I. Введение

CVE-2024-0204 представляет собой уязвимость для обхода аутентификации в продукте Fortra's GoAnywhere. MFT Эта уязвимость позволяет злоумышленнику, не прошедшему проверку подлинности, создать пользователя с правами администратора для приложения с возможностью удалённой эксплуатации (CWE-425).

Уязвимость затрагивает Fortra GoAnywhere MFT версий 6.x начиная с 6.0.1 и версий 7.x до 7.4.1 и также существует PoC код эксплоита. Исправление в версии 7.4.1 было выпущено 7 декабря 2023 года. Что касается ландшафта угроз, то в 2023 году приложения для передачи файлов были главной мишенью злоумышленников, что подчёркивает важность обеспечения безопасности таких приложений.

Из опубликованной рекомендации компании следует, что уязвимость можно устранить, удалив /InitialAccountSetup.xhtml и перезапустив службу. Для экземпляров, развёрнутых в контейнере, файл может быть заменён пустым файлом с последующим перезапуском службы.

II. GoAnywhere Managed File Transfer (MFT)

GoAnywhere MFT – это программное решение, которое упрощает для централизации, упрощения и автоматизации перемещения данных, обмена данными между системами, сотрудниками, клиентами и торговыми партнёрами.

GoAnywhere MFT может быть развернут в различных средах, локально, в облаке на таких платформах, как Microsoft Azure и AWS, или в гибридных средах.

GoAnywhere MFT поддерживает широкий спектр протоколов для безопасной передачи файлов, включая SFTP (FTP по SSH), FTPS (FTP по SSL/TLS), SCP (безопасное копирование по SSH), HTTP/s, AS2, AS3, AS4 и другие. Он также предоставляет более 60 различных задач, которые могут быть объединены в рабочие процессы без необходимости программирования или написания сценариев.

В дополнение к своим основным возможностям передачи файлов GoAnywhere MFT также включает функции защиты паролем, двухфакторной аутентификации и интеграции с различными другими системами и приложениями.

III. Отраслевое применение решения

GoAnywhere MFT широко используется в различных секторах благодаря функциональности безопасного автоматизировать обмен данными:

- Информационные технологии и услуги
- Программное обеспечение для компьютеров
- Финансовые услуги
- Медицинские услуги и Здравоохранение
- Обрабатывающая промышленность
- Конслатинг.

В сфере информационных технологий и услуг GoAnywhere MFT используется для интеграции с веб- и облачными приложениями, обеспечивая безопасность данных и автоматизированную передачу файлов с использованием централизованного подхода корпоративного уровня. Его также можно использовать для стандартизации процессов передачи файлов, уменьшая необходимость привлечения групп разработчиков для разработки отдельных решений:

- **Интеграция с веб-и облачными приложениями**: это помогает безопасно интегрировать передачу файлов с веб-и облачными приложениями.
- **Централизация процессов передачи файлов**: GoAnywhere MFT предоставляет централизованную платформу для управления всеми операциями передачи файлов, уменьшая необходимость участия команд разработчиков
- **Автоматизация передачи файлов**: автоматизирует повторяющиеся и сложные задачи по передаче файлов, экономя время и уменьшая количество ошибок.
- **Повышение безопасности**: решение предлагает функции безопасности корпоративного уровня, помогая компаниям, оказывающим ИТ-услуги, защищать конфиденциальные данные во время передачи.

В сфере компьютерного программного обеспечения GoAnywhere MFT может использоваться для автоматизации и обеспечения безопасности передачи файлов, уменьшая потребность «ручного применения» в пользовательских сценариях. Его также можно использовать для создания, редактирования и мониторинга

заданий на передачу файлов, а также для выполнения различных рабочих процессов и переводов данных.

- **Автоматизация распространения программного обеспечения**: Безопасная автоматизация распространения обновлений программного обеспечения и исправлений среди клиентов.
- **Совместная работа**: обеспечение безопасной совместной работы между разработчиками, особенно при работе с исходным кодом и другими конфиденциальными данными.
- **Соответствие нормативным требованиям**: Оказание помощи компаниям-разработчикам ПО в соблюдении требований к разработке программного обеспечения и обработке данных.

