Fraunhofer Institute for Material
Flow and Logistics IML

OpenSSF Scorecard

Do we need to improve our security practices?

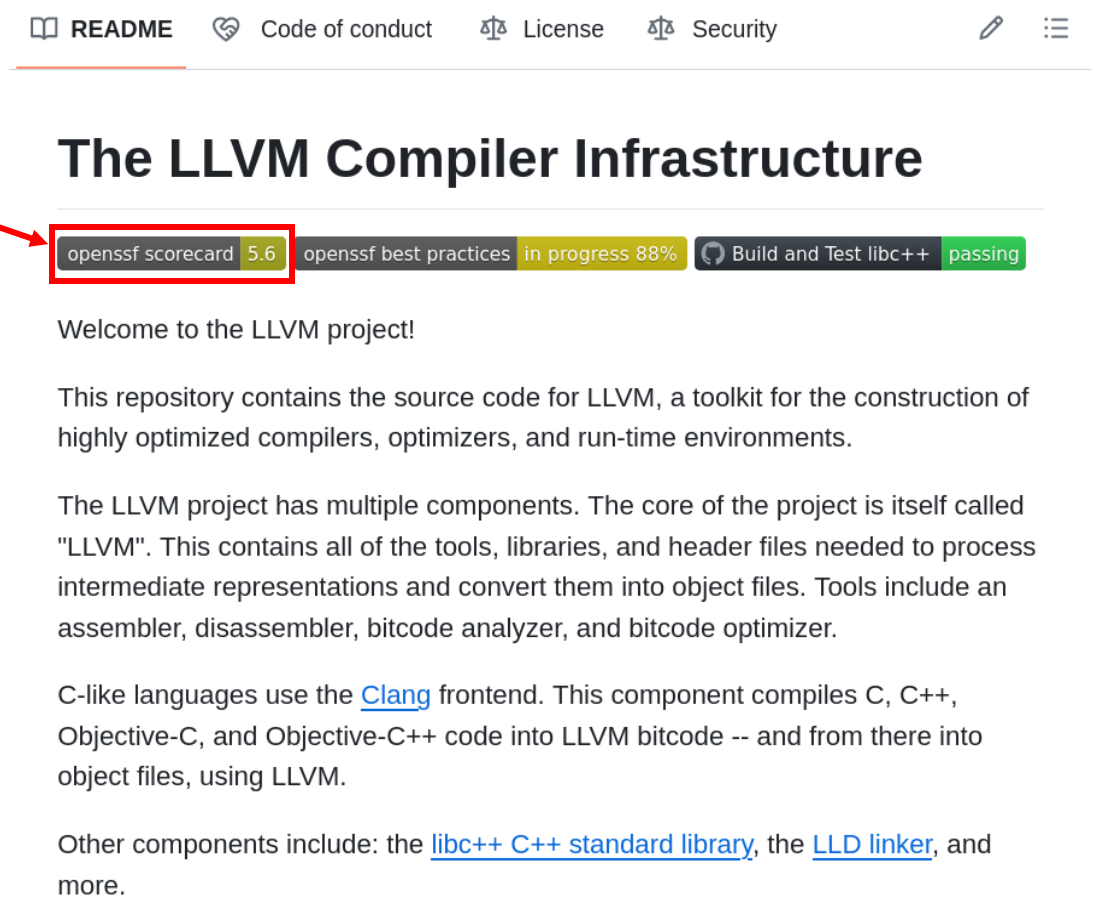
Marius Brehler

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

