

# Evaluation of Free and Open Source Tools for Automated Software Composition Analysis

Laura Bottner, Mercedes-Benz Tech Innovation GmbH  
Artur Hermann, Ulm University  
Jeremias Eppler, Mercedes-Benz Tech Innovation GmbH  
Prof. Dr.-Ing. Thomas Thüm, Ulm University  
Prof. Dr. rer. nat. Frank Kargl, Ulm University

Mercedes-Benz

In cooperation with University of Ulm



CSCS2023 - 5. Dezember 2023, Darmstadt

# Table of Contents

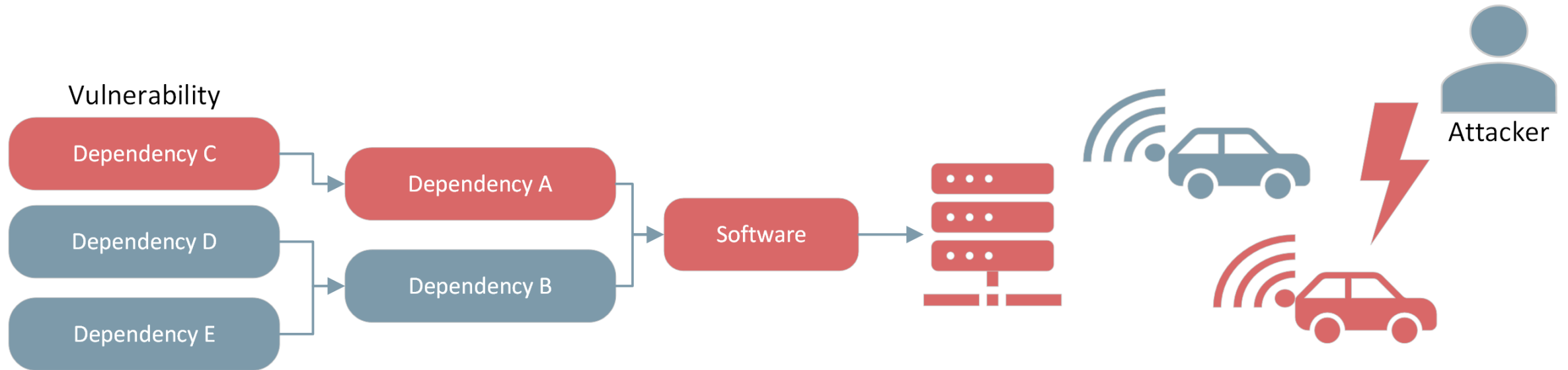
Introduction

Motivation

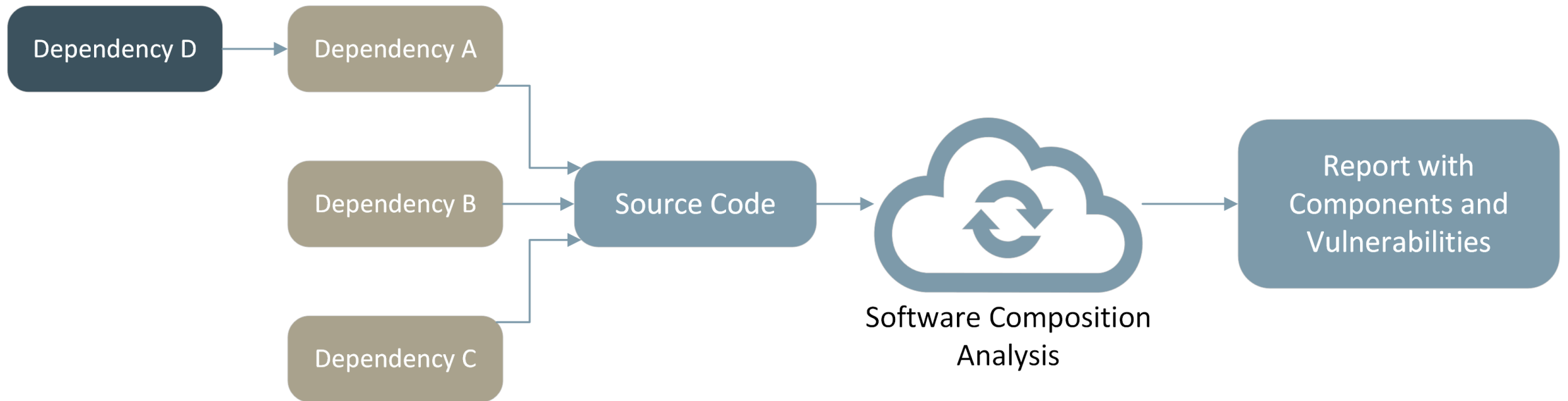
Methodology

Conclusion

# Why do we need SCA?



# Definition of SCA



# Motivation

Main Objective: Securing the software supply chain for automotive software

- Different approaches: metadata-based, code-centric [1]
- Many Challenges: [2, 3]
