OPC Classic Возможность подключения данных Уведомление

2022 Обновление безопасности Microsoft Windows DCOM

Влияние и дальнейшие действия

Декабрь 2021

Matrikon: powering interoperability
Matrikon: обеспечение совместимости

Исполнительное резюме

8 июня 2021 года компания Microsoft выпустила обновление безопасности, которое изменило способ обеспечения безопасности DCOM в операционной системе Windows. Это обновление Windows было сделано в ответ на недавно обнаруженную уязвимость, подробно описанную в CVE 2021 26414. В результате этого изменения коммуникации OPC, полагающиеся на DCOM, могут перестать работать, когда изменения Windows начнут применяться в 2022 году.

Microsoft будет развертывать полное обновление безопасности DCOM поэтапно, чтобы дать пользователям Windows время на подготовку до того, как обновление станет обязательным. График и подробности этапов описаны в этом документе.

Пользователям, желающим продолжать использовать свою инфраструктуру OPC Classic в архитектурах, которые полагаются на

DCOM, настоятельно рекомендуется реализовать одно из следующих решений:

- Решение: Устраните зависимость от DCOM, перейдя на такое решение, как Matrikon OPC UA Tunneller (UAT), которое не зависит от этого или будущих обновлений DCOM и не требует изменений в существующих приложениях OPC.
- Устранение последствий: Протестируйте свои системы (инструкции приведены ниже) и сделайте необходимые приготовления для работы с этим раундом обновлений безопасности DCOM. Будущие обновления, скорее всего, потребуют дальнейшего изучения и корректировки.

Обзор обновления безопасности Windows DCOM

Это обновление Windows DCOM Security требует, чтобы приложения OPC Classic поддерживали аутентификацию уровня Packet Integrity, если они используются в архитектурах, которые все еще полагаются на DCOM.

Чтобы приложение OPC Classic поддерживало уровень аутентификации Packet Integrity, эта функциональность должна быть реализована в самом приложении. Потребуется обновление программного обеспечения от производителей, чьи приложения не поддерживают этот уровень аутентификации; поэтому конечные пользователи не смогут обойти эту проблему с помощью изменения настроек безопасности Windows.

Как только обновление безопасности DCOM будет введено в действие:

- Клиенты OPC Classic, которые не поддерживают уровень аутентификации Packet Integrity и полагаются на DCOM, не смогут подключиться к удаленным серверам OPC Classic.
- Локальные связи клиент/сервер OPC Classic не будут затронуты.
- Приложения OPC UA не будут затронуты, поскольку OPC UA не использует DCOM.

Как это обновление влияет на коммуникации OPC Classic

COM и DCOM Справочное руководство

Все приложения OPC Classic основаны на запатентованной технологии Microsoft Component Object Model (COM). Поэтому Windows автоматически задействует функциональность Distributed COM (DCOM), когда приложения на базе COM пытаются взаимодействовать по сети. Несмотря на то, что DCOM в конечном итоге будет постепенно отменен, он продолжает поддерживаться в Windows из-за большой базы пользователей, которые полагаются на него.

Поскольку все клиенты и серверы OPC Classic являются COM-компонентами, на их взаимодействие распространяются ограничения, налагаемые системой безопасности Windows DCOM. Поэтому изменение параметров безопасности Windows с помощью обновлений ОС может негативно повлиять на способность приложений OPC Classic к взаимодействию.

Обсуждаемое здесь обновление безопасности DCOM может повлиять на возможность взаимодействия компонентов OPC, поскольку многие из этих приложений проходят аутентификацию только при первом установлении соединения со своими аналогами, а не на основе каждого пакета.