В сфере финансовых услуг GoAnywhere MFT используется для защиты конфиденциальных данных клиентов и выполнения требований соответствия. Это помогает контролировать обмен конфиденциальными данными о держателях карт и отслеживать перемещения файлов для упрощения аудита. Например, Sentinel Benefits & Financial Group использует GoAnywhere MFT для создания и редактирования заданий на передачу файлов, мониторинга безопасности, выполнения различных рабочих процессов.

- **Безопасные транзакции**: Автоматизация и защита финансовых транзакций, обеспечение защиты конфиденциальных данных.
- **Соответствие требованиям**: Соблюдение требований, таких как PCI DSS, для защиты данных о держателях карт.
- **Эффективная обработка данных**: оптимизация процесса создания, редактирования и мониторинга заданий на передачу файлов, на примере Sentinel Benefits & Financial Group.

В отрасли здравоохранения GoAnywhere MFT может использоваться для безопасной передачи данных пациентов и другой конфиденциальной информации, помогая организациям здравоохранения соответствовать таким требованиям как HIPAA. Его также можно использовать для автоматизации передачи файлов, уменьшая потребность в ручных процессах с целью повышения эффективности.

- **Соблюдение требований медицинского сектора**: обеспечение соответствия передачи данных медицинским требованиям, таким как HIPAA.
- **Защита данных пациента**: безопасная передача медицинской информации пациента (PHI) при соблюдении правил HIPAA.
- **Безопасный обмен данными о пациентах**: безопасный обмен данными о пациентах между поставщиками медицинских услуг, страховщиками и другими заинтересованными сторонами.
- **Функциональная совместимость**: облегчение обмена медицинскими данными между различными системами и организациями.
- **Автоматизация передачи медицинских данных**: Автоматизация передачи электронных медицинских записей (EHRs), результатов лабораторных исследований и других важных медицинских данных.
- **Автоматизация рабочих процессов в сфере здравоохранения**: автоматизация передачи результатов лабораторных исследований, платёжной информации и других данных, связанных со здравоохранением.

В обрабатывающей промышленности GoAnywhere MFT может использоваться для автоматизации и обеспечения безопасности передачи файлов дизайна, производственных данных и другой конфиденциальной информации. Его также можно использовать для интеграции с другими системами и приложениями, повышая эффективность и уменьшая потребность в ручных процессах.

- **Безопасная передача файлов**: защита передачи конфиденциальных производственных файлов.
- **Интегрированные цепочки поставок**: Интегрированные цепочки поставок для эффективного обмена данными при взаимодействии с партнёрами.
- **Автоматизация производственных процессов**: автоматизация передачи производственных данных, таких как уровень запасов, данные о заказе и отслеживание отгрузки.

В консалтинговой сфере GoAnywhere MFT может использоваться для безопасной передачи конфиденциальных клиентских данных и другой информации. Его также можно использовать для автоматизации передачи файлов, уменьшая потребность в ручных процессах и повышая эффективность.

- **Безопасность клиентских данных**: обеспечение безопасной передачи конфиденциальных клиентских данных во время проведения консультационных мероприятий.
- **Проектное сотрудничество**: Обеспечение безопасной совместной работы над проектами, которые предполагают обмен данными между консультантами и клиентами.
- **Эффективность и автоматизация**: Автоматизация обмена данными и отчётами с клиентами, повышение эффективности и сокращение ручного труда.

IV. Первопричина CVE

Основная причина CVE-2024-0204 идентифицирована как CWE-425: Forced Browsing. Эта уязвимость возникает, когда веб-приложение некорректно обеспечивает авторизацию скриптов или файлов, позволяя обходить

механизмы аутентификации и получать несанкционированный доступ.

