DOI 10.36622/1682-7813.2025.28.1.007
УДК 004.056

АНАЛИЗ МЕТОДОВ РЕАЛИЗАЦИЙ И СОСТАВЛЯЮЩИХ АТАК ПОВЫШЕНИЯ ПРИВИЛЕГИЙ НА LINUX-ПОДОБНЫЕ СИСТЕМЫ

Э.В. Бирих, **Н.С. Ершова**

Проведено исследование механизмов повышения привилегий в Linux-подобных системах и методов эксплуатации злоумышленниками уязвимостей в системах. Анализ охватывает распространённые способы эксплуатации различных уязвимостей для реализации атак, а также включает в себя рассмотрение использования злоумышленниками критически важных элементов системы, подверженных данным воздействиям. В ходе исследования были выявлены ключевые аспекты, которые злоумышленники используют для получения несанкционированного доступа и повышения своих привилегий. Полученные результаты представляют собой важную основу для разработки эффективных методов защиты и предотвращения атак в будущем, способствующих укреплению безопасности систем и минимизации рисков, связанных с подобными уязвимостями. Эти основы имеют важное значение для ИБ-специалистов, а особенно для архитекторов безопасности, стремящихся создать более защищенные среды.

Ключевые слова: Linux; операционные системы; атаки повышения привилегий; повышение привилегий; типовые реализации атак повышения привилегий.

Введение

Предотвращение атак повышения привилегий играет важную роль в обеспечении информационной безопасности операционных систем. Для эффективной разработки методов защиты важно понимать принцип реализации атак, целевые файлы и объекты операционных систем. Атаки повышения привилегий могут включать в себя различные действия, такие как попытки получения администраторских прав, доступ к конфиденциальной информации и другие потенциальные угрозы, которые представляют опасность для целостности и конфиденциальности данных. Особенную опасность представляют атаки со стороны легитимных пользователей операционной системы, так как у них есть физический доступ к оборудованию, а также доступ к системе через учетную запись, что облегчает задачу проникновения в сетевой периметр организации. Быстрый и эффективный анализ атак, ускоряет их выявление и предотвращение, а также предотвращает ущерб и минимизирует риски утечки конфиденциальной информации. Цель данной статьи — провести анализ составляющих атак повышения привилегий в Linux-подобных системах и методов их реализации. Эта работа позволит понять типовые способы реализаций атак, уязвимые места в системе, что в дальнейшем послужит основой для формирования методов защиты в зависимости от особенностей конкретной системы. Ведь для построения комплексной системы защиты, важно понимать, как может действовать злоумышленник.

Система привилегий в Linux и основные составляющие атак

Операционная система Linux представляет собой мощную и гибкую систему, используемую во множестве различных контекстов, от серверов до встраиваемых систем. В условиях импортозамещения в России она нашла широкое применение в качестве операционной системы на рабочих станциях сотрудников. В основе Linux лежит ядро, которое управляет аппаратными ресурсами и обеспечивает базовые функции операционной системы, такие как управление памятью, управление процессами и файловыми системами.

В Linux существует концепция пользовательских привилегий, которая определяет уровень доступа к системным ресурсам. Пользователи могут иметь различные уровни привилегий, начиная от

обычного пользователя до суперпользователя (root), который имеет полный доступ ко всем системным ресурсам. Наибольшие привилегии самые критичные и в целях безопасности должны иметься у ограниченного количества администраторов.

Прежде чем приступить к анализу составляющих атак, следует рассмотреть основные понятия, используемые в данной статье.

Ядро Linux — это центральная часть операционной системы, отвечающая за взаимодействие с аппаратным обеспечением и выполнение основных системных задач. Ядро обеспечивает абстракцию между аппаратным обеспечением и пользовательскими приложениями, предоставляя набор системных вызовов для выполнения различных операций [1].