  - Vulnerability Database
  - Metadata Incompleteness
  - Language Dependency

[1] Imtiaz, N., Thorn, S., and Williams, L. A comparative study of vulnerability reporting by software composition analysis tools. (2021)

[2] Ponta, S. E., Plate, H., and Sabetta, A. Detection, assessment and mitigation of vulnerabilities in open source dependencies. (2020)

[3] Prana, G. A. A., Sharma, A., Shar, L. K., Foo, D., Santosa, A. E., Sharma, A., and Lo, D. Out of sight, out of mind? how vulnerable dependencies affect open-source projects. (2021)

# Motivation

## Automated SCA FOSS tools

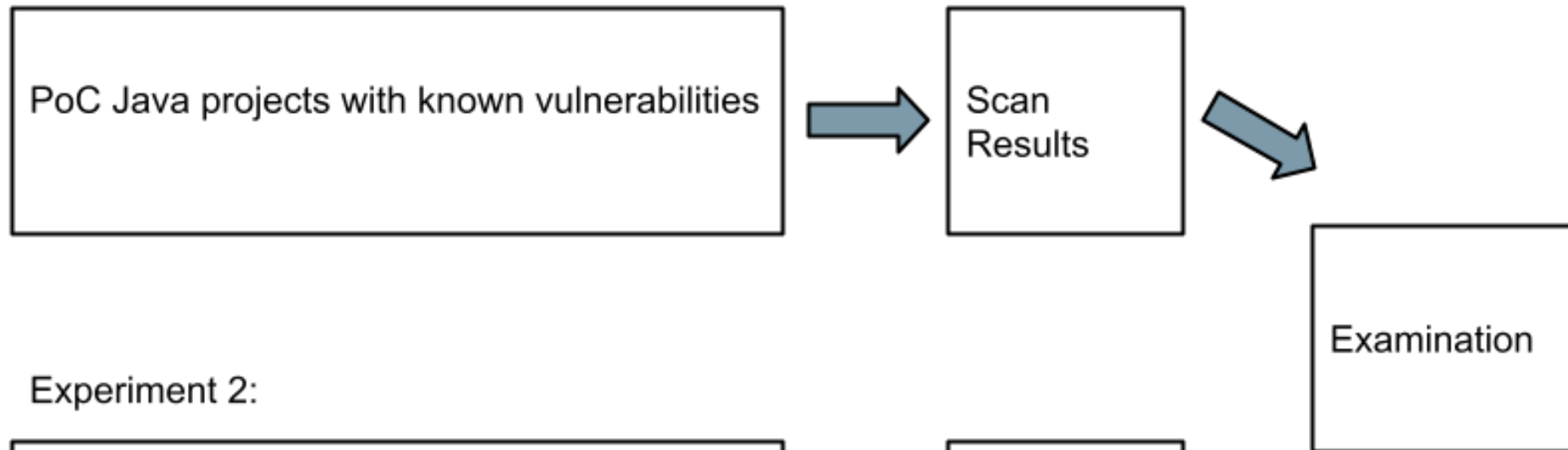
- OWASP Dependency Check (ODC) works metadata-based
- Eclipse Steady (ES) novel code-centric SCA approach
  - Additional reachability analysis with ES (ES\_reach)