Эксплойт эксплуатирует проблему «path traversal», которая представляет собой тип уязвимости в системе безопасности, позволяющей получить доступ к файлам и каталогам, хранящимся за пределами корневой web-папки. В частности, уязвимость GoAnywhere Fortra позволяет не прошедшему проверку подлинности манипулировать переменными, которые ссылаются на файлы для доступа к произвольным файлам и каталогам, хранящимся в файловой системе». В случае CVE-2024-0204 это позволяет получить доступ к уязвимому файлу /InitialAccountSetup.xhtml и создать пользователя с правами администратора (на чтение и запись и выполнение команд).

Это позволяет эффективно обойти существующие требования к аутентификации и авторизации, поскольку злоумышленнику не нужно предоставлять какие-либо действительные учётные данные для получения административного доступа к системе. Эта уязвимость представляет высокий риск для клиентов, у которых есть доступный через Интернет портал администратора.

V. Воздействие CVE и затронутые системы

Влияние CVE-2024-0204 на пользователей MFT GoAnywhere значительно из-за критического характера уязвимости:

- **Создание неавторизованных пользователей-администраторов**: уязвимость позволяет злоумышленнику, не прошедшему проверку подлинности, создать пользователя-администратора, что может привести к несанкционированному доступу к системе
- **Возможность утечки данных**: Имея административный доступ, злоумышленники могут получить доступ к конфиденциальным данным, что может привести к утечке данных
- **Развёртывание вредоносного ПО**: Злоумышленники с правами администратора могут внедрять вредоносное ПО, в том числе программы-вымогатели, которые могут нарушить работу и привести к финансовым потерям
- **Полный захват системы**: Создание пользователей уровня администратора может позволить злоумышленникам получить полный контроль над уязвимой системой
- **Риск вымогательства**: Учитывая простоту использования, существует риск вымогательства, поскольку злоумышленники потенциально угрожают опубликовать конфиденциальные данные, если они не получат платёж
- **Нарушение работы**: Несанкционированный доступ и потенциальные последующие атаки могут нарушить нормальную работу затронутых организаций
- **Соблюдение требований и юридические проблемы**: Организации, пострадавшие от нарушения, вызванного этой уязвимостью, могут столкнуться с проблемами соблюдения требований и юридическими последствиями

GoAnywhere MFT имеет оценку CVSS 9,8; разница между оценкой CVSS, равной 9,8 и 10,0 в первую очередь заключается в метрике "Scope" в системе оценки CVSS. Оценка CVSS, равная 10,0 указывает на то, что уязвимость имеет наиболее серьёзные показатели воздействия и возможности использования, и её воздействие выходит за рамки самого уязвимого компонента, затрагивая также другие компоненты. Оценка CVSS, равная 9,8, также представляет уязвимость с наиболее серьёзными показателями эксплуатируемости и воздействия, но её влияние не распространяется за пределы уязвимого компонента.

Проще говоря, оценка CVSS, равная 10,0, предполагает уязвимость, которая может нанести более масштабный ущерб всей системе, потенциально ставя под угрозу дополнительные системы за пределами начальной точки эксплуатации. Оценка 9,8, хотя и остаётся критической, указывает на уязвимость, которая ограничивается затронутым компонентом и не способна влиять на другие части системы.

VI. Схема атаки и сценарий

Уровень сложности атаки CVE-2024-0204 низкий. Это означает, что условия, необходимые для использования уязвимости, нетрудно достичь, и атака может проводиться без каких-либо особых условий. Низкий уровень сложности в сочетании с критической серьёзностью уязвимости делает её серьёзной проблемой безопасности.

A. Схема атаки

Схема атаки для CVE-2024-0204, уязвимости обхода аутентификации в MFT GoAnywhereFortra, выглядит следующим образом:

- **Первоначальный доступ**: Злоумышленник, не прошедший проверку подлинности, получает доступ к порталу администрирования MFT GoAnywhere. Это возможно из-за проблемы с обходом пути, которую представляет эта уязвимость
- **Эксплуатация**: злоумышленник использует проблему с обходом пути, чтобы получить доступ к /InitialAccountSetup.xhtml
- **Создание пользователя-администратора:** как только злоумышленник получит доступ к InitialAccountSetup.xhtml, он может создать пользователя-администратора со всеми соответствующими права администратора на чтение и запись, а также возможности выполнения команд
- **Возможное дальнейшее использование**: Имея административный доступ, злоумышленник потенциально может получить доступ к конфиденциальным данным, внедрить вредоносное ПО или получить полный контроль над системой