Влияние на клиентов OPC Classic

Разрешения клиента устанавливаются с помощью функции CoInitializeSecurity. Эта функция может быть вызвана только один раз для каждого экземпляра; последующие вызовы не будут выполнены и вернут ошибку. Если клиент OPC Classic вызывает эту функцию, настройки основываются на параметрах, включенных в вызов. Если клиент не вызывает эту функцию, ОС вызовет ее от имени приложения, основываясь на настройках DCOM по умолчанию. Любой клиент, вызывающий эту функцию, должен внести изменения в свой исходный код, чтобы установить требуемый объект безопасности (Authentication Level) в требуемое значение (Packet Integrity). Клиенты, которые не вызывают CoInitializeSecurity, не будут затронуты, предполагая, что разрешения DCOM по умолчанию установлены должным образом.

Влияние на серверы OPC Classic

Серверные приложения могут также вызывать CoInitializeSecurity. Серверы Matrikon, которые делают это, указывают, что будут использоваться разрешения, установленные в утилите DCOMCNFG. Таким образом, изменение пользовательских разрешений определяет параметры безопасности, которые будут использоваться. Это обновление безопасности не повлияет на серверы в той же степени, что и на клиентов.

Как Matrikon UAT решает проблемы, связанные с DCOM

Matrikon UAT обеспечивает немедленное решение этой проблемы, поскольку компоненты UAT:

- устанавливать локальные соединения с соответствующими сторонними клиентами и серверами OPC Classic

- использовать безопасное соединение между собой на основе TCP/IP. (UAT не затрагивается этим обновлением безопасности DCOM).

Устранив зависимость от DCOM для удаленной связи OPC, Matrikon UAT

- устраняет проблемы, созданные этим обновлением безопасности DCOM,

- защищает архитектуры OPC Classic от будущих обновлений безопасности

Наконец, UAT обеспечивает полную совместимость с программным обеспечением OPC Classic всех производителей. Благодаря активной установке UAT, клиенты Matrikon освобождаются от зависимости от других поставщиков программного обеспечения OPC, которые должны вносить изменения в свое программное обеспечение для соответствия обновлениям безопасности Microsoft DCOM.

График обновления безопасности DCOM

В таблице ниже приведен график поэтапного обновления безопасности Windows DCOM:

Дата	Обновление Фаза развертывания	Действия
Июнь 2021	• Windows DCOM обновления безопасности реализованы, но отключены по умолчанию. • MSFT предоставляет ключ реестра для включения новые возможности.	• Пользователи обновляют Windows последними обновлением системы безопасности. • Используйте ключ реестра, предоставленный MSFT, чтобы включить новые функции безопасности. • Пользователи могут протестировать свои системы, чтобы оценить влияние новых функций безопасности.
Q1 2022	• Новые функции безопасности включены по умолчанию. • Пользователи могут отключить эти функции с помощью ключ реестра.	• В течение этого времени клиенты могут отключить новые функции безопасности, чтобы позволить поставщикам внедрить необходимые изменения программного обеспечения в клиентских приложений OPC Classic.

Q2 2022	Новые функции безопасности DCOM • функции включены по по умолчанию. Эти функции больше не • могут больше нельзя отключить.	• Клиентские приложения OPC Classic, которые не реализуют новые функции безопасности больше не могут создавать удаленные соединения к серверам OPC Classic.

Какие системы затронуты??

Компания Microsoft предоставляет информацию о том, как пользователи могут оценить последствия обновления безопасности DCOM, в следующей статье базы знаний: KB 5004442

Затронутые версии Windows

На момент написания этой статьи обновление безопасности DCOM применяется к следующим версиям Windows:

- Windows Server 2019 (установка ядра сервера)
- Windows Server 2019
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2008 R2 для x64-разрядных систем Пакет обновления 2
- Windows Server 2008 для 32-разрядных систем Пакет обновления 2
- Windows 10 для систем на базе x64
- Windows 10 для 32-разрядных систем
- Windows 8.1 для систем на базе x64
- Windows 8.1 для 32-разрядных систем
- Windows RT 8.1
- Windows 7 для систем на базе x64 Пакет обновления 1
- Windows 7 для 32-разрядных систем Пакет обновления 1

Полный список типов обновлений и сборок Windows, на которые распространяется данное обновление, см. в руководстве Microsoft Update Guide.