Уязвимость – это слабое место или недостаток в системе, программном обеспечении или сети, которое может быть использовано злоумышленниками для выполнения нежелательных действий. Уязвимости могут возникать из-за ошибок программирования, неправильной конфигурации или недостаточной защиты системы [2].

Эксплуатация уязвимостей – это процесс использования уязвимостей для получения несанкционированного доступа к системе или выполнения вредоносных действий. Эксплуатация может включать различные методы, такие как использование вредоносного кода, подделка запросов или использование специальных инструментов и скриптов.

Атака – это преднамеренное действие, направленное на нарушение работы системы, кражу данных или причинение вреда с использованием уязвимостей [3]. Атаки повышения привилегий — это тип атак, при которых злоумышленник получает доступ к ресурсам или действиям, которые изначально были ему недоступны.

Важно упомянуть, что в соответствии с методикой оценки угроз ФСТЭК России [4], в информационных системах присутствуют два типа нарушителей:

1) внутренние нарушители – это лица, которые имеют легальный доступ к информационной системе организации и могут использовать этот доступ для несанкционированных действий. Внутренние нарушители могут действовать преднамеренно (например, недовольные сотрудники) или непреднамеренно (например, сотрудники, совершающие ошибки из-за недостатка знаний) [5],

2) внешние нарушители – это лица или группы, которые не имеют легального доступа к информационной системе организации и пытаются получить такой доступ извне. Внешние нарушители могут использовать различные методы для взлома систем, такие как эксплойты, фишинг, вредоносное ПО и атаки на уязвимости.

Теперь перейдём к рассмотрению типов атак на повышение привилегий. Горизонтальные и вертикальные атаки на повышение привилегий – это два основных типа атак, используемых для увеличения уровня доступа к системе или данным.

Горизонтальная атака. Этот тип атаки направлен на повышение привилегий внутри одного уровня системы. Например, когда пользователь с низкими привилегиями пытается получить доступ к ресурсам или функциям, которые доступны другому непривилегированному пользователю [6].

Вертикальная атака. Атаки, направленные на повышение привилегий на более высоком уровне системы. Например, пользователь с низкими привилегиями может получить доступ к управлению системой или к критически важным данным, которые обычно доступны только для администраторов или же суперпользователя [7].

Для предотвращения атак важно понимать основные этапы проведения, ведь чем раньше её остановить, тем меньший ущерб будет нанесен. К этапам атак повышения привилегий относят следующие:

1. Начальное проникновение. Атака обычно начинается с нахождения уязвимости в целевой системе, с целью использовать её для получения начального доступа к системе.

2. Закрепление в системе. Например, установка вредоносного программного обеспечения или изменение конфигурации системы для сохранения доступа даже после перезагрузки или обновлений системы.

3. Изучение системы. На этом этапе исследуется система для получения

информации о её структуре, уровне привилегий различных пользователей, конфигурации системных сервисов и установленных средствах защиты.

4. Эксплуатация уязвимостей для повышения привилегий. Злоумышленники использует полученную информацию для нахождения и эксплуатации уязвимостей, которые позволяют ему повысить свои привилегии. Это может включать использование эксплойтов для уязвимостей в ядре системы, системных сервисах или приложениях.

5. Распространение по сети (при необходимости). Если целью атаки является получение контроля над несколькими системами, атакующие могут использовать свой повышенный доступ для проникновения в другие компьютеры в сети [8].

6. Маскирование следов. Для того чтобы избежать обнаружения, хакеры предпринимают меры по маскированию своих действий. Такие как удаление или изменение логов, использование руткитов для скрытия своих процессов и файлов, а также изменение конфигурации системных средств защиты.

7. Поддержание доступа. Злоумышленники могут настраивать механизмы для сохранения доступа к системе на длительное время. Что может включать в себя установку бекдоров или других инструментов, которые позволят ему повторно входить в систему даже после её перезагрузки или обновления.

