOW      | <a href="#">CVE-2010-4756</a>    | libc6          | 2.41-12+deb13u4  |       | affected | glibc: glob implementation can cause excessive CPU and memory consumption due to crafted glob expressions   |
| LOW      | <a href="#">CVE-2018-20796</a>   | libc6          | 2.41-12+deb13u4  |       | affected | glibc: uncontrolled recursion in function check_dst_limits_calc_pos_1 in posix/regexec.c                    |
| LOW      | <a href="#">CVE-2019-1010022</a> | libc6          | 2.41-12+deb13u4  |       | affected | glibc: stack guard protection bypass                                                                        |
| LOW      | <a href="#">CVE-2019-1010023</a> | libc6          | 2.41-12+deb13u4  |       | affected | glibc: running ldd on malicious ELF leads to code execution because of wrong size computation               |
| LOW      | <a href="#">CVE-2019-1010024</a> | libc6          | 2.41-12+deb13u4  |       | affected | glibc: ASLR bypass using cache of thread stack and heap                                                     |
| LOW      | <a href="#">CVE-2019-1010025</a> | libc6          | 2.41-12+deb13u4  |       | affected | glibc: information disclosure of heap addresses of pthread_created thread                                   |
| LOW      | <a href="#">CVE-2019-9192</a>    | libc6          | 2.41-12+deb13u4  |       | affected | glibc: uncontrolled recursion in function check_dst_limits_calc_pos_1 in posix/regexec.c                    |
| LOW      | <a href="#">CVE-2022-0563</a>    | libblastlog2-2 | 2.41.5-0+deb13u1 |       | affected | util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled with libreadline           |
| LOW      | <a href="#">CVE-2022-0563</a>    | 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      | <a href="#">CVE-2025-6141</a>       | libncursesw6  | 6.5+20250216-2                    |       | affected | gnu-ncurses: ncurses Stack Buffer Overflow                                                        |
| LOW      | <a href="#">CVE-2022-0563</a>       | libsmartcols1 | 2.41.5-0+deb13u1                  |       | affected | util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled with libreadline |
| LOW      | <a href="#">CVE-2021-45346</a>      | libsqlite3-0  | 3.46.1-7+deb13u2                  |       | affected | sqlite: crafted SQL query allows a malicious user to obtain sensitive information                 |
| LOW      | <a href="#">CVE-2025-70873</a>      | libsqlite3-0  | 3.46.1-7+deb13u2                  |       | affected | sqlite: SQLite: Information Disclosure via Crafted ZIP File                                       |
| LOW      | <a href="#">CVE-2013-4392</a>       | libsystemd0   | 257.13-1~deb13u1                  |       | affected | systemd: TOCTOU race condition when updating file permissions and SELinux security contexts       |
| LOW      | <a href="#">CVE-2023-31437</a>      | libsystemd0   | 257.13-1~deb13u1                  |       | affected | An issue was discovered in systemd 253. An attacker can modify a seale ...                        |
| LOW      | <a href="#">CVE-2023-31438</a>      | libsystemd0   | 257.13-1~deb13u1                  |       | affected | An issue was discovered in systemd 253. An attacker can truncate a sea ...                        |
| LOW      | <a href="#">CVE-2023-31439</a>      | libsystemd0   | 257.13-1~deb13u1                  |       | affected | An issue was discovered in systemd 253. An attacker can modify the con ...                        |
| LOW      | <a href="#">CVE-2026-40228</a>      | libsystemd0   | 257.13-1~deb13u1                  |       | affected | systemd: systemd-journald: Unintended output to user terminals via logger command                 |
| LOW      | <a href="#">CVE-2025-6141</a>       | libtinfo6     | 6.5+20250216-2                    |       | affected | gnu-ncurses: ncurses Stack Buffer Overflow                                                        |
| LOW      | <a href="#">CVE-2013-4392</a>       | libudev1      | 257.13-1~deb13u1                  |       | affected | systemd: TOCTOU race condition when updating file permissions and SELinux security contexts       |