B. Сценарий атаки

Возможные сценарии атак для CVE-2024-0204 могут включать:

- **Атаки программ-вымогателей**: Учитывая историю использования продуктов для передачи файлов в качестве шлюзов для атак программ-вымогателей, есть опасения, что CVE-2024-0204 может быть использован аналогичным образом. Злоумышленники могли использовать доступ администратора, полученный благодаря этой уязвимости, для развёртывания программ-вымогателей, шифрующих файлы и требующих выкуп за их расшифровку
- **Эксфильтрация данных**: злоумышленники могут использовать доступ администратора для получения конфиденциальных данных. Это могут быть личные данные, финансовая информация или служебные бизнес-данные.
- **Захват системы**: имея доступ администратора, злоумышленники потенциально могут получить полный контроль над системой. Это может быть использовано для нарушения работы, развёртывания дополнительного вредоносного ПО или использования системы в качестве стартовой площадки для дальнейших атак
- **Вымогательство**: Злоумышленники могут угрожать опубликовать конфиденциальные данные, если они не получат оплату. Это может нанести особый ущерб организациям, которые обрабатывают конфиденциальные данные клиентов или несвободную информацию
- **Саботаж**: В более деструктивном сценарии злоумышленники могут использовать доступ администратора для удаления или изменения данных, нарушения операций или иного саботажа организации. Это может привести к значительным последствиям для бизнеса, включая простои и финансовые потери

VII. Последствия

Потенциальные последствия атаки с использованием CVE-2024-0204 на пользователей MFT GoAnywhere:

- **Несанкционированный административный доступ**: злоумышленники могут создать пользователя-администратора через портал администрирования без надлежащей авторизации, что приводит к несанкционированному доступу к системе
- **Утечка данных**: Имея доступ администратора, злоумышленники потенциально могут получить доступ к конфиденциальным данным, отфильтровать их или манипулировать ими, что приведёт к утечке данных
- **Компрометация системы**: Злоумышленники могут использовать доступ администратора для дальнейшей компрометации системы, потенциально влияя на целостность, доступность и конфиденциальность системы и данных
- **Нарушение работы**: Несанкционированный доступ может быть использован для нарушения работы, что может иметь значительные последствия для бизнеса, включая простои и финансовые потери
- **Вымогательство и программы-вымогатели**: существует риск вымогательства, когда злоумышленники угрожают опубликовать конфиденциальные данные, если они не получат оплату. Уязвимость также может быть использована в качестве шлюза для атак программ-вымогателей, как это было с предыдущими уязвимостями в продуктах для передачи файлов
- **Ущерб репутации**: Успешная атака может нанести ущерб репутации пострадавшей организации, что приведёт к потере доверия клиентов и потенциальным юридическим последствиям
- **Нарушения требований законодательства**: Организациям могут грозить штрафы и санкции регулирующих органов, если нарушение приведёт к несоблюдению законов о защите данных и отраслевых нормативных актов

VIII. CVE PoC

По GitHub-ссылке https://github.com/horizon3ai/CVE-2024-0204 размещён PoC-эксплойт. Этот скрипт, разработанный Horizon3.ai, демонстрирует, как можно использовать уязвимость обхода аутентификации в GoAnywhere MFT.

Скрипт работает путём отправки POST-запроса в /InitialAccountSetup.xhtml приложения MFT GoAnywhere. Запрос включает параметры для создания нового пользователя с правами администратора, эффективно минуя механизм аутентификации.

A. Параметры скриптов

Параметры включают информацию, необходимую для создания новой учётной записи пользователя:

- **Имя пользователя**: желаемое имя пользователя для новой учётной записи администратора.
- **Пароль**: пароль для новой учётной записи, который должен соответствовать требованиям по сложности GoAnywhere MFT.
- **Адрес электронной почты**: адрес электронной почты, связанный с новой учётной записью администратора.
- **Полное имя**: полное имя физического лица, связанного с новой учётной записью.
- **Разрешения**: Уровень доступа или роли, назначенные новому пользователю, в данном случае права администратора.