8. Реализация конечной цели. На последнем этапе атакующие достигают своей конечной цели, которая может включать кражу данных, изменение конфигурации системы, установку вредоносного ПО или отключение средств защиты [9].

Критическая информация о системе для проведения атак

В процессе атак невправленных на повышение привилегий, злоумышленники могут использовать различные критически важные данные и системные параметры для достижения своих целей. Выделим ключевую информацию для операционной системы Linux, на которую в первую очередь нацелены хакеры, и минимальные способы её использования:

- Версия операционной системы. Злоумышленники анализируют версию операционной системы, чтобы определить специфичные для данной версии уязвимости. Определение уязвимых версий позволяет атакующим использовать известные эксплойты.
- Уязвимые пакеты. Определение установленных пакетов, содержащих известные уязвимости, позволяет злоумышленникам запускать атаки на повышение привилегий, используя эксплойты, предназначенные для конкретных версий программного обеспечения.
- Файлы и папки с полным контролем. Обнаружение файлов и папок, к которым злоумышленник имеет возможность изменять доступ, позволяет им изменять конфигурационные файлы и внедрять вредоносный код для дальнейшего получения контроля над системой.
- Подключенные диски. Получение информации о всех подключенных дисках и устройствах хранения данных позволяет атакующим анализировать и извлекать конфиденциальные данные, а также модифицировать файлы для обхода систем безопасности.
- Потенциально конфиденциальные файлы. Определение файлов, содержащих конфиденциальные данные, таких как учетные записи пользователей и пароли, позволяет злоумышленникам получить доступ к важной информации для дальнейших атак на повышение привилегий.
- Сетевая информация. Данные о сетевых интерфейсах и адресной таблице ARP, которые могут быть использованы для сетевых атак.
- Состояние и политики безопасности межсетевого экрана. Анализ информации о настройках и политике межсетевого экрана позволяет злоумышленникам находить способы обхода его защиты и осуществления атак на внутренние ресурсы сети.
- Активные процессы. Список текущих процессов, выполняемых в системе, помогает злоумышленникам выявлять уязвимые приложения и сервисы, которые можно использовать для выполнения вредоносного кода.

• Учетные данные. Хранение и использование учетных записей пользователей позволяют злоумышленникам использовать легитимные учетные записи для повышения привилегий и выполнения команд с повышенными правами.

• Права Sudo. Получение информации о правах Sudo позволяет злоумышленникам формировать список целей и использовать команды с повышенными привилегиями для выполнения вредоносных действий и получения контроля над системой.

• Переменные Path. Изменение параметров окружения, таких как переменные Path, позволяет злоумышленникам перенаправлять выполнение команд на вредоносные программы.

• Docker. Использование контейнеров Docker для обхода механизмов безопасности и выполнения привилегированных команд позволяет получить доступ к системным ресурсам.

• Условия переполнения буфера. Уязвимости, связанные с переполнением буфера, позволяют хакерам выполнять произвольный код и получать контроль над системой.

• Параметры системы. Изменение общих параметров и конфигураций системы предоставляет возможность манипулировать настройками для повышения привилегий и обхода систем безопасности.

Эти векторы представляют собой ключевые точки атаки, которые могут быть использованы злоумышленниками для получения несанкционированного доступа и повышения своих привилегий в системе. Особенно важно защищать перечисленные выше системные составляющие, чтобы предотвратить атаки на повышение привилегий и обеспечить безопасность операционной системы.

Уязвимые точки файловой системы Linux

Также важнейшей составляющей атак на Linux является файловая система и критические файлы и директории, которые часто используются в атаках на повышение привилегий и требуют особого внимания при обеспечении безопасности. Список основных критических файлов и директорий в Linux, описывающий, как злоумышленник может их использовать для реализации атак на повышение привилегий включает в себя:

• Файл /etc/passwd содержит информацию о пользователях системы, включая имена пользователей, UID и домашние директории. Можно попытаться добавить нового пользователя с повышенными привилегиями или изменить существующие записи для получения несанкционированного доступа [10].

