МЕТОДИ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ У ЛАНЦЮГУ ПОСТАЧАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Сухарєв І.С., Настенко А.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Забезпечення безпеки ланцюга постачання програмного забезпечення (ПЗ) та контроль використання сторонніх бібліотек наразі є важливою складовою сучасного процесу розробки ПЗ. Значна частина сучасних програмних продуктів створюється з активним використанням готових бібліотек і пакетів відкритого коду [1], що дає змогу скоротити час і вартість розробки. Водночас використання зовнішніх залежностей створює додаткові ризики, пов'язані з можливими вразливостями, компрометацією пакетів або використанням застарілих компонентів. Ускладнення структури залежностей, зокрема транзитивних, ускладнює своєчасне виявлення таких загроз [2].

Метою доповіді є дослідження методів автоматизованого виявлення вразливостей у зовнішніх залежностях програмних проєктів із використанням спеціалізованих баз даних і сервісів безпеки, а також розробка алгоритму формування рекомендацій щодо оновлення, заміни або вилучення потенційно небезпечних компонентів.

У доповіді наводяться результати розробки програмного засобу мовою Python, який реалізує функції побудови повного дерева залежностей проєкту, автоматичного зіставлення версій бібліотек із записами в базах CVE та OSV [3], оцінювання критичності виявлених вразливостей за метрикою CVSS [4], а також формування звітів з рекомендаціями щодо зниження ризиків шляхом оновлення компонентів, їх заміни або пошуку безпечніших альтернатив.

Наведені результати свідчать, що впровадження подібних інструментів у CI/CD-процеси дозволяє значно зменшити ймовірність успішних атак на ланцюжок постачання та забезпечує безперервний моніторинг безпеки програмного продукту без суттєвого ускладнення процесу розробки. Отримані результати підтверджують необхідність комплексного підходу до аудиту стороннього коду як важливої складової методології DevSecOps.

Список літератури

1. OWASP Top 10 Software Supply Chain Security. OWASP Foundation. 2023. URL: https://owasp.org/www-project-top-10-software-supply-chain-security-risks/.

2. Tkachov, A., Hapon, A., Balagura, D., Sievierinov, O., Bukatych, I., & Havrylova, A. (2024, November). Analysis of the software security protection. In *2024 8th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)* (pp. 1-8). IEEE.

3. Vulnerability Analysis in Open Source Dependencies. GitHub Security Advisory Database. URL: https://github.com/advisories .

4. CVSS v3.1 Specification Document. FIRST.org. URL: https://www.first.org/cvss/v3.1/specification-document .