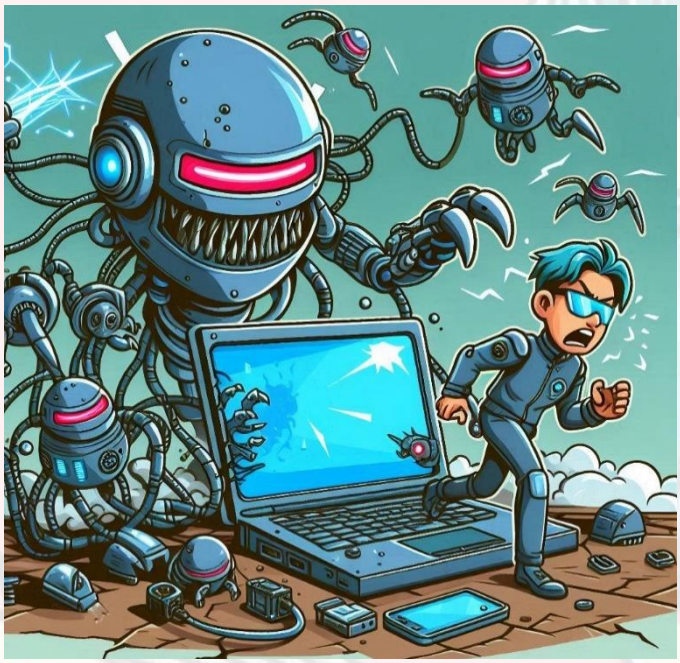

Аннотация – документ содержит анализ CVE-2024–2111, уязвимости в Oracle VM VirtualBox, влияющей на хосты Windows. Анализ охватывает различные аспекты уязвимости, включая её технические детали, механизмы использования, потенциальное воздействие на различные отрасли.

Этот документ содержит высококачественное описание уязвимости, предлагая ценную информацию специалистам по безопасности и другим заинтересованным сторонам из различных отраслей. Анализ полезен для понимания рисков, связанных с CVE-2024–2111, и внедрения эффективных мер по защите систем от потенциальных атак.

I. Введение

CVE-2024-2111 – это уязвимость системы безопасности, выявленная в Oracle VM VirtualBox, которая, в частности, затрагивает хосты Windows и присутствует в версиях до версии 7.0.16. Это позволяет злоумышленнику с низкими привилегиями, имеющему доступ для входа в систему, к инфраструктуре, где выполняется Oracle VM VirtualBox, потенциально захватить систему

Злоумышленник, использующий эту уязвимость, может получить несанкционированный контроль над уязвимой виртуальной машиной Oracle VirtualBox. Конкретный технический механизм включает локальное повышение привилегий посредством перехода по символической ссылке, что может привести к произвольному удалению и перемещению файла.

II. Технические детали

- **Тип уязвимости**: локальное повышение привилегий (LPE) позволяет злоумышленнику с низкими привилегиями, у которого уже есть доступ к системе, получить более высокие привилегии.
- **Вектор атаки и сложность**: Вектор CVSS 3.1 для этой уязвимости равен (CVSS: 3.1/AV:L/AC:L/PR: L/ UI: N/ S:U/C:H/I: H /A:H). Это указывает на то, что вектор атаки локальный (AV:L), что означает, что злоумышленнику необходим локальный доступ к хосту. Сложность атаки низкая (AC:L), и никакого взаимодействия с пользователем (UI:N) не требуется. Требуемые привилегии невелики (PR:L), что предполагает, что базовые привилегии позволяют воспользоваться этой уязвимостью.
- **Воздействие**: Все показатели воздействия на конфиденциальность, целостность и доступность оцениваются как высокие (C:H/I:H/A:H), что указывает на то, что эксплойт может привести к полному нарушению конфиденциальности, целостности и доступности уязвимой системы.
- **Способ эксплуатации**: Уязвимость реализуется атакой с символическими ссылкам (symlink). Это включает в себя манипулирование ссылками для перенаправления операций, предназначенных для легитимных файлов или каталогов, на другие подконтрольные цели, приводя к произвольному удалению или перемещению файла, и позволяя выполнять произвольный код с привилегиями.
- **Конкретный механизм**: Уязвимость конкретно связана с манипуляциями с файлами журналов системной службой VirtualBox (VboxSDS). Служба, работающая с системными привилегиями, управляет файлами журнала в каталоге, не имеющими строгого контроля доступа, что потенциально приводит к повышению привилегий. Служба выполняет операции переименования / перемещения файлов рекурсивно, что позволяет этим злоупотреблять.
- **Меры по устранению этой уязвимости**: Пользователям рекомендуется обновить свои установки Oracle VM VirtualBox до версии 7.0.16 или более поздней, которая содержит необходимые исправления для устранения этой уязвимости

III. Подверженные отрасли

Oracle VM VirtualBox широко используется в различных отраслях благодаря своим возможностям виртуализации, которые позволяют запускать несколько операционных систем на одном физическом компьютере.