• /etc/shadow хранит зашифрованные пароли пользователей и связанную информацию о них. Если получить доступ к этому файлу, то можно попытаться взломать зашифрованные пароли с помощью атак перебора (brute force) или радужных таблиц (rainbow tables).

• Файл /etc/sudoers определяет права доступа пользователей к выполнению команд с повышенными привилегиями с помощью «sudo». Злоумышленник может изменить этот файл, чтобы предоставить пользователю root-доступ или отключить проверку пароля, что позволит выполнять команды с административными правами [10].

• /root/ – домашняя директория пользователя root, содержащая конфиденциальные файлы и конфигурации. Доступ к этой директории может позволить получить важную конфиденциальную информацию и контроль над системой.

• Директория /var/log/ с журналами системных событий и приложений. Злоумышленник может попытаться изменить или удалить журналы для скрытия своей активности и предотвращения обнаружения атаки.

• /boot/ содержит файлы загрузки системы, включая ядро и загрузочный загрузчик GRUB. Изменения в этих файлах могут позволить внедрить вредоносный код, который будет выполняться при загрузке системы.

• Директория для временных файлов /tmp/ может использоваться для хранения вредоносных файлов или выполнения атак типа «символьная ссылка» (symlink attack), перенаправляя легитимные операции на вредоносные файлы.

• /home/ содержит домашние директории всех пользователей системы.

Доступ к этим директориям может позволить получить конфиденциальные данные пользователей и использовать их для дальнейших атак.

- /bin/ и /sbin/ содержат важные системные исполняемые файлы и утилиты. Злоумышленник может заменить или изменить эти файлы для выполнения вредоносных действий с повышенными привилегиями.
- Системные библиотеки /lib/ и /lib64/, используемые приложениями и сервисами. Изменения в этих директориях могут позволить внедрить вредоносный код, который будет выполняться при запуске системных приложений.
- Псевдо-файловая система /proc/, предоставляющая информацию о работающих процессах и системных параметрах. Злоупотребление доступом к этой директории может позволить злоумышленнику получить конфиденциальную информацию о процессах и системе, что можно использовать для дальнейших атак [11].
- Файлы устройств, представляющие различные аппаратные компоненты системы /dev/ можно использовать для несанкционированного доступа к аппаратным ресурсам или создания поддельных устройств.
- Конфигурация загрузочного менеджера GRUB /boot/grub/grub.cfg. Изменения в этом файле могут позволить злоумышленнику внедрить вредоносный код, который будет выполняться при загрузке системы, или предотвратить загрузку системы.
- Файл статического сопоставления IP-адресов и доменных имен /etc/hosts. Злоумышленник может изменить этот файл для перенаправления трафика на вредоносные серверы или для выполнения атак типа «человек посередине» (man-in-the-middle).
- Информация о файловых системах и их монтировании /etc/fstab. Неправильная конфигурация этого файла может привести к сбоям в работе системы, что злоумышленник может использовать для создания условий для дальнейших атак.
- Конфигурации сетевых интерфейсов /etc/network/interfaces. Злоумышленник может изменить сетевые настройки, чтобы перенаправить трафик или отключить сетевые соединения.
- Настройки DNS-серверов /etc/resolv.conf. Изменение этого файла может позволить злоумышленнику перенаправить DNS-запросы на вредоносные серверы.
- Конфигурация сервера SSH /etc/ssh/sshd_config. Неправильная конфигурация может ослабить безопасность удаленного доступа и позволить злоумышленнику получить несанкционированный доступ через SSH.
- Задания cron, выполняемые автоматически по расписанию /etc/cron.d/. Злоумышленник может добавить вредоносные задания cron, которые будут выполняться с повышенными привилегиями.
- Параметры настройки ядра /etc/sysctl.conf. Изменения в этом файле могут позволить злоумышленнику ослабить безопасность системы или изменить её поведение.
- Задания cron для отдельных пользователей /var/spool/cron/. Злоумышленник может добавить вредоносные задания cron для выполнения с повышенными привилегиями.

