

OpenSSF Scorecard

Do we need to improve our security practices?

Marius Brehler

What is OpenSSF Scorecard?



- Automated tool created by the Open Source Security Foundation (OpenSSF)
- Helps consumers of open source software to assess whether their dependencies are safe
- Helps maintainers to improve security best practices

**This work is not affiliated with or otherwise sponsored by the OpenSSF.
OpenSSF and the OpenSSF logo design are trademarks of The Linux Foundation.**

OpenSSF Scorecard @ LLVM

- Scorecard action and badge added on Nov 1, 2023 with PR [#69933](#)
- Action to run checks is executed once a day
- LLVM's scorecard report is available at <https://securityscorecards.dev/viewer/?uri=github.com/llvm/llvm-project>

README Code of conduct License Security

The LLVM Compiler Infrastructure

openssf scorecard 5.6 openssf best practices in progress 88% Build and Test libc++ passing

Welcome to the LLVM project!

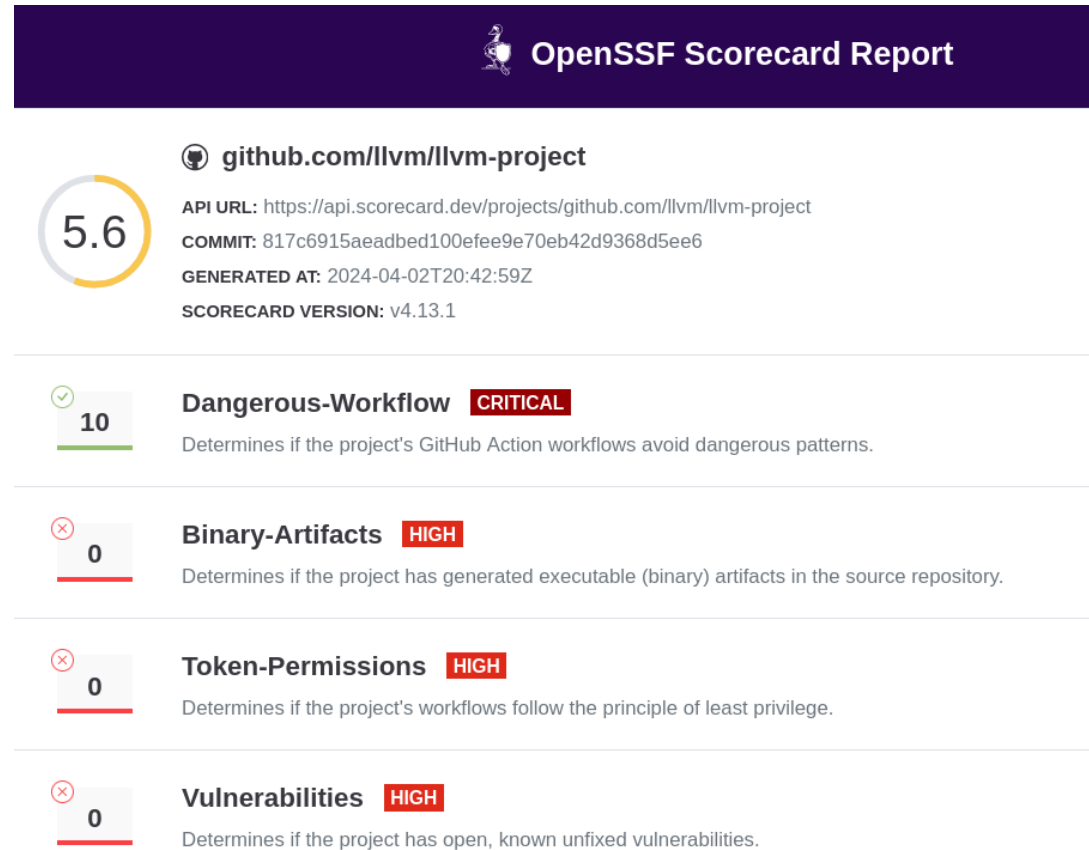
This repository contains the source code for LLVM, a toolkit for the construction of highly optimized compilers, optimizers, and run-time environments.

The LLVM project has multiple components. The core of the project is itself called "LLVM". This contains all of the tools, libraries, and header files needed to process intermediate representations and convert them into object files. Tools include an assembler, disassembler, bitcode analyzer, and bitcode optimizer.

C-like languages use the [Clang](#) frontend. This component compiles C, C++, Objective-C, and Objective-C++ code into LLVM bitcode -- and from there into object files, using LLVM.

Other components include: the [libc++ C++ standard library](#), the [LLD linker](#), and more.

