DOI: 10.37791/2687-0649-2024-19-3-91-110

Безопасный конвейер доставки программного обеспечения

М.В. Тумбинская[1*]***, А.Х. Хаертдинов***[1]***, А.Ю. Сенцова***[2]
[1]*Казанский национальный исследовательский технический университет им. А. Н. Туполева, Казань, Россия*
[2]*Уфимский университет науки и технологий, Уфа, Россия*
[*]*tumbinskaya@inbox.ru*

Аннотация. Наличие уязвимостей в программном обеспечении является актуальной проблемой. Уязвимости могут служить основой для нарушения конфиденциальности и утечки информации. Целью данного исследования является повышение уровня защищенности программного обеспечения на всех этапах жизненного цикла от этапа разработки до этапа внедрения и эксплуатации. Достижение поставленной цели возможно путем автоматизированного анализа программного кода и увеличения типов обнаруживаемых уязвимостей. В работе предложен безопасный конвейер доставки программного обеспечения, который позволяет проводить статический и динамический анализ программного кода, анализ поиска уязвимостей в сторонних компонентах и docker-образах. Рассмотрены популярные программные инструменты, их отличительные особенности, дано обоснование выбора программных решений, которые заложены в основу разрабатываемого безопасного конвейера доставки. Новизной работы является возможность конвейера в автоматизированном режиме обнаруживать уязвимости на всех этапах жизненного цикла программного обеспечения, начиная от планирования и проектирования вплоть до тестирования, развертывания и мониторинга в производственной среде, что позволяет устранять уязвимости на ранних стадиях, тем самым повышая уровень защищенности программного обеспечения. Проведено тестирование безопасного конвейера доставки программного обеспечения. Исходя из результатов оценки, разработанный безопасный конвейер доставки программного обеспечения показал, что в среднем средствами инструмента Semgrep было выявлено 98% уязвимостей, средствами инструмента OWASP ZAP – 90% уязвимостей, средствами инструмента Dependency-Track – 96% уязвимостей, средствами инструмента Trivy – 88% уязвимостей. Результаты исследования и экспериментальные данные показали, что в среднем точность обнаружения уязвимостей составляет 93%. Практическая ценность работы заключается в том, что разработанный безопасный конвейер доставки программного обеспечения может быть использован в качестве инструмента для обнаружения уязвимостей программного кода специалистами – разработчиками программного обеспечения, а также специалистами по информационной безопасности ИТ-компаний. Полученные результаты могут быть использованы в области разработки защищенного программного обеспечения, формализации и интерпретации уязвимостей в программном коде, что позволит создавать новые правила их выявления и разработки контрмер по их нейтрализации.

Ключевые слова: уязвимость, DevSecOps, конвейер доставки, docker-образ, безопасная разработка, анализ программного кода

Для цитирования: *Тумбинская М.В., Хаертдинов А.Х., Сенцова А.Ю.* Безопасный конвейер доставки программного обеспечения // Прикладная информатика. 2024. Т. 19. № 3. С. 91–110. DOI: 10.37791/2687-0649-2024-19-3-91-110

Secure software delivery pipeline

***M. Tumbinskaya*[1*], *A. Khaertdinov*[1], *A. Sentsova*[2]**
[1]*Kazan National Research Technical University named after A.N. Tupolev, Kazan, Russia*
[2]*Ufa University of Science and Technology, Ufa, Russia*
[*]*tumbinskaya@inbox.ru*

Abstract. The presence of vulnerabilities in software is a pressing problem. Vulnerabilities can serve as a basis for breach of confidentiality and information leakage. The purpose of this study is to increase the level of software security at all stages of the life cycle from development and implementation to operation. Achieving this goal is possible through automated analysis of program code and increasing the types of vulnerabilities detected. The work proposes a secure software delivery pipeline that allows for static and dynamic analysis of program code, analysis of the search for vulnerabilities in third-party components and Docker images. The article reviewed popular software tools, their distinctive features, and provided justification for the choice of software solutions that form the basis of the developed secure delivery pipeline. The novelty of the work is the ability of the pipeline to automatically detect vulnerabilities at all stages of the software life cycle, from planning and design to testing, deployment and monitoring in a production environment, which allows you to eliminate vulnerabilities at an early stage, thereby increasing the level of software security. Conducted testing and approbation of a secure software delivery pipeline. Based on the assessment results, the developed secure software delivery pipeline showed that on average 98% of vulnerabilities were identified using the Semgrep tool, 90% of vulnerabilities using the OWASP ZAP tool, 96% of vulnerabilities using the Dependency-Track tool, and 88% using the Trivy tool. The results of the study and experimental data showed that on average, as a result of testing, the accuracy of detecting vulnerabilities is 93%. The practical value of the work lies in the fact that the developed secure software delivery pipeline can be used as a tool for detecting program code vulnerabilities by software development specialists, as well as information security specialists of IT companies. The results obtained can be used in the field of secure software development, formalization and interpretation of vulnerabilities in program code, which will make it possible to create new rules for their identification and development of countermeasures to neutralize them.

Keywords: vulnerability, DevSecOps, delivery pipeline, Docker image, secure development, code analysis

For citation: Tumbinskaya M., Khaertdinov A., Sentsova A. Secure software delivery pipeline. *Prikladnaya informatika*=Journal of Applied Informatics, 2024, vol.19, no.3, pp.91-110 (in Russian). DOI: 10.37791/2687-0649-2024-19-3-91-110

Введение

Разработка и доставка программного обеспечения в производственную среду составляют неотъемлемую часть процесса создания и поддержки программных продуктов. С ростом сложности и объема проектов, а также с увеличением требований к скорости и качеству разработки все большую популярность приобретает методология DevOps (Development & Operations), которая объединяет разработку и операционные процессы и позволяет повысить уровень автоматизации и ускорить процесс доставки программного обеспечения (ПО). С целью обеспечения безопасности и качества программного обеспечения на всех этапах его жизненного цикла применяется