Злоумышленники могут использовать эти файлы и директории для реализации различных атак на повышение привилегий и других злонамеренных действий. Обеспечение безопасности этих файлов и директорий критически важно для защиты Linux-системы от киберугроз.

Классы атак повышения привилегий

Рассмотрим основные классы атак повышения привилегий, которые могут происходить в Linux-системах с примерами эксплуатации уязвимостей для их реализации:

- Exploit of Sudo. Например, уязвимость CVE-2023-22809, эксплуатация которой является атакой класса «Exploit of Sudo». Эта уязвимость позволяет пользователю с правами sudoedit редактировать любой файл от имени пользователя, указанного в конфигурации runas, путем инъекции вредоносной переменной окружения. Например, можно изменить пароль root в файле /etc/shadow. Эта уязвимость позволяет

пользователю с правами sudoedit редактировать любой файл от имени пользователя, указанного в конфигурации runas, путем инъекции вредоносной переменной окружения. Для версий sudo (<=1.9.12p1). Запускается команда sudoedit, предварительно установив вредоносную переменную окружения EDITOR «EDITOR='vim -- /etc/shadow' sudoedit /etc/custom/service.conf». Это открывает файл /etc/shadow с правами на чтение и запись. Если злоумышленник получает доступ к файлу /etc/shadow, он может изменить пароли всех пользователей, включая root, добавлять новые учетные записи с правами суперпользователя, удалять существующие учетные записи, копировать хэши паролей для восстановления по ним паролей, получая контроль над системой [12].

- Privilege Escalation via Kernel [13]. Например, CVE-2024-26808 — это уязвимость типа use-after-free в ядре Linux, связанная с модулем Netfilter. Атакующий мог использовать неправильную обработку NETDEV_UNREGISTER для повышения привилегий. В ядре Linux, когда сетевое устройство отключается (NETDEV_UNREGISTER), его нужно удалить из цепочки Netfilter. Если этого не сделать, остается старая ссылка на устройство в списке хуков, что может привести к использованию освобожденной памяти. Для реализации такой атаки злоумышленник может создать сетевой пакет, который вызовет отключение сетевого устройства. А затем может использовать освобожденную память для выполнения произвольного кода. В дальнейшем он также может использовать переполнение кэша для записи в другие области памяти, что позволяет ему изменять критические структуры ядра [14].

- Setuid Programs. Программы с setuid устанавливают бит setuid, который позволяет им выполнять код с правами владельца файла, часто root [15]. CVE-2021-3156 (Baron Samedit) была обнаружена в утилите sudo, которая широко используется в Linux для выполнения команд с привилегиями суперпользователя. Уязвимость позволяет локальному пользователю с низкими привилегиями получить root-доступ. Хакер создает специальный ввод, который вызывает переполнение буфера в sudo. Например, он может использовать следующую команду «sudoedit -s '\' `perl -e 'print "A" x 65536'». Команда вызывает переполнение буфера, что позволяет хакеру выполнить произвольный код с привилегиями root. В результате хакер получает доступ к командной оболочке с правами суперпользователя.

- Filesystem Permissions. Неправильная настройка разрешений файловой системы может привести к повышению привилегий. Например, неправильная обработка символьных ссылок (symlinks) позволяет локальным пользователям с низкими привилегиями получить доступ к файлам и каталогам, к которым у них обычно нет доступа, путем создания специальных символьных ссылок. Хакер находит уязвимую систему, на которой установлен уязвимый драйвер файловой системы. Проверяет возможность создания символьных ссылок в уязвимой файловой системе. Хакер создает специальный символьный ссылку, который указывает на файл или каталог с ограниченным доступом. Например, он может создать ссылку на файл с конфиденциальными данными «ln -s /etc/shadow /tmp/malicious_link». Хакер использует созданную символьную ссылку для доступа к защищенному файлу. Далее можно получить доступ к файлу, используя «cat /tmp/malicious_link».