OpenSSF Scorecard Report



- The report covers 18 Scorecard checks
- The checks are assigned to the risk levels Low, Medium, High, and Critical
- Checks with high risk level and low score currently are
 - Binary-Artifacts
 - Branch-Protection
 - Code-Review
 - Token Permissions
 - Vulnerabilities

Code Scanning Alerts

llvm / llvm-project

<> Code Issues 5k+ Pull requests 2k Actions **Security 60** Insights

Overview

Reporting

Policy

Advisories

Vulnerability alerts

Dependabot

Code scanning 60

Code scanning

All tools are working as expected Tools 1 + Add tool

is:open branch:main

60 Open ✓ 1,070 Closed

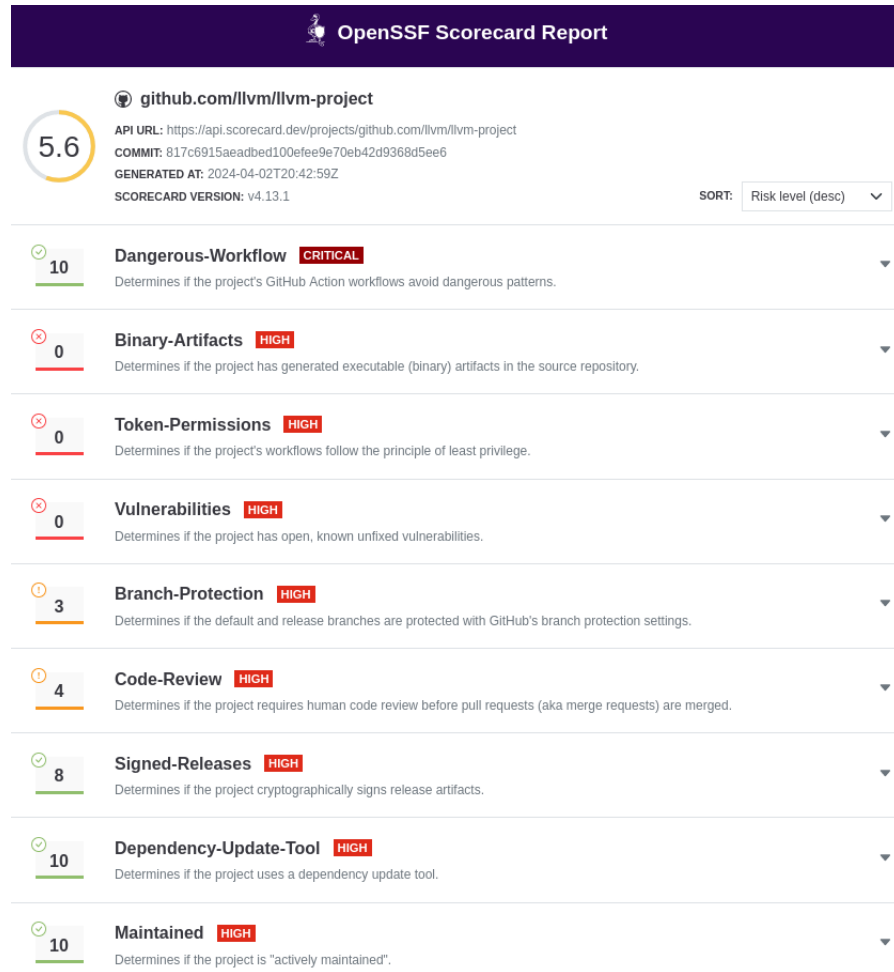
Tool Branch Rule Severity Sort

- Branch-Protection** (High) main
#1095 opened last week • Detected by Scorecard in no file associated with ...1
- Vulnerabilities** (High) main
#1130 opened last week • Detected by Scorecard in no file associated with ...1
- Code-Review** (High) main
#1042 opened 6 months ago • Detected by Scorecard in no file associated with ...1
- Token-Permissions** (High) main
#1076 opened 3 months ago • Detected by Scorecard in .github/workflows/release-tasks.yml:4
- Token-Permissions** (High) main
#1075 opened 3 months ago • Detected by Scorecard in .github/workflows/release-doxygen.yml:34

60 open and 1,070 closed alerts

Rule (w. Severity High)	Open (Closed) Alerts
Branch-Protection	1
Vulnerabilities	1
Code-Review	1
Token-Permissions	5 (5)
Binary-Artifacts	48 (962)

Do we need to improve our security practices?



- Yes, but not all scores seem relevant
 - *Open Source Security Podcast* with Kurt Seifried and Josh Bressers [Episode 293](#) – Scoring OpenSSF Security Scoring
 - E.g. (Branch-Protection) *Warn: codeowner review is not required on branch 'main'* can be ignored
- Scores for Branch-Protection and Code-Review could be *improved* but would drastically change established practices