## Both tools can scan Java code without limitations

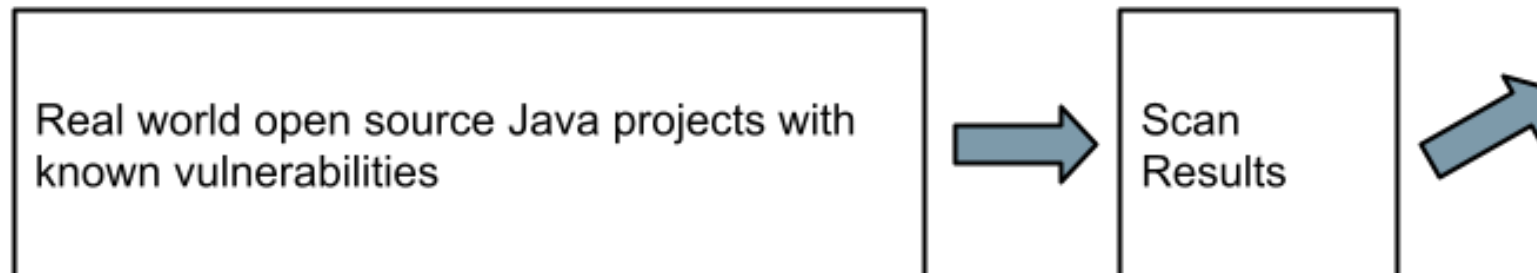
- Which SCA tool (ES or ODC) provides better qualitative scan results
- Can ES\_reach significantly reduce the number of False Positives

# Experimental Evaluation

Experiment 1:

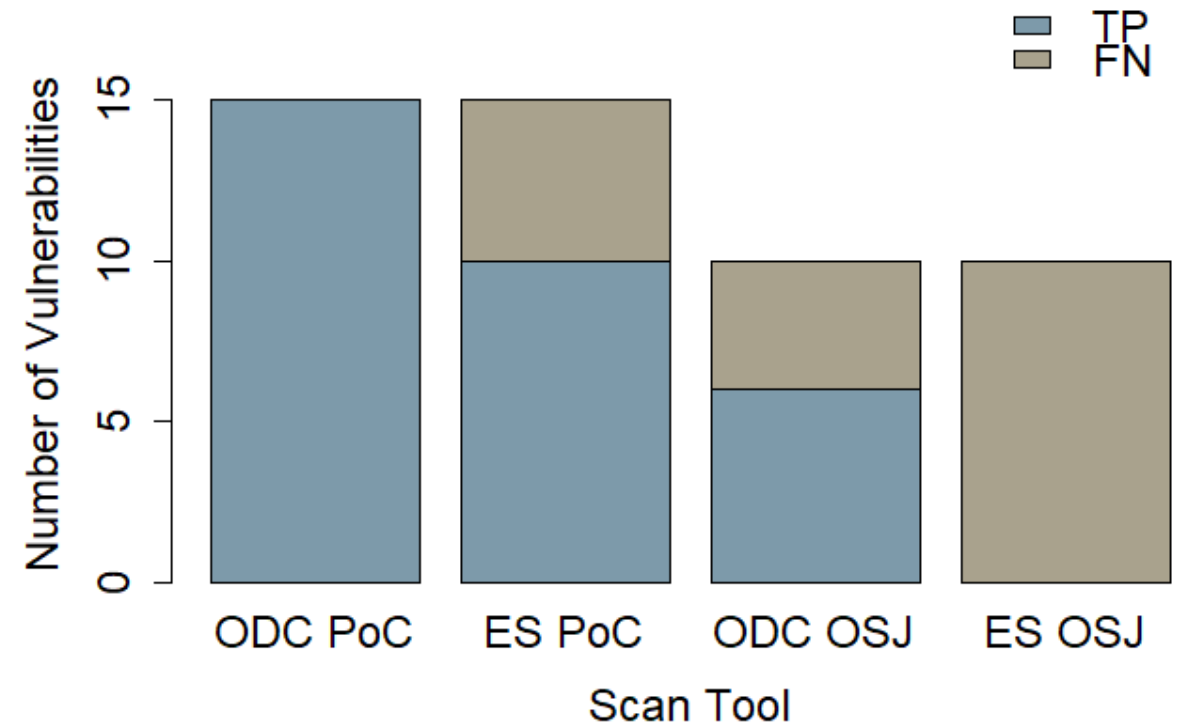


Experiment 2:



# True Positive and False Negative rate

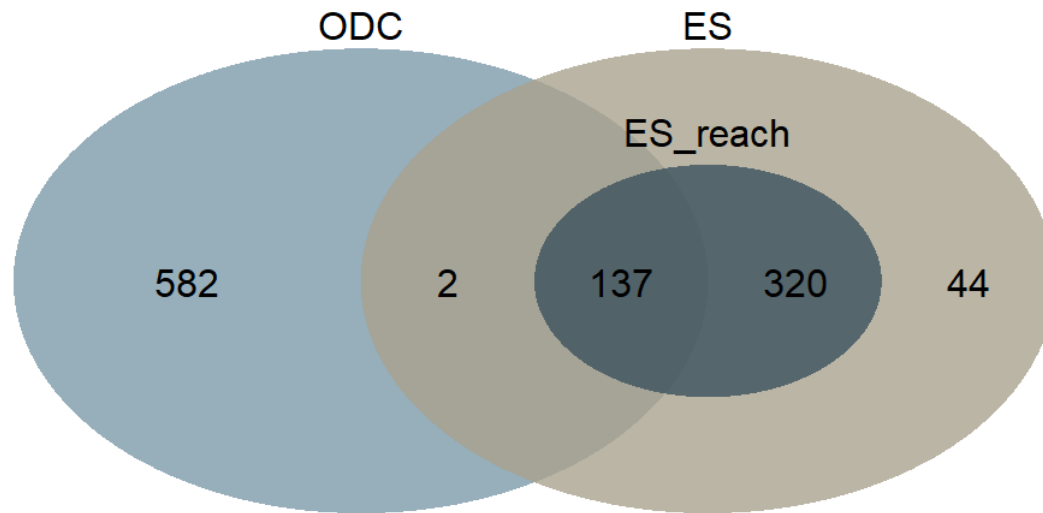
True Positive (TP) and False Negative (FN) rate for ODC and ES for the known vulnerabilities in the PoC (Experiment 1) and OSJ (Experiment 2) projects



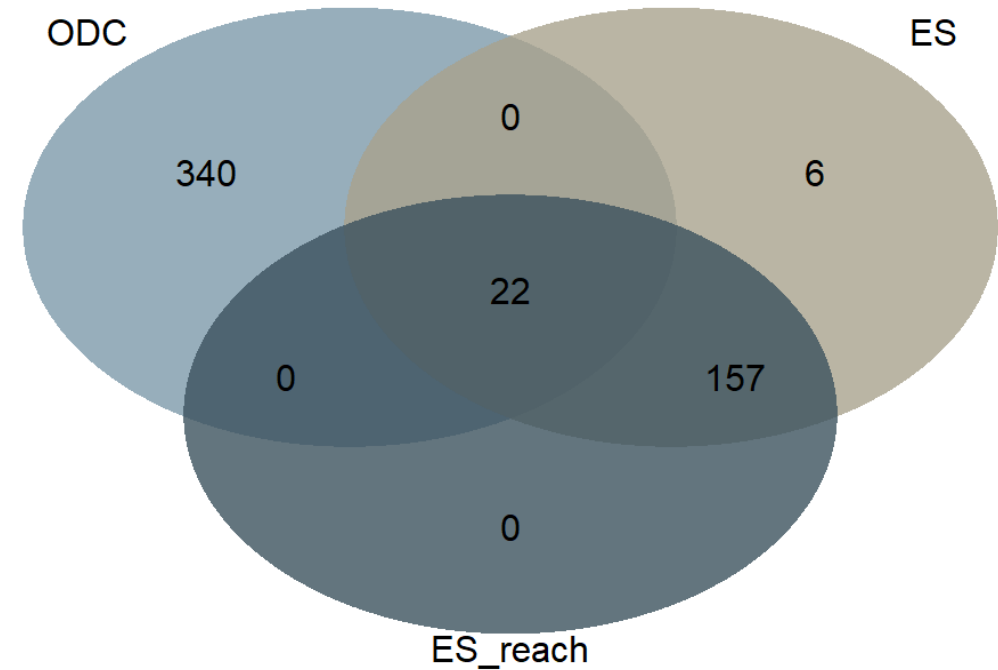


# Total number of reported vulnerabilities

ES reachability analysis and total number of reported vulnerabilities by ODC and ES



Results for PoC projects (Experiment 1)



Results for the OSJ projects (Experiment 2)

