Your Title Here

Your Name: Yao-Wen Chang
Student ID: 1346258

Submission Date

[?]

1 Abstract

This literature review will introduce Continuous Integration/Continuous Delivery (CI/CD). Also, the 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.

2 Introduction

Continuous Integration/Continuous 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.

The following section will go through

References