

Posudek diplomové práce

Bc. Marek Szymutko

V rámci softwarového vývoje ve společnosti Red Hat se často setkáváme s výzvou, jak rychle a efektivně reagovat na softwarové zranitelnosti ve formě tzv. CVE (Common Vulnerabilities and Exposures). Abychom mohli našim zákazníkům garantovat vysokou úroveň bezpečnosti, bylo nutné vytvořit sadu nástrojů pro práci s dokumenty SBOM (Software Bill of Materials). Tyto dokumenty představují základní stavební kámen procesů, které umožňují efektivní detekci zranitelností v softwaru a zároveň transparentně informují zákazníky o složení jednotlivých produktů.

Bylo proto velkým přínosem, když jsme společně s Bc. Markem Szymutkem našli průnik mezi jeho diplomovou prací zaměřenou na bezpečnost a reálnými potřebami společnosti Red Hat. Jeho práce se soustředí na několik klíčových aspektů této problematiky a reaguje na aktuální legislativní požadavky kladené na poskytovatele softwaru.

Teoretická část práce přehledně shrnuje význam SBOM dokumentů ve vývoji softwaru a popisuje aktuální standardy, se kterými lze v současnosti pracovat. Následně identifikuje hlavní problémy, které se student rozhodl adresovat – konkrétně vývoj nástroje pro ověřování kvality SBOM dokumentů a jejich bezztrátovou konverzi mezi aktuálně podporovanými formáty (SPDX a CycloneDX). Hodnocení kvality SBOM dokumentů je klíčové, neboť přímo ovlivňuje schopnost organizace identifikovat zranitelnosti ve svých produktech.

Z pohledu samotného vývoje těchto nástrojů nemám studentovi co vytknout. Výsledný software má otevřený zdrojový kód dostupný na platformě GitHub a využívá standardní CI/CD (continuous integration & continuous delivery) procesy pro zajištění kvality a distribuce. Během spolupráce student průběžně a otevřeně komunikoval své nápady a architektonická rozhodnutí. Pracoval velmi samostatně, a to jak při vývoji, tak při studiu problematiky. Na konzultace přicházel vždy připravený, s novými poznatky a jasným plánem dalšího postupu.

Zvlášť bych chtěl vyzdvihnout architektonickou kvalitu navrženého řešení, které je promyšlené tak, aby bylo snadno rozšiřitelné a nebylo omezeno pouze na úzký případ použití. Příkladem může být implementace obecného dotazovacího jazyka nebo tzv. kuchařek pro definici validačních pravidel.

Výstupy této diplomové práce jsou jednoznačně využitelné v praxi. Již nyní pracujeme na integraci obou nástrojů do našich interních procesů, kde nám pomohou dále zvyšovat bezpečnost softwaru dodávaného společnostmi Red Hat.

Ing. Aleš Raszka
Principal Software Engineer
Red Hat