Эти параметры отправляются в теле HTTP POST-запроса как часть полезной нагрузки запроса. Сервер обрабатывает эти параметры и создаёт новую учётную запись пользователя с указанными реквизитами.

После запуска скрипта ожидаемым ответом будет указание на то, что сценарий успешно создал нового пользователя с правами администратора в приложении MFT GoAnywhere. Конкретные детали ответа будут зависеть от поведения приложения при создании пользователем:

- **Успешный ответ HTTP**: код состояния, указывающий на успешное выполнение (например, HTTP 200 OK) с веб-сервера, означающий, что запрос POST был успешно обработан.
- **Сообщение с подтверждением**: сообщение или JSON-ответ от приложения, подтверждающий создание нового пользователя с правами администратора.
- **Сообщения об ошибках**: сообщения об ошибках, которые указывали бы на то, что запрос был выполнен неудачно.
- **Административный доступ**: возможность входа в систему с недавно созданными учётными данными администратора, подтверждающими, что пользователь был создан с ожидаемыми разрешениями.

IX. Другие уязвимости связанные с CVE

Другие уязвимости, обнаруженные в GoAnywhere MFT, включают:

- CVE-2021-46830
- CVE-2023-0669

CVE-2021-46830 – это проблема «path traversal», которая потенциально может позволить внешнему пользователю, который самостоятельно регистрируется, получить доступ к непреднамеренным областям памяти приложения. Это влияет на версии GoAnywhere MFT, предшествующие версии 6.8.3.

CVE-2023-0669 – это внедрение команды предварительной аутентификации, которая может быть использована произвольным пользователем. Уязвимость связана с десериализацией ненадёжных данных без надлежащей проверки, что влияет на конфиденциальность и целостность.

A. Схема и сценарий атак [CVE-2021-46830]

Исходя из характера уязвимости CVE-2021-46830 процесс атаки для такой уязвимости включает следующие шаги:

- **Обнаружение**: злоумышленник обнаруживает, что веб-приложение уязвимо для обхода пути из-за неадекватной проверки входных данных.
- **Эксплуатация**: злоумышленник создаёт запрос, который включает последовательности обхода каталогов (например, ../) для перехода из корневого веб-каталога в каталоги, которые должны быть недоступны.
- **Доступ**: созданный запрос позволяет злоумышленнику получить доступ или выполнить файлы, находящиеся за пределами предполагаемых каталогов, доступных через Интернет.
- **Воздействие**: В зависимости от файлов или каталогов, к которым осуществляется доступ, злоумышленник потенциально может прочитать конфиденциальную информацию, выполнить несанкционированные команды или использовать доступ для дальнейшей компрометации системы.

В частности, для CVE-2021-46830 уязвимость позволяла внешнему пользователю, который самостоятельно регистрируется, получать доступ к непреднамеренным областям приложения MFT GoAnywhere, что потенциально могло привести к несанкционированному раскрытию информации или дальнейшим атакам.

Сценарий потенциальной атаки может выглядеть следующим образом:

- **Первоначальный доступ**: злоумышленник идентифицирует приложение MFT GoAnywhere, доступное по сети и позволяющее саморегистрацию пользователей.
- **Использование**: злоумышленник самостоятельно регистрируется, а затем изменяет пути к файлам в приложении для доступа к каталогам и файлам за пределами предполагаемой области действия.
- **Раскрытие информации**: злоумышленник читает файлы, к которым у него не должно быть доступа, потенциально получая доступ к конфиденциальной информации.
- **Дальнейшие атаки:** В зависимости от характера данных, к которым осуществляется доступ, и функциональности приложения злоумышленник потенциально может использовать полученную информацию для проведения дальнейших атак.

