Проблемы безопасности системы сканирования и печати ОС Linux

Певзнер Александр Ефимович, pzz@apevzner.com
АО Электронная Москва, Нижний Сусальный пер. д. 5 стр 19.
Член OpenPrinting. Автор популярных пакетов ipp-usb и sane-airscan.

Актуальность

Несмотря на тотальную цифровизацию, бумажные документы сохраняют ключевую роль в официальном документообороте. Системы сканирования и печати выступают критическим звеном в формировании документооборота организаций, а утечка информации, проходящей через них, способна привести к катастрофическим последствиям.

Привычно воспринимая принтеры и сканеры как рядовые периферийные устройства, мы склонны недооценивать их сложность. Однако, будучи высокотехнологичными электронными устройствами, функционирующими в тандеме со сложным программным обеспечением на стороне операционной системы, они обладают существенными информационными уязвимостями и могут выступать в качестве мишени для целенаправленных атак.

Цель и фокус исследования

В докладе представлен обзор систем сканирования и печати в среде Linux с точки зрения информационной безопасности. Акцент сделан не на случайных ошибках реализации (например, переполнении буфера), а на уязвимостях, заложенных в архитектуру этих систем и дизайн используемых протоколов.

Векторы атак

Рассуждая о возможных целях атак на системы сканирования и печати, авторы выделяют три наиболее значимых направления:

1. **Выполнение кода с повышенными привилегиями** — за счет использования уязвимостей в сервере печати.
2. **Косвенные атаки на операционную систему** — через компрометацию оборудования. Этому особенно подвержена система сканирования, которая в силу архитектурных особенностей вынуждена предоставлять пользователю прямой доступ к устройствам через USB.
3. **Несанкционированный доступ к информации** — содержащейся в печатаемых и сканируемых документах, с использованием особенностей соответствующих протоколов.

Наиболее опасной и трудно поддающейся защите представляется именно последняя цель.

Архитектура системы сканирования (SANE)

Система сканирования ОС Linux (SANE) устроена просто. Фактически она состоит из набора драйверов (SANE backends), каждый из которых является динамической библиотекой и работает со своим типом сканера. Диспетчер (sane-dll.so) загружает драйверы и распределяет между ними пользовательские запросы.

Драйверы SANE загружаются и исполняются непосредственно в контексте пользовательского прикладного процесса, осуществляющего сканирование (например, графического клиента simple-scan).

USB-сканеры обслуживаются непосредственно драйверами SANE, а не ядерными драйверами. Чтобы обычные пользователи могли работать с ними, правила **systemd-udevd** предоставляют права низкоуровневого доступа к физическому порту.

Архитектура системы печати (CUPS)

Система печати имеет более сложную структуру. Центральную роль здесь играет сервер печати CUPS. На большинстве дистрибутивов CUPS исполняется с правами root и без какой-либо изоляции. Для своей работы он использует вспомогательные компоненты:

- **Бэкенды** — отвечают за низкоуровневую работу с оборудованием, исполняются с правами `root:lp`.
- **Фильтры (cups-filters)** — отвечают за преобразование изображений в формат, поддерживаемый аппаратурой, исполняются с правами `lp:lp`.

Проприетарные драйвера могут устанавливать свои фильтры и свои бэкенды.

Протоколы и тенденции

Поскольку большинство современных принтеров и сканеров подключаются через USB или сеть (Ethernet/WiFi), доклад фокусируется именно на этих вариантах.

В индустрии наблюдается тенденция к переходу на «бездрайверные» технологии, когда оборудование реализует стандартные протоколы из открытых спецификаций. Это позволяет отказаться от специфичных драйверов в пользу единого общесистемного драйвера, поддерживающего все устройства класса. В связи с этим повышенное внимание уделяется именно «бездрайверным» протоколам.

Рассматриваемые протоколы разделены на три группы:

1. **Протоколы обнаружения устройств:**
    - DNS-SD (IETF/Apple)
    - WS-Discovery (WSD/Microsoft)
2. **Протоколы сканирования:**
    - eSCL (IETF/Apple)
    - WS-Scan (WSD/Microsoft)
3. **Протоколы печати:**
    - IPP

- AppSocket (принтер на порту 9100)
- LPD

К «бездрайверным» протоколам относятся eSCL/WS-Scan (сканирование) и IPP (печать). Их общей чертой является использование HTTP в качестве транспорта со всей присущей HTTP инфраструктурой авторизации и защиты контента.

Структура доклада и целевая аудитория

Доклад содержит описание рассматриваемого программного обеспечения и протоколов на уровне, достаточном для понимания, а также анализ возможных уязвимостей. Доклад сопровождается практическими примерами. Все примеры проверены на действующем программном обеспечении и оборудовании.

Предполагаемая целевая аудитория: квалифицированные системные программисты, разработчики и мейнтейнеры операционных систем и их компонент.

Заключение

В настоящее время вопросам информационной безопасности уделяется большое внимание. Достаточно глубоко проработаны вопросы целостности операционной системы, изоляции ее отдельных компонентов, а также устранения уязвимостей, связанных с дефектами программного кода. Однако наблюдается нехватка работ, посвященных системному анализу крупных подсистем в целом.

На примере подсистем сканирования и печати показано: даже если исключить возможность взлома отдельных компонентов и исходить из их функционирования в абсолютно штатном режиме, строго соответствующем спецификациям, этого может оказаться недостаточно для обеспечения гарантий целостности и конфиденциальности пользовательских данных.

Авторы полагают, что другие крупные подсистемы операционной системы заслуживают аналогичного анализа, однако его проведение выходит за рамки настоящего доклада.