The cases about vulnerability findings

Wonyoung Choi

Introduction

Wonyoung Choi, a.k.a Toru

Lead mobile developer, OCBC Bank

Active speaker in SEA

https://www.linkedin.com/in/toruchoi

@TORU_0239

What have we learnt from log4j issue?

How many dependencies have you used?

What tools you use to detect the vulnerability?

Security and code defect scanning tools

- Blackduck by Synopsys
- Coverity by Synopsys
- Sonarqube
- Lint

Security and code defect scanning tools

- Blackduck by Synopsys
- Coverity by Synopsys
- Sonarqube
- Lint

Caused issues!

What if embedded plugin caused security issues?

Nothing but blaming Google. :D

But it happened!

Security issues in the plugged-in components

- Databinding
- Lint in Android studio

How to resolve?

- Keep dependencies updated with the latest version
- Replacing dependencies regarding issue
- Excluding the corresponding dependencies
- Not only dependencies but also build tools and language

Use case

- Updated Android project with Java 11 and Gradle 7
- Updated all the dependencies with the latest ones
- Removed Databinding and replaced with Viewbinding
- Took Lint out of build process

How to check the vulnerability issue?

Use case

- Tried applying OWASP into sample project
- Inspired by this article
  https://proandroiddev.com/keep-your-app-secure-with-dependencycheck-585d61aff3c
- Checking the latest version frequently in maven repository / using AS