# Trivy Vulnerability Scan Report

Image: node:lts

Scan Time: 2025-04-13T14:36:59Z

## Vulnerability Severity Summary

| Severity | Count |
|---|---|
| CRITICAL | 5 |
| HIGH | 98 |
| MEDIUM | 542 |
| LOW | 670 |

## 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>)

**binutils: Memory leak with the C++ symbol demangler routine in libiberty [LOW]**
CVE: CVE-2017-13716
The C++ symbol demangler routine in cplus-dem.c in libiberty, as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (excessive memory allocation and application crash) via a crafted file, as demonstrated by a call from the Binary File Descriptor (BFD) library (aka libbfd).
Fix Available: %!s(<nil>)

**libiberty: Integer overflow in demangle_template() function [LOW]**
CVE: CVE-2018-20673
The demangle_template function in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.31.1, contains an integer overflow vulnerability (for "Create an array for saving the template argument values") that can trigger a heap-based buffer overflow, as demonstrated by nm.
Fix Available: %!s(<nil>)

**libiberty: heap-based buffer over-read in d_expression_1 [LOW]**
CVE: CVE-2018-20712
A heap-based buffer over-read exists in the function d_expression_1 in cp-demangle.c in GNU libiberty, as

distributed in GNU Binutils 2.31.1. A crafted input can cause segmentation faults, leading to denial-of-service, as demonstrated by c++filt.

Fix Available: %!s(<nil>)