# Code Review (Experiment 1)

Manual investigation of 36 vulnerabilities for ODC and ES

- Five vulnerabilities were TP, three of them detected by both tools
- FP of ODC because of missing application context
- FP of ES because of failed version matching
- FN of ES because of missing entry in Vulnerability Database

# Code Review (Experiment 1)

Manual investigation of 12 vulnerabilities for ES and ES\_reach

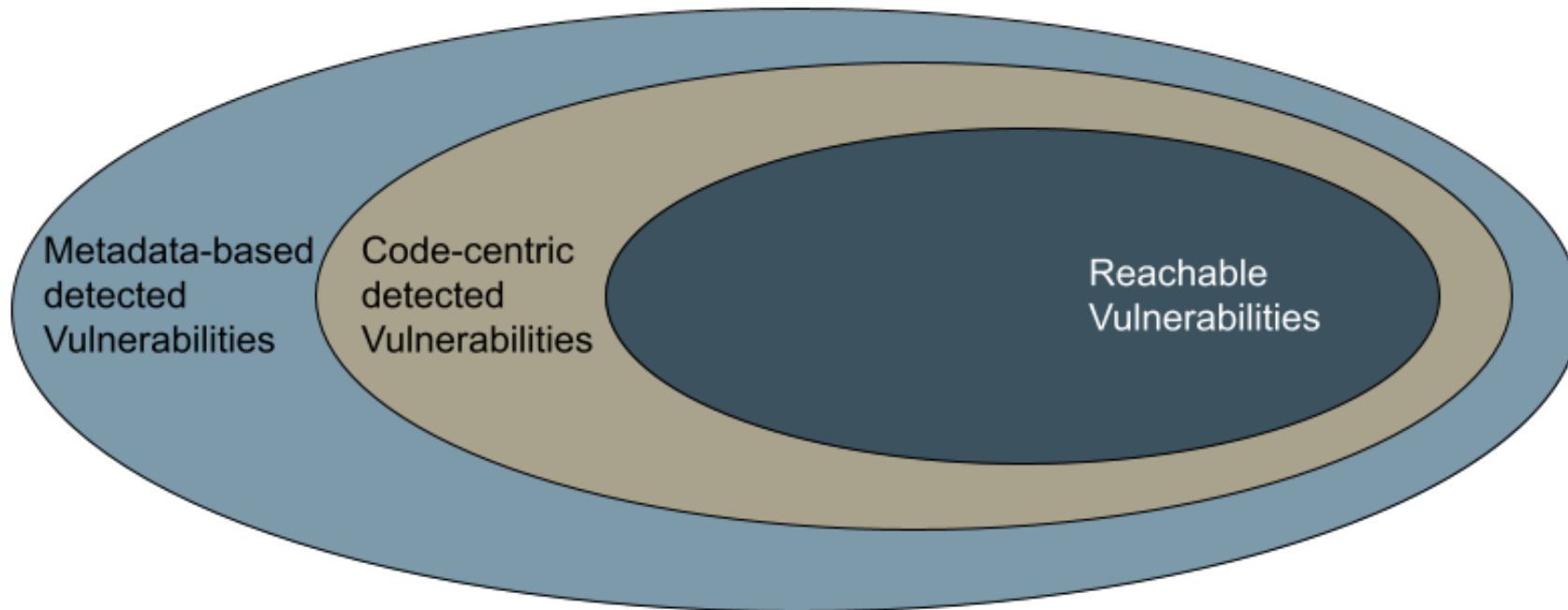
- All vulnerabilities were FP
- Ten were FP because of failed version matching
- Two were FP because of non-exploitable configurations (reported by ES, ES\_reach and ODC)

# Key Findings

- Different findings because of missing information in ES Vulnerability Database and ES wrong version matching
- Based on manual analysis high FP rate for both tools
- Both tools resolved same dependencies
- Most of the manual identified TP were in the intersection of both tools
- ODC significantly more TP than ES
- ES\_reach marked overall only two FP in the intersection

# Conclusion

- The quality of the Vulnerability Database is crucial
  - Metadata-based SCA (ODC) is less prone to False Negatives
  - Code-centric SCA can reduce the number of False Positives
- We propose a hybrid solution of both approaches