- Web Application Vulnerabilities. Веб-приложения с уязвимостями могут быть использованы для выполнения команд на сервере с повышенными привилегиями. CVE-2024-3094 (Silent Intruder Exploit). Эта уязвимость связана с внедрением вредоносного кода в утилиты XZ Utils, которые используются для сжатия файлов в Linux. Вредоносный код может быть внедрен в версии 5.6.0 и 5.6.1, что делает эту уязвимость особенно опасной. Хакер создает вредоносный пакет, который содержит внедренный код, который, например, может создать исполняемый файл с вредоносным кодом «echo 'echo "I am a malicious payload" > /tmp/malicious_payload' > /tmp/exploit.sh» «chmod +x /tmp/exploit.sh». Хакер использует уязвимость для внедрения вредоносного пакета в систему. Например, он может

использовать команду для сжатия файла с вредоносным кодом «xz -z /tmp/exploit.sh» и запустить исполняемый файл с вредоносным кодом командой «/tmp/exploit.sh». Таким образом, уязвимость в веб-приложениях на Linux может быть использована для внедрения вредоносного кода и получения доступа к системе [16].

Анализ и понимание способов эксплуатации уязвимостей для реализации этих атак позволяет администраторам систем и специалистам по безопасности более эффективно защищать информационные ресурсы. А эффективное противодействие угрозам повышения привилегий является основополагающим компонентом стратегии обеспечения информационной безопасности в современных Linux-системах.

Заключение

В результате проведенного исследования были выявлены и проанализированы различные составляющие атак повышения привилегий на Linux-подобные системы. Каждый из рассмотренных методов атак имеет свои особенности, преимущества и недостатки, которые необходимо учитывать при разработке стратегий защиты.

Продолжение исследования в этой области может быть направлено на более глубокое понимание процессов атак и разработку актуальных методов защиты, учитывающих особенности операционной системы, приложений и файловой системы. Это подчеркивает необходимость постоянного обновления и совершенствования систем безопасности, чтобы оставаться на шаг впереди злоумышленников.

Понимание и эффективное предотвращение атак повышения привилегий играют ключевую роль в обеспечении безопасности Linux-подобных систем. Комплексный подход к анализу таких атак, включая их обнаружение, анализ и разработку мер по предотвращению, позволяет значительно повысить уровень защиты и быстроту реагирования на инциденты. Внедрение надежных методов защиты является важным шагом в обеспечении безопасности информационных систем и защите от потенциальных угроз, а для их разработки важно понимать, на что могут быть направлены атаки, и как их могут реализовать.

Список литературы

1. Elbrus Bootcamp. Что такое Linux? / URL: https://elbrusboot.camp/blog/chto-takoie-linux/ (дата обращения: 25.11.2024).

2. Кибрарий. Уязвимость. / URL: https://www.sberbank.ru/ru/person/kibrary/vocabulary/uyazvimost (дата обращения: 27.11.2024).

3. Difference between Threat and Attack. / URL: https://www.geeksforgeeks.org/difference-between-threat-and-attack/ (дата обращения: 27.11.2024).

4. Методический документ. Методика оценки угроз безопасности информации. Утвержден ФСТЭК России 05.02.2021 [Сайт: ФСТЭК России.] / URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (дата обращения: 30.11.2024).

5. Бирих, Э.В. Современные проблемы обеспечения внутренней безопасности распределенной сети органов государственной власти / Э.В. Бирих, А.С. Гаврилов, Е.Н. Сацук // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018) : VII Междунар. науч.-техн. и науч.-методич. конф. Сб. науч. статей. В 4-х томах, Санкт-Петербург, 28 февраля 01 2018 года / Под ред. С.В. Бачевского. Т.1. СПб: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2018. С. 105.

