УДК 004.056

В.В. ПЕРОВ
Научный руководитель – к.т.н., доцент А.П. ДУРАКОВСКИЙ
Национальный исследовательский ядерный университет «МИФИ», Москва

ИССЛЕДОВАНИЕ ФАКТОРОВ ВОЗНИКНОВЕНИЯ ЛОЖНОПОЛОЖИТЕЛЬНЫХ И ЛОЖНООТРИЦАТЕЛЬНЫХ РЕЗУЛЬТАТОВ СТАТИЧЕСКОГО АНАЛИЗА ИСХОДНОГО КОДА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Цель исследования – анализ основных причин возникновения ложноположительных и ложноотрицательных результатов статического анализа исходного кода программы и разработка рекомендаций по их снижению. В рамках работы выполнен обзор современных инструментов статического анализа и их особенностей, проведен анализ влияния специфических языковых конструкций, стандартов оформления кода и архитектурных паттернов на точность анализа.

Введение

В современном мире программное обеспечение (ПО) играет ключевую роль во всех сферах деятельности человека – от бизнеса и промышленности до образования и здравоохранения. Возрастает количество ПО, использующих в своем составе зависимости с открытым исходным кодом, которое несет в себе множество угроз уязвимостей [1]. Эффективным инструментом обеспечения требований по безопасному ПО является статический анализ исходного кода. Одним из основных препятствий на пути его эффективного использования являются ложноположительные и ложноотрицательные результаты.

Анализ факторов возникновения ложных результатов статического анализа кода

Ложноположительные результаты статического анализа ПО могут быть вызваны следующими факторами:

1) **Сложность языковых конструкций и особенностей языков программирования.** Современные языки, такие как JavaScript и Python, поддерживают динамическую типизацию, который усложняет статический анализ. Динамические языковые особенности могут привести к увеличению числа ложноположительных срабатываний из-за неопределенности типов и структур данных на этапе компиляции [2].

2) **Недостаточный контекстный анализ.** Инструменты статического анализа часто не учитывают весь контекст выполнения программы, что может приводить к ошибочным интерпретациям сложных конструкций.

3) **Ограничения алгоритмов и правил анализа.** Проблемы с точностью статического анализа часто возникают из-за использования упрощённых алгоритмов, которые ограничивают возможности инструмента.

Ложноотрицательные результаты статического анализа ПО могут быть вызваны следующими факторами:

1) скрытые или сложные уязвимости. Некоторые уязвимости остаются невыявленными при использовании стандартных инструментов, что связано с ограничениями в анализе потоков данных.

2) использование внешних библиотек и компонентов. Недостаточная информация о сторонних модулях может привести к тому, что уязвимости, связанные с их использованием, останутся незамеченными.

3) обфускация и некорректные практики написания кода. Использование нестандартных или запутанных методов программирования усложняет анализ и может приводить к пропуску ошибок.

Заключение

Ложноположительные результаты в статическом анализе исходного кода возникают, когда инструмент сообщает об ошибке, которой нет. Это может быть вызвано сложностью языковых конструкций, динамической типизацией, недостаточным контекстным анализом или ограничениями применяемых алгоритмов. Ложноотрицательные результаты возникают, когда реальные уязвимости остаются незамеченными, что может быть связано с использованием внешних библиотек, сложностью межпроцедурных взаимодействий и неэффективностью обработки обфусцированного кода. Эти проблемы затрудняют объективную оценку качества программного обеспечения и требуют улучшения подходов к анализу.

Список литературы

1. Марков А.С. Важная веха в безопасности открытого программного обеспечения / А.С. Марков // Вопросы кибербезопасности. – 2023. – № 1(53). – С. 2–12. – DOI 10.21681/2311-3456-2023-1-2-12. – EDN OHYLTR.

2. Tymchuk, Yuriy (June 2017). The False False Positives of Static Analysis. In: Seminar Series on Advanced Techniques and Tools for Software Evolution SATToSE 2017. Madrid, Spain. 07–09. Juni 2017.