System & Software Security
SBOM

Nuno Pereira
João Pereira
Davide Baggio

October 2024

We confirm that this report was fully produced by the team members **Davide Baggio, João Pereira and Nuno Pereira** and we are jointly responsible for all content presented in this work. All used sources were attributed properly.

Davide Baggio, João Pereira, Nuno Pereira

Contents

1 Introduction

Software systems increasingly outsource parts of application logic to first- or third-party *dependencies* — pieces of code that are used in conjunction or as a part of the application's business logic but that are not part of the application itself. (Needs references)

Keeping track of dependencies can be an arduous task, which can be more easily managed using software tools and components such as *package managers* that keep track of an application's dependencies and their versions (Needs references) , like *npm* or *cargo* [1, 2].

2 Overview of reviewed papers

3 Metrics defined

4 Analysis and Comparison of reviewed papers

5 Conclusion

References

[1] NodeJS Team. *NPM: Node Package Manager*. URL: https://www.npmjs.com/. (accessed: 15.10.2024).

[2] Rust Team. *Cargo*. URL: https://doc.rust-lang.org/cargo/. (accessed: 15.10.2024).