6. Никишова А. В. Программный комплекс обнаружения атак на основе анализа данных реестра // Вестник Волгоградского государственного университета. Серия 10. Инновационная деятельность. 2012. № 6. С. 152–155.

7. H. Aljifri, M. Smets, and A. Pons, IP traceback using header compression, Computers &Security 22 (2003). No. 2. P. 136–151.

8. Positive Technologies. Этапы APT-атак. / URL: https://www.ptsecurity.com/ru-ru/research/knowledge-base/etapy-celevyh-atak/ (дата обращения: декабрь 2024).

9. Лапсарь А.П. Повышение устойчивости объектов критической

информационной инфраструктуры к целевым компьютерным атакам / А.П. Лапсарь, С.А. Назарян, А.И. Владимирова // Вопросы кибербезопасности. 2022. №2 (48). С. 39-51.

10. Управление пользователями. URL: https://firstvds.ru/technology/linux-user-management (дата обращения: 19.12.2024).

11. Файловая система proc в Linux. URL: https://losst.pro/fajlovaya-sistema-proc-v-linux (дата обращения: 19.12.2024).

12. Уязвимость в sudo, позволяющая изменить любой файл в системе. URL: https://www.opennet.ru/opennews/art.shtml?num=58507 (дата обращения: 20.12.2024).

13. Richard Dezso. Linux Privilege Escalation Techniques for Hacking. URL: https://www.stationx.net/linux-privilege-escalation/ (дата обращения: 22.12.2024).

14. CVE-2024-26808. Common Vulnerabilities and Exposures. URL: https://www.suse.com/security/cve/CVE-2024-26808.html (дата обращения: 23.12.2024).

15. Использование SETUID, SETGID и Sticky bit для расширенной настройки прав доступа в операционных системах Linux. URL: https://ruvds.com/ru/helpcenter/suid-sgid-sticky-bit-linux/ (дата обращения: 24.12.2024).

16. CVE-2024-3094: уязвимость в библиотеке XZ Utils. URL: https://axiomjdk.ru/announcements/2024/04/04/cve-2024-3094-ujazvimost-v-biblioteke-xz-utils/ (дата обращения: 24.12.2024).

Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича

St. Petersburg State University of Telecommunications named
after Professor M.A. Bonch-Bruevich

Поступила в редакцию 20.01.2025

Информация об авторах

Бирих Эрнест Владимирович – старший преподаватель кафедры ЗСС Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, e-mail: be1982@mail.ru

Ершова Наталья Сергеевна – студент, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, e-mail: Ershova.for.work@yandex.ru

ANALYSIS OF IMPLEMENTATION METHODS AND COMPONENTS OF PRIVILEGE ESCALATION ATTACKS ON LINUX-LIKE SYSTEMS

E.V. Birikh, N.S. Ershova

A study of privilege escalation mechanisms in Linux-like systems and methods of exploiting vulnerabilities in systems by intruders has been conducted. The analysis covers common ways of exploiting various vulnerabilities for attacks, and also includes consideration of the use of critical system elements exposed to these impacts by attackers. The study identified key aspects that attackers use to gain unauthorized access and enhance their privileges. The results obtained provide an important basis for developing effective methods of protecting and preventing attacks in the future, contributing to strengthening system security and minimizing the risks associated with such vulnerabilities. These fundamentals are important for information security professionals, and especially for security architects seeking to create more secure environments.

Keywords: Linux; operating systems; privilege escalation attacks; privilege escalation; typical implementations of privilege escalation attacks.

Submitted 20.01.2025

Information about authors

Ernest V. Birikh – senior lecturer at the Department of ZSS of the St. Petersburg State University of Telecommunications named after Prof. M.A. Bonch-Bruevich, e-mail: be1982@mail.ru

Natalya S. Ershova – student, St. Petersburg State University of Telecommunications named after Prof. M.A. Bonch-Bruevich, e-mail: Ershova.for.work@yandex.ru