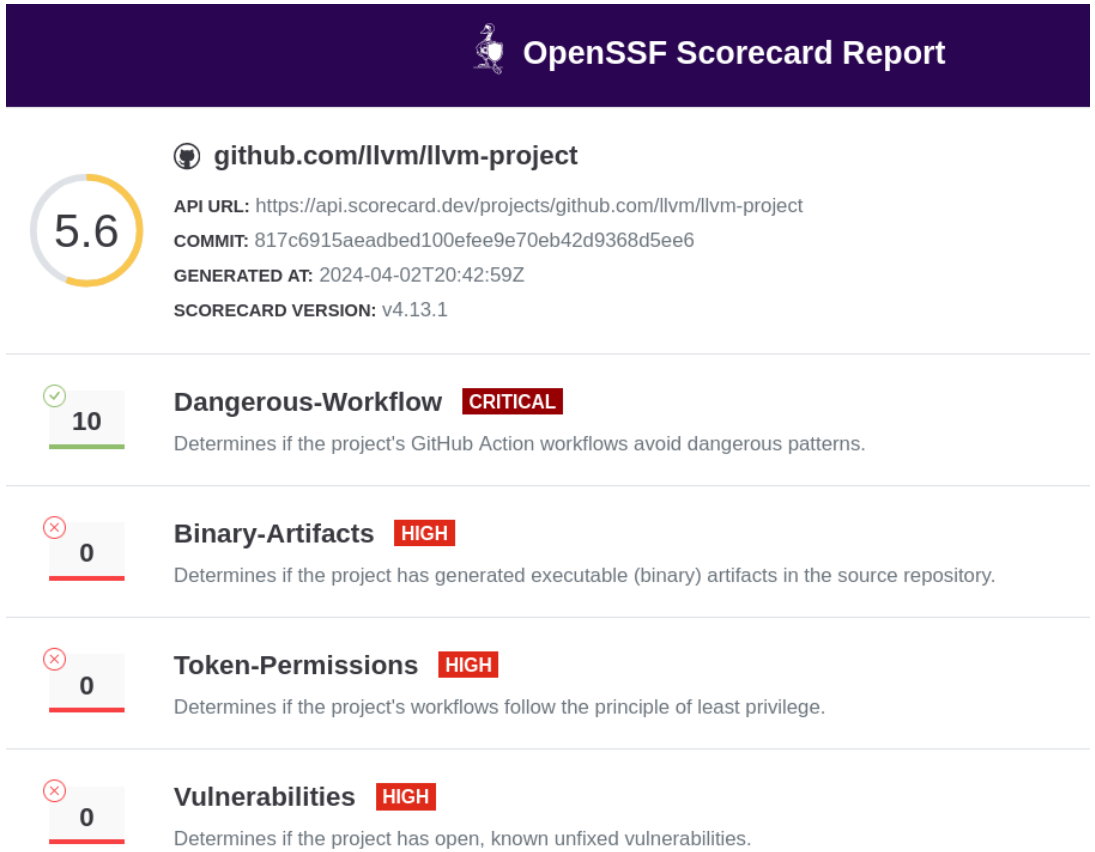
OpenSSF Scorecard @ LLVM

- 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



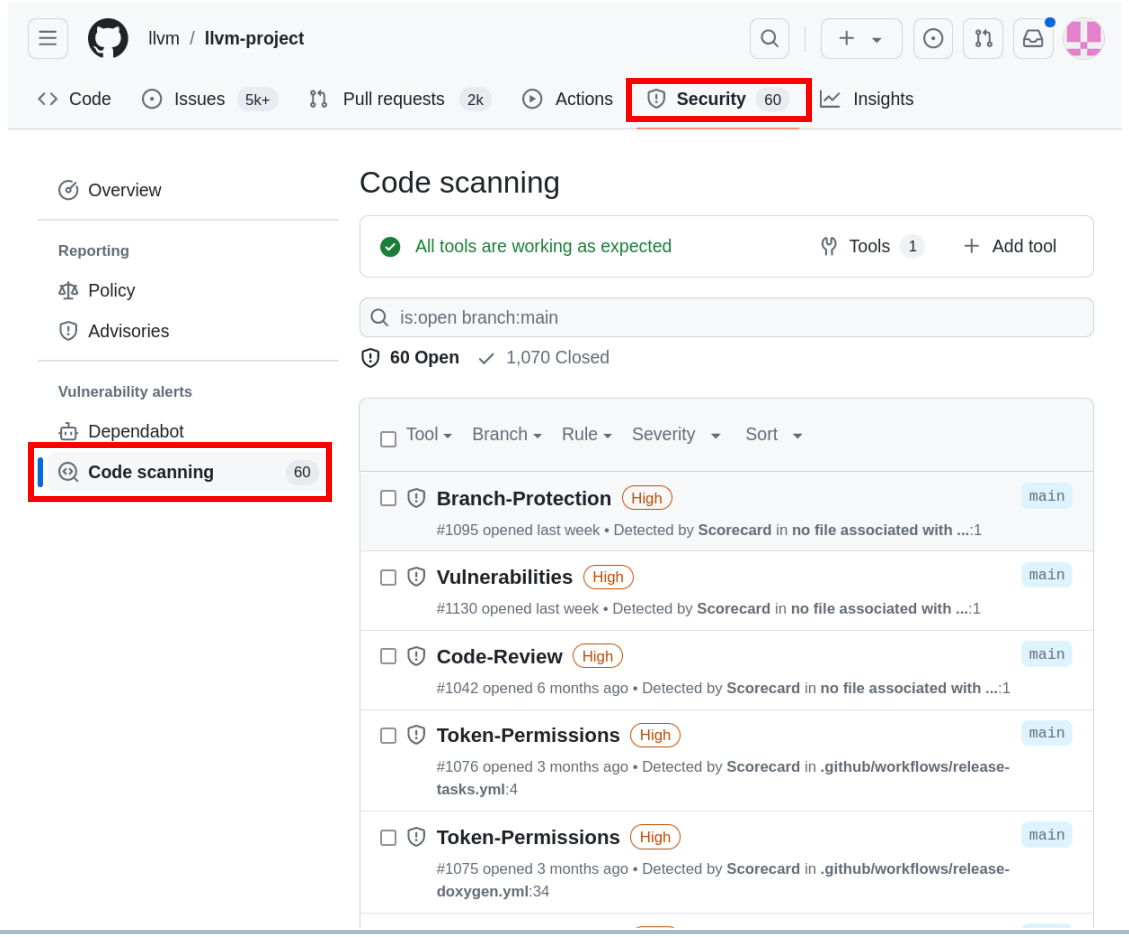
Fraunhofer IML

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