B. Схема и сценарий атаки [CVE-2023-0669]

Исходя из характера уязвимости CVE-2021-46830 процесс атаки для такой уязвимости включает следующие шаги:

- **Разведка**: злоумышленник идентифицирует уязвимую целевую систему, которая доступна и имеет конкретную уязвимость, в данном случае CVE-2023-0669.
- **Подготовка атаки**: злоумышленник создаёт вредоносный ввод или полезную нагрузку, предназначенные для использования уязвимости.
- **Доставка**: злоумышленник отправляет обработанную полезную нагрузку в целевую систему. Это может быть связано с сетевыми

запросами, вредоносными файлами или другими способами, в зависимости от характера уязвимости.

- **Эксплуатация**: Полезная нагрузка запускает уязвимость, позволяя злоумышленнику выполнять произвольный код или команды, обходить механизмы безопасности или иным образом компрометировать систему.
- **Пост-эксплуатация**: после успешного использования злоумышленник может выполнять такие действия, как установление постоянного доступа, повышение привилегий, кража данных или распространение на другие системы.

Сценарий потенциальной атаки для уязвимости типа CVE-2023-0669, требующей взаимодействия человека, может включать:

- **Социальная инженерия**: злоумышленник может использовать методы социальной инженерии, чтобы обманом заставить пользователя выполнить определённые действия, которые приведут к срабатыванию уязвимости. Это может быть связано с отправкой вредоносного документа или ссылки пользователю.
- **Вредоносный документ**: Злоумышленник может создать документ, который использует уязвимость при открытии пользователем или взаимодействии с ним. Этот документ может быть замаскирован под легитимный файл, чтобы увеличить шансы пользователя открыть его.
- **Удалённое выполнение кода**: если уязвимость допускает удалённое выполнение кода, злоумышленник потенциально может выполнить произвольный код в системе жертвы после обработки вредоносного документа.
- **Повышение привилегий**: злоумышленник может использовать уязвимость для получения более высоких привилегий в системе, что потенциально может привести к полной её компрометации.
- **Кража или манипулирование данными**: имея возможность выполнять код, злоумышленник может украсть конфиденциальные данные, манипулировать ими или установить в систему дополнительное вредоносное ПО.
- **Закрепление**: злоумышленник может закрепиться в уязвимой системе, обеспечивая постоянный доступ и дальнейшую эксплуатацию.

C. Различия в схеме и сценарии атаки

С точки зрения воздействия, CVE-2024-0204 позволяет злоумышленнику обойти аутентификацию и создать пользователя с правами администратора, в то время как CVE-2021-46830 позволяет злоумышленнику перемещаться по каталогам и получать доступ к файлам или выполнять их вне предполагаемых каталогов, доступных через Интернет.

С точки зрения воздействия, CVE-2024-0204 связан с проблемой обхода пути в веб-приложении, которая позволяет злоумышленнику обойти аутентификацию и создать пользователя с правами администратора, в то время как CVE-2023-0669 связан с уязвимостью, которая может быть вызвана обработкой специально созданного документа.

С точки зрения сценария, CVE-2024-0204 предполагает получение злоумышленником полного административного доступа к системе, в то время как CVE-2021-46830 предполагает получение злоумышленником несанкционированного доступа к определённым областям приложения. Ключевое различие между ними заключается в том, что CVE-2024-0204 допускает прямой административный доступ без необходимости взаимодействия с пользователем, в то время как CVE-2023-0669 требует, чтобы пользователь взаимодействовал с вредоносным документом для запуска уязвимости. CVE-2024-0204 является уязвимостью веб-приложения, тогда как CVE-2023-0669 связан с обработкой документов, вероятно, в контексте рабочего стола или сервера.

D. Воздействие [CVE-2021-46830]

Воздействие CVE-2021-46830 выражается в том, что она позволяет внешнему пользователю, который самостоятельно регистрируется, получать доступ к непреднамеренным областям приложения MFT GoAnywhere, что может привести к несанкционированному раскрытию информации или дальнейшим атакам.

