УДК 004.021

ОСОБЕННОСТИ БИНАРНОЙ ЭКСПЛУАТАЦИИ МЕТОДА SIGRETURN ORIENTED PROGRAMMING (SROP).

Коновалов П.И, Глыбовский П.А, Андрушкевич Д.В.
Научный руководитель – кандидат технических наук, Глыбовский П.А.
(Военно-космическая академия им. А.Ф.Можайского)

Введение. Под бинарной эксплуатацией понимается использование уязвимостей в скомпилированных приложениях**.** За последние годы это направление заняло главенствующие позиции как в сложности реализации атак, так и в эффективности их применения. Эксперты по информационной безопасности постоянно борятся с хакерами, исправляя те или иные недостатки программ, тем самым заставляя их создавать новые методы взлома. В данной статье рассмотрен метод SROP. Он основан на подмене команд при перехвате сигналов, таких как Ctrl+C, например, в тот момент, когда они завершают выполнять свои задачи и передают управление процессором текущему процессу.

Сигнал — это программное прерывание, посылаемое вашей программе, когда происходит определенное событие. Он выполняет определенные действия, например, копирует выделенный текст, вследствие передачи сигнала его обработчику.

Основная часть. Ядро операционной системы (ОС) приостанавливает выполнение текущего процесса в момент получения сигнала и изменяет контекст центрального процессора (ЦП) пользовательского пространства таким образом, что соответствующий обработчик сигнала вызывается с правильными аргументами. Когда этот обработчик сигнала заканчивает работу, исходный контекст ЦП пространства пользователя восстанавливается. В частности, программа возвращается из обработчика, используя команду sigreturn, которая считывает кадр сигнала из стека, помещаемого туда ядром при получении сигнала. Кадр содержит всю информацию, необходимую для безопасного возврата из обработчика: значения регистров, указатель стека, флаги и т. д. Проблема в том, что любой, кто управляет стеком, может настроить такой сигнальный кадр. Вызвав sigreturn, могут создавать последовательности команд, выполняющие их инструкции.

Выводы. Рассмотрен метод Sigreturn Oriented Programming и принципы его функционирования с целью обезопасить разработчиков от написания уязвимого кода, эксплуатация недостатков которого может привести к непредсказуемым последствиям.

Список использованных источников:

1. Sigreturn Oriented Programming / [Электронный ресурс] // URL: https://lo0l.com/2020/01/01/srop.html (дата обращения: 17.02.2023).
2. Sigreturn Oriented Programming - An Introduction / [Электронный ресурс] // URL: https://www.pwnthebox.net/reverse/engineering/and/binary/exploitation/series/2021/05/09/sigreturn-oriented-programming.html (дата обращения: 17.02.2023).

Коновалов П.И. (автор) Подпись

Андрушкевич Д.В. (автор) Подпись

Глыбовский П.А. (научный руководитель) Подпись