A. Информационные технологии и разработка программного обеспечения

- **Инфраструктура виртуализации**: ИТ-компании и поставщики облачных услуг часто используют VirtualBox для создания виртуальных сред и управления ими. Использование уязвимости приводит к несанкционированному доступу к виртуальным машинам и контролю над ними, нарушению целостности и конфиденциальности размещённых служб и данных.
- **Нарушение работы сервиса**: успешная атака приводит к нарушению работы сервисов, предоставляемых клиентам, что приведёт к простою и потенциальным финансовым потерям.

B. Образование и профессиональная подготовка

- **Данные исследований**: VirtualBox используются в исследовательских и академических целях. Несанкционированный доступ ставит под угрозу данные исследований и интеллектуальную собственность.
- **Доступность услуг**: Сбой в работе виртуальных сред может повлиять на платформы онлайн-обучения и административные функции.

C. Кибербезопасность и криминалистика:

- **Безопасность данных**: Специалисты по кибербезопасности и криминалистике используют виртуальные машины для анализа вредоносных программ, проведения тестов на проникновение и forensics-расследований в изолированных средах. Скомпрометированный VirtualBox приводит к несанкционированному доступу к конфиденциальным данным и инструментам, что приводит к нарушению целостности расследований.
- **Несанкционированный доступ**: получение доступа к forensics-инструментам и данным с целью манипуляции доказательствами или срыва текущих расследований через повышение привилегий.

D. Предприятие и бизнес:

- **Данные клиентов**: Предприятия используют VirtualBox для различных целей, включая разработку программного обеспечения, тестирование и запуск устаревших приложений. Успешный эксплойт приводит к доступу к корпоративным данным, интеллектуальной собственности и важным бизнес-приложениям.
- **Операционные последствия**: утечка данных, потеря конфиденциальной информации и нарушение бизнес-операций, и финансовый и репутационный ущерб.

E. Демонстрации продукции и продажи:

- **Данные о клиентах**. VirtualBox часто используется для демонстрации продукции и презентаций продаж, сорвать демонстрации, получить доступ к программному обеспечению или манипулировать демонстрационной средой.
- **Влияние на бренд**: потеря доверия клиентов, потенциальному раскрытию проприетарного программного обеспечения и негативным последствиям для продаж и маркетинговых усилий.

F. Промышленная автоматизация:

- **Автоматизация**: В промышленной автоматизации VirtualBox используется для моделирования и тестирования систем автоматизации перед развёртыванием. Скомпрометированный VirtualBox приводит к несанкционированному доступу к промышленным системам управления, что потенциально приведёт к сбоям в производственных процессах.
- **Перебои в обслуживании**: это может привести к простою производства, угрозе безопасности и финансовым потерям из-за сбоев в производственных операциях.

G. Удалённая работа и виртуальные рабочие столы:

- **Конфиденциальные данные**: VirtualBox широко используется для предоставления виртуальных рабочих столов удалённым работникам. Использование уязвимости позволяет злоумышленникам получить контроль над виртуальными рабочими столами, получить доступ к конфиденциальным корпоративным данным и нарушить работу удалённых рабочих мест.
- **Утечка данных**: приводит к утечке данных, снижению производительности и повышению рисков безопасности для удалённых сотрудников и организаций, в которых они работают.

H. Финансовые услуги:

- **Безопасность данных**: Финансовые учреждения используют виртуализацию для изоляции конфиденциальных данных и приложений. Получение системных привилегий приводит к доступу, изменению, удалению конфиденциальные финансовые данные, и финансовым последствиям.
- **Комплаенс-риски**: Нарушения могут привести к несоблюдению финансовых положений и стандартов, привлечению штрафных санкций и нанесению ущерба репутации.