Серьёзность воздействия будет зависеть от конкретных данных и функциональных возможностей, открытых в результате непреднамеренного доступа. Например, если области, к которым осуществляется доступ, содержат конфиденциальные данные, злоумышленник потенциально может украсть эти данные, или в случае если позволяют выполнять определённые команды или функции, злоумышленник потенциально может использовать это для дальнейшей компрометации системы.

E. Воздействие [CVE-2023-0669]

Воздействие CVE-2023-0669 можно охарактеризовать следующим образом:

- **Несанкционированный доступ**: злоумышленник потенциально может получить несанкционированный доступ к системе или данным, в зависимости от характера уязвимости и конфигурации системы.
- **Кража данных**: если уязвимость позволяет получить доступ к данным, злоумышленник потенциально может украсть конфиденциальную информацию.
- **Компрометация системы**: в некоторых случаях злоумышленник потенциально может использовать уязвимость для выполнения произвольного кода или команд, что может привести к полной компрометации системы.

- **Отказ в обслуживании**: если уязвимость вызывает сбой системы или перестаёт отвечать на запросы, это потенциально может привести к отказу в обслуживании.

F. Различия в воздействии

CVE-2024-0204 оказывает более серьёзное воздействие, поскольку позволяет злоумышленнику получить полный административный доступ к системе, в то время как CVE-2021-46830 потенциально может привести к несанкционированному раскрытию информации или дальнейшим атакам.

CVE-2024-0204 оказывает более серьёзное воздействие, поскольку позволяет злоумышленнику получить полный административный доступ к системе, в то время как влияние CVE-2023-0669 будет зависеть от характера уязвимости и конфигурации системы.

G. Последствия [CVE-2021-46830]

Потенциальные последствия атаки, использующей эту уязвимость, могут включать:

- **Несанкционированный доступ**: возможность получить несанкционированный доступ к каталогам и файлам за пределами предполагаемой области действия, что может привести к несанкционированному доступу к конфиденциальной информации или системным ресурсам.
- **Раскрытие информации**: злоумышленник может прочитать файлы, к которым у него не должно быть доступа, что приведёт к раскрытию конфиденциальной информации.
- **Компрометация системы**: В зависимости от характера данных, к которым осуществляется доступ, и функциональности приложения злоумышленник потенциально может использовать полученную информацию для проведения дальнейших атак, что может привести к полной компрометации системы.
- **Манипулирование данными**: если злоумышленник получает доступ на запись к определённым файлам или каталогам, он потенциально может манипулировать данными, что может иметь различные последствия в зависимости от характера данных и функциональности системы.

H. Последствия [CVE-2023-0669]

Потенциальные последствия CVE-2023-0669 могут включать:

- **Несанкционированный доступ**: злоумышленник может получить несанкционированный доступ к системе, что потенциально приведёт к дальнейшей эксплуатации.
- **Кража данных**: злоумышленник может украсть конфиденциальные данные из взломанной системы, которые могут включать личную, финансовую или служебную информацию.
- **Компрометация системы**: злоумышленник может выполнить произвольный код, направленный на компрометацию системы, позволяя ему изменять, удалять или шифровать файлы.
- **Развёртывание вредоносного ПО**: Злоумышленник может использовать уязвимость для развёртывания вредоносного ПО, включая программу-вымогатель или бэкдор, для поддержания постоянного доступа к системе.
- **Отказ в обслуживании**: злоумышленник может нарушить работу служб путём сбоя системы или потребления ресурсов, что приведёт к отказу в обслуживании.
- **Повышение привилегий**: если уязвимость позволяет, злоумышленник может повысить свои привилегии в системе, получив более высокий уровень контроля.

I. Различия последствий

CVE-2024-0204 может привести к полной компрометации системы из-за несанкционированного административного доступа, в то время как CVE-2021-46830 может привести к несанкционированному доступу к определённым областям приложения и потенциальному раскрытию информации.

И CVE-2024-0204 и CVE-2023-0669 могут привести к полной компрометации системы, но CVE-2024-0204 предполагает несанкционированный административный доступ к веб-приложению, в то время как CVE-2023-0669 предполагает удалённое выполнение кода, возможно, из-за ошибки обхода пути.