Trivy Vulnerability Scan Report

Image: nginx

Scan Time: 2025-04-05T16:09:39Z

Vulnerability Severity Summary

Severity	Count
CRITICAL	2
HIGH	14
MEDIUM	44
LOW	100

Sample Vulnerabilities

It was found that apt-key in apt, all versions, do not correctly valid ... [LOW]
CVE: CVE-2011-3374
It was found that apt-key in apt, all versions, do not correctly validate gpg keys with the master keyring, leading to a potential man-in-the-middle attack.
Fix Available: %!s(<nil>)

[Privilege escalation possible to other user than root] [LOW]
CVE: TEMP-0841856-B18BAF
%!s(<nil>)
Fix Available: %!s(<nil>)

util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled with libreadline [LOW]
CVE: CVE-2022-0563
A flaw was found in the util-linux chfn and chsh utilities when compiled with Readline support. The Readline library uses an "INPUTRC" environment variable to get a path to the library config file. When the library cannot parse the specified file, it prints an error message containing data from the file. This flaw allows an unprivileged user to read root-owned files, potentially leading to privilege escalation. This flaw affects util-linux versions prior to 2.37.4.
Fix Available: %!s(<nil>)

coreutils: Non-privileged session can escape to the parent session in chroot [LOW]
CVE: CVE-2016-2781
chroot in GNU coreutils, when used with --userspec, allows local users to escape to the parent session via a crafted TIOCSTI ioctl call, which pushes characters to the terminal's input buffer.
Fix Available: %!s(<nil>)

coreutils: race condition vulnerability in chown and chgrp [LOW]
CVE: CVE-2017-18018

In GNU Coreutils through 8.29, chown-core.c in chown and chgrp does not prevent replacement of a plain file with a symlink during use of the POSIX "-R -L" options, which allows local users to modify the ownership of arbitrary files by leveraging a race condition.

Fix Available: %!s(<nil>)