Смягчение последствий

Пользователям OPC Classic, которые намерены продолжать использовать DCOM в своих архитектурах OPC Classic, необходимо обратить пристальное внимание на детали и сроки описанных ниже этапов. Неспособность адекватно смягчить изменения в безопасности DCOM может привести к потере связи с данными.

До обновления Q1 2022

В течение этого периода новые обновления безопасности DCOM устанавливаются в Windows, но по умолчанию они отключены. Однако в целях тестирования их можно включить с помощью ключа реестра, предоставленного Microsoft.

Чтобы проверить действие этого обновления безопасности DCOM на непроизводственной системе, пользователи могут:

1. Включите функции безопасности с помощью ключа реестра.
2. Установите для параметра Default Authentication Level в настройках DCOM по умолчанию значение Packet Integrity.
3. Установите уровень аутентификации по умолчанию в настройках Custom DCOM для каждого объекта OPC-сервера на Packet Integrity.
4. Проверьте возможность подключения всех клиентских приложений ко всем серверным приложениям в соответствии с их системной конфигурацией и топологией.

Любое клиентское приложение OPC Classic, которое перестает соединяться с настроенными серверами OPC Classic, скорее всего, само вызывает CoInitializeSecurity и не устанавливает соответствующий уровень аутентификации. Обратитесь к поставщику приложения для получения запланированных обновлений для работы с усиленной средой.

До обновления Q2 2022

Убедитесь, что все соединения OPC функционируют должным образом. Если остались проблемы, используйте ключ реестра для отключения функций безопасности и убедитесь, что оставшиеся проблемы решены, прежде чем изменения безопасности DCOM будут включены навсегда.

После обновления второго квартала

После обновления безопасности, запланированного на 2 квартал 2022 года, у администраторов больше не будет возможности отключать функции безопасности. Единственными вариантами на данный момент будут следующие:

- Получите обновленные версии затронутых приложений от поставщиков программного обеспечения

- Переход к использованию таких решений, как Matrikon UAT, которые исключают использование DCOM
- Переход на другие методы коммуникации, такие как OPC UA

На данный момент не существует никаких обходных путей конфигурации для решения этой проблемы безопасности.

Устранение последствий Matrikon

As На данный момент компания Matrikon активно обновляет свои приложения OPC Classic для обеспечения их корректной работы с примененным обновлением безопасности DCOM.

Клиенты, желающие решить эту и будущие проблемы, связанные с безопасностью DCOM, в своих архитектурах на базе OPC Classic с помощью Matrikon OPC UA Tunneller, могут:

- Загрузите бесплатную пробную версию Matrikon OPC UA Tunneller.

- Для получения информации о лицензировании обратитесь к представителю компании Matrikon.

Отказ от ответственности

Были предприняты все усилия для обеспечения точности информации, представленной в этом документе, о вопросах, связанных с обновлением Microsoft Windows DCOM Security. Подробные сведения об этом обновлении основаны на информации, полученной из различных источников Microsoft. Читатели должны следить за самой актуальной информацией от Microsoft об этом и будущих обновлениях Windows. Читателям также рекомендуется следовать лучшим корпоративным практикам в области ИТ и ОТ.

Вся информация в данном документе предоставлена добросовестно. Однако компания Matrikon не делает никаких заявлений или гарантий любого рода, явных или подразумеваемых, относительно точности, адекватности, действительности, надежности, доступности или полноты информации в этом документе.

Дополнительная информация

Чтобы узнать больше о компании Matrikon,

посетите сайт http://www.MatrikonOPC.com

или свяжитесь с вашим менеджером по работе с клиентами Matrikon.

Контактная информация

sales@matrikonopc.com