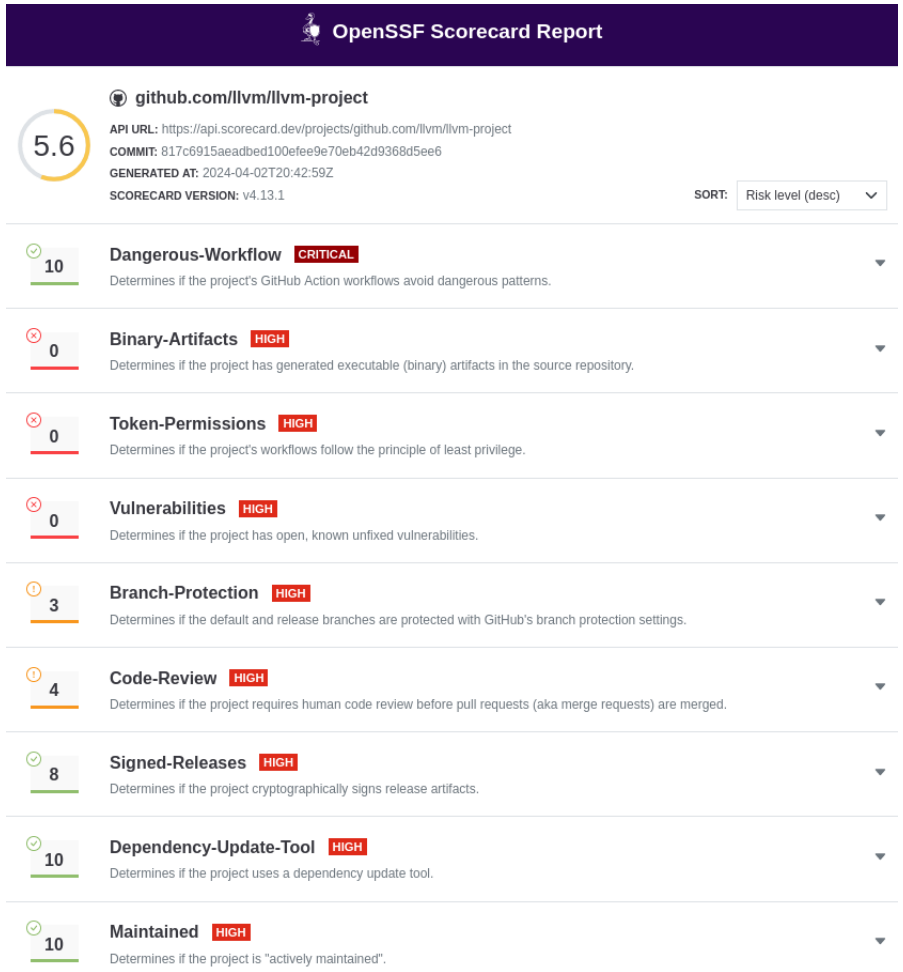


60 open and 1,070 closed alerts

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

Fraunhofer IML

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