I. Здравоохранение:

- **Данные о пациентах**: Поставщики медицинских услуг используют виртуализированные среды для управления записями пациентов и другой конфиденциальной информацией. Использование уязвимости приводит к несанкционированному доступу к данным пациента, нарушая законы о конфиденциальности, такие как HIPAA.
- **Операционные последствия**: Системные преобразования могут нарушить работу важнейших служб здравоохранения, что повлияет на уход за пациентами и операционную эффективность.

J. Правительство и оборона:

- **Национальная безопасность**: Правительственные учреждения и оборонные организации используют виртуализацию для безопасных и эффективных операций. Нарушение приводит к несанкционированному доступу к секретной информации, и угрозе национальной безопасности.
- **Сбои в работе**: скомпрометированные системы могут нарушить работу основных государственных служб и оборонных операций.

IV. Технические подробности

Основной причиной CVE-2024–2111 в Oracle VM VirtualBox является уязвимость локального повышения привилегий, которая возникает из-за неправильной обработки символических ссылок и файловых операций в среде VirtualBox.

- **Переход по символической ссылке**: Уязвимость позволяет использовать переход по символической ссылке, когда VirtualBox, работающий от имени NT AUTHORITY \SYSTEM, пытается переместить или удалить файлы журнала в каталоге C:\ProgramData\VirtualBox. Этот каталог и его операции доступны для записи всем пользователям, чего не должно быть в случае операций, выполняемых с привилегиями системного уровня.
- **Неправильное обращение с файлами**: VirtualBox управляет файлами журналов, перемещая их для создания резервных копий и удаляя самый старый журнал, если существует более десяти журналов. Эта операция выполняется без надлежащей проверки, чтобы гарантировать, что файлы, с которыми манипулируют, не связаны вредоносным образом с другими критически важными системными файлами или каталогами.
- **Небезопасные разрешения**: Этот каталог C:\ProgramData\VirtualBox наследует разрешения, которые позволяют всем пользователям создавать и изменять файлы. Этот параметр с ограниченными правами доступа позволяет пользователям с низкими привилегиями создавать символические ссылки, которые могут перенаправлять файловые операции, предназначенные для файлов журналов, в любой другой файл или каталог, что приводит к несанкционированным действиям, выполняемым с повышенными привилегиями

V. Схема атаки и сценарий

CVE-2024-2111 – уязвимость локального повышения привилегий в Oracle VM VirtualBox, конкретно затрагивающая хосты Windows.

A. Схема атаки

- **Первоначальный доступ и настройка среды**: Злоумышленник должен иметь права пользователя низкого уровня и доступ для входа в систему, в которой установлен Oracle VM VirtualBox. Затронутые версии предшествуют версии 7.0.16.
- **Использование перехода по символическим ссылкам**: Суть уязвимости заключается в использовании перехода по символическим ссылкам в среде VirtualBox. Это позволяет злоумышленнику выполнять несанкционированные действия, такие как произвольное удаление и перемещение файлов.
- **Манипулирование файлами журналов**: VirtualBox пытается управлять файлами журналов в каталоге C:\ProgramData\VirtualBox. Эти файлы журнала обрабатываются системой с повышенными привилегиями. Система пытается переместить эти файлы журналов для их резервного копирования, сохраняя только последние 10 журналов и пытаясь удалить 11-й журнал.
- **Повышение привилегий**: Манипулируя символическими ссылками или самими файлами журнала, злоумышленник может заставить систему выполнять произвольные действия с привилегиями системного уровня.
- **Захват системы**: как только злоумышленник повысит свои привилегии до системного уровня, он может выполнять дальнейшие вредоносные действия, потенциально приводящие к полному захвату системы.

B. Сценарий атаки

1) Начальная настройка

- **Окружающая среда**: необходим доступ к системе Windows, в которой запущена уязвимая версия Oracle VM VirtualBox (до версии 7.0.16).
- **Разрешения**: низкоуровневый пользовательский доступ с возможностью входа в систему.

2) Этапы эксплуатации

- **Определение целевой каталог**: идентификация каталога C:\ProgramData\VirtualBox, который используется VirtualBox для хранения файлов журналов и доступен для записи всем пользователям.
- **Создание символических ссылок**: создание символических ссылок каталоге C:\ProgramData\VirtualBox для перенаправления файловых операций (перемещение или удаление) на критически важные системные файлы или каталоги.
- **Запуск файловых операций**:
  - **Операция перемещения**: когда VirtualBox пытается переместить файл журнала, он вместо этого перемещает целевой файл, что потенциально приводит к несанкционированному перемещению файлов.
  - **Операция удаления**: когда VirtualBox пытается удалить старый файл журнала, вместо этого он удаляет целевой системный файл.
- **Повышение привилегий**: манипулируя этими файловыми операциями, злоумышленник может выполнять действия, которые обычно ограничены учётными записями с более высокими привилегиями. Это может привести к повышению привилегий до NT AUTHORITY\SYSTEM, самого высокого уровня привилегий в системах Windows.

