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=git
  hub.com/llvm/llvm-project

The LLVM Compiler Infrastructure

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, bytecode analyzer, and bytecode 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.
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

<table>
<thead>
<tr>
<th>Rule (w. Severity High)</th>
<th>Open (Closed) Alerts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch-Protection</td>
<td>1</td>
</tr>
<tr>
<td>Vulnerabilities</td>
<td>1</td>
</tr>
<tr>
<td>Code-Review</td>
<td>1</td>
</tr>
<tr>
<td>Token-Permissions</td>
<td>5 (5)</td>
</tr>
<tr>
<td>Binary-Artifacts</td>
<td>48 (962)</td>
</tr>
</tbody>
</table>
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