УДК 004.056

С.К. МУРАВЬЁВ

*Национальный исследовательский ядерный университет «МИФИ», Москва*

*ООО «Научно-техническое предприятие «Криптософт», Пенза*

# УГРОЗЫ ВРЕДОНОСНОГО ВМЕШАТЕЛЬСТВА В ПРОЦЕССЫ ОПТИМИЗАЦИИ ИСХОДНОГО КОДА

С целью повышения безопасности разрабатываемого программного обеспечения в работе рассмотрена возможность вредоносного изменения конвейера оптимизации исходного кода через штатные интерфейсы компилятора, позволяющие принципиально изменить алгоритм работы компилируемого приложения, даны рекомендации по нейтрализации подобных угроз. Результаты работы могут быть использованы при разработке перспективных средств разработки безопасного программного обеспечения (РБПО).

В настоящее время уделяется особое внимание вопросам снижения числа уязвимостей в разрабатываемом программном обеспечении (ПО). При этом уязвимости в ПО могут быть следствием не только ошибок, допущенных на этапе подготовки исходного кода, но и появиться в результате процедур оптимизации кода и сборки программ, выполняемых компилятором [1]. Осуществление преднамеренных действий в отношении инструментальных средств, применяемых при разработке ПО, внутренними и внешними нарушителями способно привести к возникновению различных угроз безопасности информации [2], что делает актуальным исследование угроз вредоносного вмешательства в процессы оптимизации исходного кода.

Ключевым элементом современных средств разработки ПО являются оптимизирующие компиляторы, которые в процессе компиляции применяют к исходному коду конвейер оптимизации, включающий множество операций для его анализа и трансформации, называемых проходами. При этом наиболее известные компиляторы, входящие в состав LLVM [3] и GCC [4], предоставляют штатные программные интерфейсы для разработки и подключения расширений, способных кардинально изменить процесс оптимизации исходного кода.

Одна из самых типичных задач, решаемая оптимизаторами компиляторов, заключается в поиске таких участков исходного кода, результат выполнения которых не меняется в процессе выполнения целевого приложения, и их замена на соответствующие константные

значения. Используя штатные интерфейсы компилятора, злоумышленник может включить в состав конвейера оптимизации вредоносный проход, который способен заменить использование вычисляемого или получаемого значения, обрабатываемого целевым приложением и которое связано с обеспечением безопасности информации, на константу с требуемым злоумышленнику значением. Примером такой вредоносной оптимизации может выступать замена инициализирующего значения для генератора случайных чисел на значение, известное злоумышленнику. После такой замены злоумышленник сможет предсказывать все числовые последовательности, получаемые с помощью такого генератора, что создаёт серьёзные угрозы безопасности информации.

Для нейтрализации подобных угроз в первую очередь необходимо зафиксировать перечень разрешенных к применению проходов оптимизации и реализовать общие требования к безопасному компилятору языков C/C++ в части формирования и контроля базы данных компиляции [1]. Также потребуется разработка и внедрение новых средств контроля конфигурации среды разработки и системного окружения операционной системы. Интерфейсы для динамического подключения к компилятору внешних модулей расширения должны быть отключены или доработаны таким образом, чтобы осуществлялся надёжный контроль аутентичности таких модулей. Защиту от описанной угрозы также можно обеспечить за счёт использования защищённой операционной системы QP ОС [5] в качестве основы для платформы РБПО.

Представленные в статье сведения могут быть использованы при проектировании и реализации перспективных средств РБПО, а также при внедрении соответствующих процессов РБПО [6].

*Список литературы*

1. ГОСТ Р 71206-2024 Защита информации. Разработка безопасного программного обеспечения. Безопасный компилятор языков C/C++. Общие требования.

2. ГОСТ Р 58412-2019 Защита информации. Разработка безопасного программного обеспечения. Угрозы безопасности информации при разработке программного обеспечения.

3. Наке К., Кван Э. LLVM 17: Инфраструктура для разработки компиляторов / пер. с англ. А.А. Слинкина. – М.: ДМК Пресс, 2024. – 370 с.

4. Interacting with the pass manager. URL: https://gcc.gnu.org/onlinedocs/gccint/Plugins-pass.html (дата обращения: 18.09.2024).

5. Егоров В.Ю. Экосистема операционной системы QP ОС // Системы и средства защиты информации: сб. ст. 15-й межведомственной научно-практической конференции им. Е.А. Матвеева. – Пенза: Издательство ПГУ, 2024. – С. 29–36.

6. ГОСТ Р 56939 – 2016. Защита информации. Разработка безопасного программного обеспечения. Общие требования.