3) Послеэксплуатации

- **Контроль над системой**: злоумышленник с системными привилегиями:

- Выполняет произвольные команды с повышенными привилегиями.
- Получает доступ к любому файлу в системе и изменяет его.
- Устанавливает вредоносного программного обеспечения или бэкдоров.
- Создаёт новые учётные записи пользователей с правами администратора.

- **Закрепление и распространение**: далее возможно закрепление в скомпрометированной системе с последующим распространением, чтобы скомпрометировать дополнительные системы.

VI. POC

В репозитории GitHub для CVE-2024–2111, размещённом mansk1es, размещён POC локального повышения привилегий

- **Уязвимый компонент**: Уязвимость конкретно влияет на то, как VirtualBox обрабатывает файлы журналов. VirtualBox, работающий от имени NT AUTHORITY \ SYSTEM, пытается переместить файлы журналов внутри C:\ProgramData\VirtualBox создать их резервную копию с помощью порядковой системы, сохраняя максимум 10 журналов. Когда количество журналов превышает это ограничение, VirtualBox пытается удалить 11-й журнал, также от имени NT AUTHORITY\SYSTEM.
- **Механизм использования**: Использованию этой уязвимости способствует тот факт, что каталог C:\ProgramData\VirtualBox доступен для записи всеми пользователями. Это позволяет использовать процесс перемещения и удаления файлов журнала для повышения привилегий. Уязвимость выявляет две ошибки, связанные с этим процессом, которые могут привести к повышению привилегий.
- **Повышение привилегий**: Используя уязвимость, символической ссылки, приводит к манипулированию файловыми операциями, выполняемыми VirtualBox с правами системного уровня, для достижения произвольного удаления или перемещения файлов. Это может привести к несанкционированным действиям

Репозиторий GitHub для CVE-2024–2111 предоставляет сценарии проверки концепции (PoC), которые демонстрируют уязвимость локального повышения привилегий в Oracle VM VirtualBox. Скрипты находятся в каталогах VirtualBoxLPE_move и VirtualBoxLPE_del.

Оба сценария демонстрируют, как манипулирование файловыми операциями (перемещение и удаление) с помощью символических ссылок может привести к повышению привилегий, позволяя пользователю с низкими привилегиями выполнять действия, обычно зарезервированные для системных процессов с более высокими привилегиями. Сценарии служат практической демонстрацией уязвимости, подчёркивая необходимость обеспечения безопасности файловых операций и проверки символических ссылок в таких приложениях, как VirtualBox

A. Входные данные для скриптов

Скрипты предназначены для использования уязвимости в Oracle VM VirtualBox на хостах Windows.

- Путь к целевому каталогу (C:\ProgramData\VirtualBox), в котором VirtualBox управляет файлами журналов.
- Параметры или конфигурации, имитирующие операции, выполняемые VirtualBox, такие как перемещение или удаление файлов журналов.

1) VirtualBoxLPE_move:

Сценарий требует ввода данных, указывающих, какие файлы журнала следует переместить, а также новое местоположение или способ, которым эти файлы должны быть перемещены. Входные данные также включают создание символических ссылок, которые перенаправляют эти операции на непреднамеренные цели.

2) VirtualBoxLPE_del:

Как и сценарий перемещения, сценарий удаления также подразумевает какие файлы журнала удалять. Сценарий также включает создание символических ссылок, которые приводят к тому, что операция удаления затрагивает непреднамеренные файлы или каталоги.

B. Результаты после запуска скриптов

1) VirtualBoxLPE_move:

После запуска результатом является перемещение файлов журнала способом, использующим уязвимость, связанную с символической ссылкой, и приводит к несанкционированному перемещению файлов, потенциально позволяя перемещать системные файлы или другие конфиденциальные файлы в места со слабыми разрешениями, повышая их привилегии.

2) VirtualBoxLPE_del:

Результатом запуска удаления будет удаление файлов или каталогов, которые изначально не предназначались для удаления. Используя символическую ссылку, происходит перенаправление процесса удаления для удаления критически важных системных файлов или других защищённых данных, что приведёт к нестабильности системы или дальнейшим нарушениям безопасности.