УДК 004.056

РАЗРАБОТКА АЛГОРИТМА ВЕРИФИКАЦИИ КОНФИГУРАЦИЙ ПАЙПЛАЙНОВ ЦЕПОЧЕК ПОСТАВОК ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Андреев Я.Е. (Университет ИТМО)
Научный руководитель – Еритенко Н.А. (Университет ИТМО)

Введение. В настоящее время сфера DevSecOps становится все более популярной, вместе с тем CI/CD-пайплайны цепочек поставок программного обеспечения стали важнейшими элементами в процессе жизненного цикла разработки программного обеспечения. Безопасность в CI/CD-процессах состоит из анализа исходного кода и зависимостей, тестирования артефактов сборки и готового программного обеспечения [1]. Между тем, конфигурационные файлы CI/CD-пайплайнов остаются слабо формализованным и недостаточно исследованным вектором атак [2, 3]. Таким образом отсутствие формализованных моделей анализа конфигураций приводит к сохранению существенной поверхности атаки и возможности эксплуатации критических уязвимостей, включая атаки класса Poisoned Pipeline Execution.

Основная часть. Доклад посвящен исследованию безопасности конфигураций CI/CD-пайплайнов как критического вектора атак на цепочки поставок программного обеспечения, доказательству актуальности угроз эксплуатации уязвимостей конфигураций CI/CD-пайплайнов, а также анализу применимости методов статического анализа кода в обеспечении безопасности конфигураций пайплайнов сборки и доставки программного обеспечения.

Согласно многочисленным исследованиям и отчетам, актуальными рисками являются недостаток механизмов управления потоками выполнения, который влечет за собой «Выполнение скомпрометированного пайплайна» (PPE) [4]. Данный риск информационной безопасности является 4-м в рейтинге «OWASP TOP-10 CI/CD risks». Суть атаки заключается во внедрении вредоносного кода, зависимостей из недоверенных источников в код CI/CD-конфигурации пайплайна, что ведет к компрометации пайплайна, раннера, инфраструктуры.

Атака PPE разделяется на прямое исполнение и косвенное [5]. Direct Poisoned Pipeline Execution – это класс атаки PPE, при которой происходит внедрение вредоносного кода непосредственно в CI/CD-конфигурацию. Indirect Poisoned Pipeline Execution – это класс атаки PPE, при которой происходит внедрение вредоносного кода в зависимости, используемые пайплайном для сборки и доставки программного обеспечения.

В работе конфигурация CI/CD-пайплайна рассматривается как самостоятельная вычислительная модель, для которой вводится формализованное представление в виде ориентированного графа потоков выполнения и зависимостей. На основе данной модели предлагается определение поверхности атаки пайплайна как множества достижимых

путей от недоверенных источников к привилегированным узлам исполнения и чувствительным данным.

На основе введенной модели разрабатывается алгоритм семантической валидации CI/CD-конфигураций, ориентированный на выявление достижимости привилегированных операций и чувствительных ресурсов из недоверенных точек входа. Эффективность алгоритма оценивается через количественное снижение поверхности атаки на тестовом наборе конфигураций с типизированными уязвимостями.

На рисунке 1 изображен алгоритм предлагаемого решения.

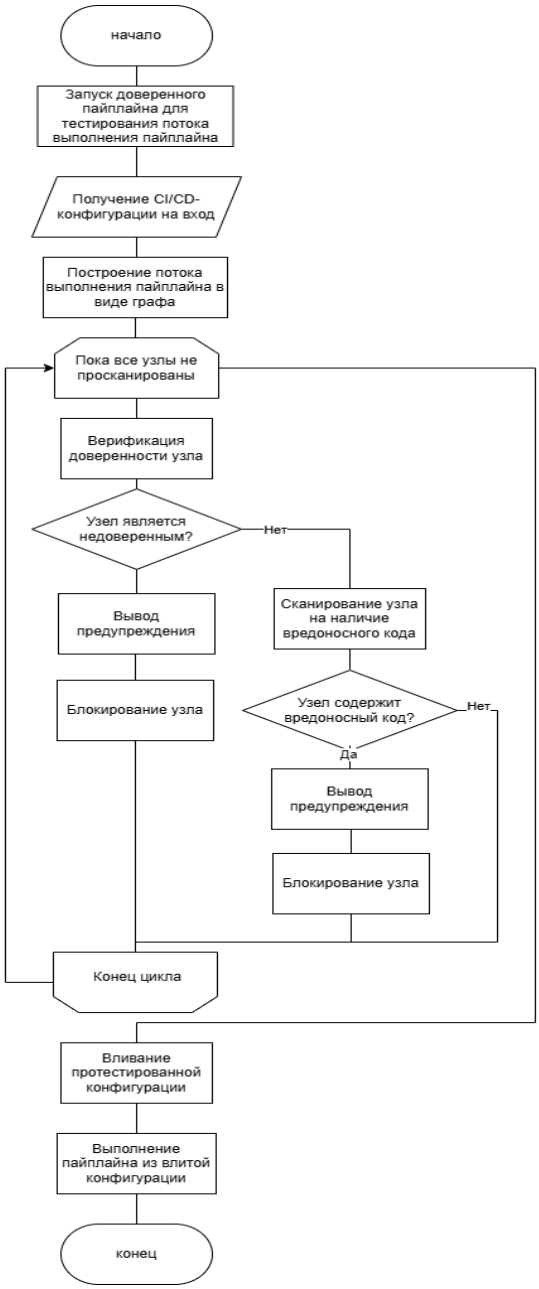

Рисунок 1 – Алгоритм предлагаемого решения

Выводы. По результатам исследований был разработан алгоритм сканирования безопасности конфигураций CI/CD-пайплайнов цепочек поставок программного обеспечения, анализирующий не только сам код конфигурации, но и зависимости, используемые пайплайном: скрипты, сторонние и вспомогательные конфигурации пайплайнов, плейбуки, репозитории.

Список использованных источников:

1. Developing a Framework for Integrating Security Testing into the CI/CD Pipeline using Automation
2. Z. Pan et al., "Ambush From All Sides: Understanding Security Threats in Open-Source Software CI/CD Pipelines," in IEEE Transactions on Dependable and Secure Computing, vol. 21, no. 1, pp. 403-418.
3. A HackerOne employee's GitHub personal access token exposed in Travis CI build logs [Электронный ресурс]. – 2017. – URL: https://hackerone.com/reports/215625
4. OWASP Top 10 CI/CD Security Risks [Электронный ресурс]. – 2021. – URL: https://owasp.org/www-project-top-10-ci-cd-security-risks/
5. Poisoned Pipeline Execution [Электронный ресурс]. – 2025. – URL: https://attack.mitre.org/techniques/T1677/

Андреев Я.Е. Подпись 

Еритенко Н.А. Подпись