| LOW      | <a href="#">CVE-2023-31437</a>      | libudev1      | 257.13-1~deb13u1                  |       | affected | An issue was discovered in systemd 253. An attacker can modify a seale ...                        |
| LOW      | <a href="#">CVE-2023-31438</a>      | libudev1      | 257.13-1~deb13u1                  |       | affected | An issue was discovered in systemd 253. An attacker can truncate a sea ...                        |
| LOW      | <a href="#">CVE-2023-31439</a>      | libudev1      | 257.13-1~deb13u1                  |       | affected | An issue was discovered in systemd 253. An attacker can modify the con ...                        |
| LOW      | <a href="#">CVE-2026-40228</a>      | libudev1      | 257.13-1~deb13u1                  |       | affected | systemd: systemd-journald: Unintended output to user terminals via logger command                 |
| LOW      | <a href="#">CVE-2022-0563</a>       | libuuid1      | 2.41.5-0+deb13u1                  |       | affected | util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled with libreadline |
| LOW      | <a href="#">CVE-2022-0563</a>       | 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      | <a href="#">CVE-2007-5686</a>       | login.defs    | 1:4.17.4-2                        |       | affected | initscripts in rPath Linux 1 sets insecure permissions for the /var/lo ...                        |
| LOW      | <a href="#">CVE-2024-56433</a>      | login.defs    | 1:4.17.4-2                        |       | affected | shadow-utils: Default subordinate ID configuration in /etc/login.defs could lead to compromise    |
| LOW      | <a href="#">TEMP-0628843-DBAD28</a> | login.defs    | 1:4.17.4-2                        |       | affected | [more related to CVE-2005-4890]                                                                   |
| LOW      | <a href="#">CVE-2022-0563</a>       | 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      | <a href="#">CVE-2025-6141</a>       | ncurses-base   | 6.5+20250216-2   |       | affected | gnu-ncurses: ncurses Stack Buffer Overflow                                                        |
| LOW      | <a href="#">CVE-2025-6141</a>       | ncurses-bin    | 6.5+20250216-2   |       | affected | gnu-ncurses: ncurses Stack Buffer Overflow                                                        |
| LOW      | <a href="#">CVE-2007-5686</a>       | passwd         | 1:4.17.4-2       |       | affected | initscripts in rPath Linux 1 sets insecure permissions for the /var/lo ...                        |
| LOW      | <a href="#">CVE-2024-56433</a>      | passwd         | 1:4.17.4-2       |       | affected | shadow-utils: Default subordinate ID configuration in /etc/login.defs could lead to compromise    |
| LOW      | <a href="#">TEMP-0628843-DBAD28</a> | passwd         | 1:4.17.4-2       |       | affected | [more related to CVE-2005-4890]                                                                   |
| LOW      | <a href="#">CVE-2011-4116</a>       | perl-base      | 5.40.1-6+deb13u1 |       | affected | perl: File:: Temp insecure temporary file handling                                                |
| LOW      | <a href="#">TEMP-0517018-A83CE6</a> | sysvinit-utils | 3.14-4           |       | affected | [sysvinit: no-root option in expert installer exposes locally exploitable security flaw]          |
| LOW      | <a href="#">CVE-2005-2541</a>       | tar            | 1.35+dfsg-3.1    |       | affected | tar: does not properly warn the user when extracting setuid or setgid files                       |
| LOW      | <a href="#">TEMP-0290435-0B57B5</a> | tar            | 1.35+dfsg-3.1    |       | affected | [tar's rmt command may have undesired side effects]                                               |
| LOW      | <a href="#">CVE-2022-0563</a>       | util-linux     | 2.41.5-0+deb13u1 |       | affected | util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled with libreadline |
| UNKNOWN  | <a href="#">TEMP-1147318-639065</a> | liblzma5       | 5.8.1-1+deb13u1  |       | affected | [GHSA-5qpq-xqfv-j9pg: Invalid write if a decoder is reinitialized after allocation failure]       |