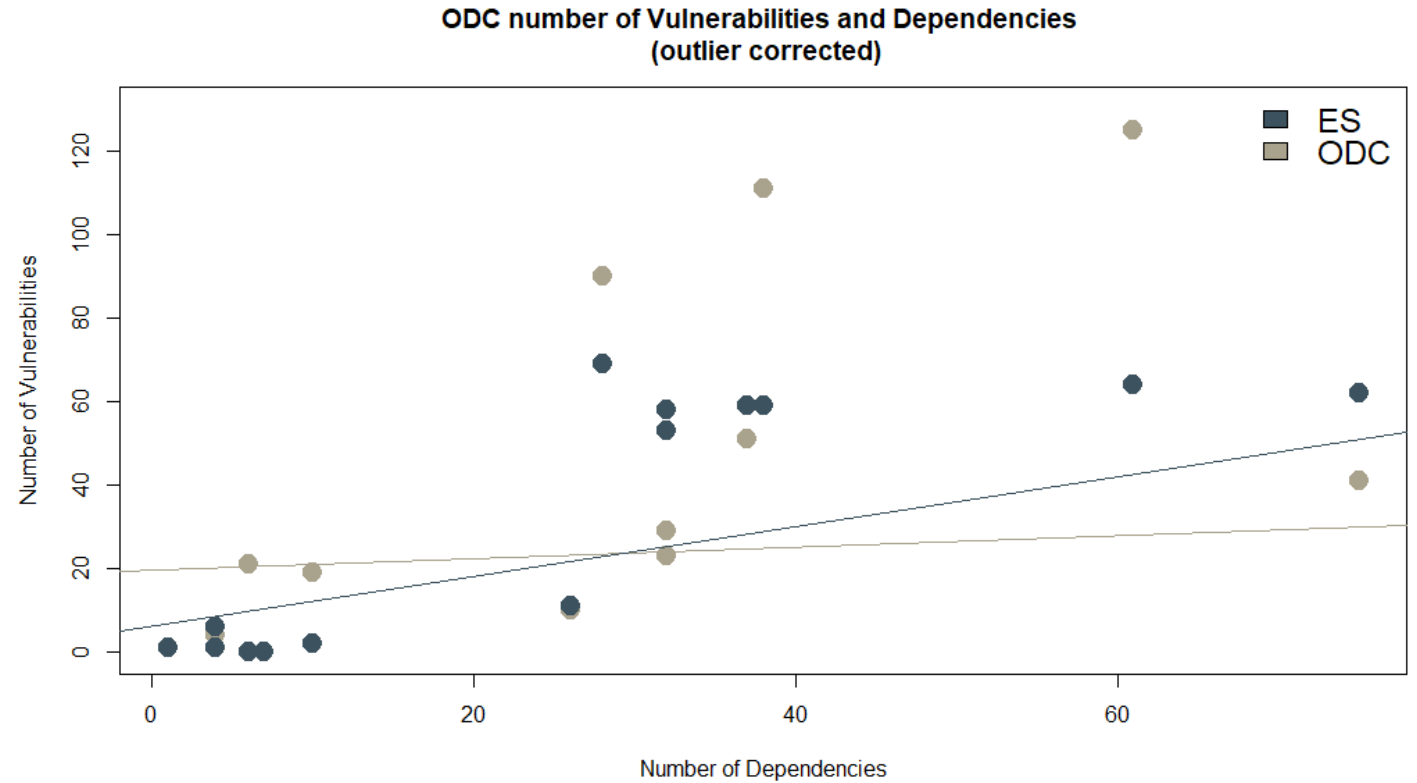
# Future Work

- Examining additional Java projects
- Exploring other programming languages, like Python, C, C++
- Examining further SCA tools
- Evaluating SCA for binaries


# APPENDIX

# Dependencies (Experiment 1)

ES and ODC identified the same dependencies







Mercedes-Benz Tech Innovation GmbH  
Wilhelm-Runge-Street 11, 89081 Ulm  
Phone +49 731 505 6102 | [techinnovation@mercedes-benz.com](mailto:techinnovation@mercedes-benz.com) | [www.mercedes-benz-techinnovation.com](http://www.mercedes-benz-techinnovation.com)  
Domicile and Court Registry: Ulm | HRB-No.: 3844 | Management: Daniel Geisel (CEO), Isabelle Krautwald

Mercedes-Benz Tech Innovation