Research Proposals

Yao-Wen Chang
Student ID: 1346258

Submission Date: September 17, 2023

[**?**]

Abstract

This literature review will introduce Continuous Integration/Continuous Delivery (CI/CD). Also, some attack surface and how the malicious attacker exploit these attack surface will be covered in this review. From the developers' and maintainers' point of view, the methods and frameworks are going to be introduced to counter the attack. In this literature review, the framework will focus on Supply Chain Level Security Artifacts (SLSA) which is adopted by Google.

1 Introduction

Continuous IntegrationContinuous Delivery (CI/CD) is a development process for quickly building and testing code changes that helps organizations maintain a consistent code base for their applications while dynamically integrating code changes. Therefore, CI/CD environments are attractive targets for malicious cyber actors (MCAs) whose goals are to compromise information by introducing malicious code into CI/CD applications, gaining access to intellectual property/trade secrets through code theft, or causing denial of service effects against applications.

Section 2 will briefly introduce CI/CD, and section 3 would target the attack surface within the process of CI/CD. Then, section 4, we are going to map the defense method to the attack method, and providing real world attack event. In section 5, our literature review would introduce SLSA framework from Google, and explain how SLSA can patch the vulnerable CI/CD process. In section 6, the aim and objects of the research will be explained. And the research plan will be introduced in section 7.

2 Definition of CI/CD

3 Attack Surface and Impact

4 Defense Method

These goals are seek to establish the trust in the software supply chain by verifying in- formation about the participants or processes [1].

Some of the projects aims at providing single solution that conflates multiple objectives [1].

Despite the previously introduced methods seems to address all the security issue existed in the code base and within the CI/CD, some of them may overemphasize one particular approach to address software supply chain security. without considering compounding factors that impact risk [1].

5 Supply Chain Level Security Artifacts

6 Research Aims and Objectives

7 Research Plan

References

[1] Marcela S. Melara and Mic Bowman. What is software supply chain security?, 2022.