Исследователи безопасности компании ARMO обнаружили уязвимость в интерфейсе io_uring операционной системы Linux, которая может быть использована руткитами для незаметной работы в системе, обойдя в том числе передовое программное обеспечение безопасности. Руткит — вредоносное ПО, которое предназначено для предоставления нелегетимного доступа к целевому устройству и контроля над ним.

Как сообщает Bleeping Computer, io_uring является интерфейсом ядра Linux, предназначенным для эффективных асинхронных операций ввода-вывода. Этот интерфейс использует кольцевые буферы для постановки в очередь запросов ввода-вывода и обрабатывает их асинхронно.

Однако множество инструментов безопасности не отслеживают операции, связанные с io_uring, что создаёт «слепое пятно» в защите. Уязвимость в io_uring позволяет руткитам выполнять широкий спектр операций, таких как чтение / запись файлов, создание сетевых соединений и изменение разрешений на файлы.

По словам обозревателей источника, это говорит о серьёзной проблеме безопасности, которую необходимо устранить для защиты систем Linux.

Все права защищены

save pdf date >>> 26.01.2026