Matrikon®
Powering Interoperability.

# OPC Classic Data Connectivity Mitteilung

## 2022 Microsoft Windows DCOM-Sicherheitsupdate

*Auswirkung und Weg nach vorn*

Dezember 2021

## Kurzzusammenfassung

Am 8. Juni 2021 veröffentlichte Microsoft ein Sicherheitsupdate, welches die Art und Weise änderte, wie das Windows-Betriebssystem die DCOM-Sicherheit durchsetzt. Diese Windows-Aktualisierung wurde als Maßnahme gegen eine kürzlich entdeckte Sicherheitslücke durchgeführt, die in CVE 2021 26414 detailliert beschrieben wird. Aufgrund dieser Änderung kann es sein, dass die OPC Kommunikation, die auf DCOM angewiesen ist, nicht mehr funktioniert, wenn die Windows-Änderungen ab 2022 in Kraft treten.

Microsoft wird das vollständige DCOM-Sicherheitsupdate in mehreren Phasen bereitstellen, um Windows-Nutzern die Zeit zu geben sich angemessen vorzubereiten, bevor das Update obligatorisch wird. Der Zeitplan und die Details der einzelnen Phasen werden in diesem Dokument beschrieben.

Nutzer, die ihre OPC Classic-Infrastruktur weiterhin in Architekturen verwenden möchten, die auf DCOM-basierter Kommunikation beruhen, wird dringend empfohlen, eine der folgenden Maßnahmen zu implementieren:

- **Lösung:** Eliminieren Sie die DCOM-Abhängigkeit, indem Sie auf eine Lösung, wie Matrikon OPC UA Tunneller (UAT) umsteigen, die von dieser oder zukünftigen DCOM-Updates nicht betroffen ist und keine Änderungen an bestehenden OPC-Anwendungen erfordert.
- **Anpassung:** Testen Sie ihre Systeme (Anweisungen finden Sie unten) und treffen Sie die notwendigen Vorbereitungen, um diese Runde von DCOM-Sicherheitsupdates zu bewältigen. Zukünftige Aktualisierungen werden voraussichtlich weitere Untersuchungen und Anpassungen erfordern.

## Übersicht des Windows DCOM-Sicherheitsupdates

Dieses Windows DCOM-Sicherheitsupdate erfordert, dass OPC Classic-Anwendungen auch die **Packet Integrity** Level Authentifizierung unterstützen, wenn sie in Architekturen eingesetzt werden, die noch auf DCOM basieren.

Damit eine OPC Classic-Anwendung die Authentifizierungsstufe Packet Integrity unterstützt, muss die Funktionalität in der Anwendung selbst implementiert werden. Die Softwarehersteller, deren Anwendungen diese Authentifizierungsstufe nicht unterstützen, müssen Software-Updates bereitstellen; deshalb können die Endbenutzer dieses Problem nicht durch Änderungen der Windows-Sicherheitseinstellungen umgehen.

Nach der Einführung des DCOM-Sicherheitsupdates:

- OPC Classic Clients, die nicht die Authentifizierungsstufe Packet Integrity verwenden und sich auf DCOM stützen, können keine Verbindung zu Remote OPC Servern herstellen.
- Die lokale OPC Client/Server-Kommunikation ist davon nicht betroffen.
- OPC UA-Anwendungen werden davon nicht betroffen sein, weil OPC UA nicht DCOM verwendet.

# Wie sich dieses Update auf die OPC Classic-Kommunikation auswirkt

## COM und DCOM Hintergrundinformationen

Alle OPC Classic-Anwendungen basieren auf Microsofts proprietärer COM-Technologie (Component Object Model). Als solches aktiviert Windows automatisch die Distributed COM (DCOM)-Funktionalität, wenn COM-basierte Anwendungen versuchen, über ein Netzwerk zu kommunizieren. Während DCOM nach und nach eingestellt wird, wird es auf Windows weiterhin unterstützt werden, da eine große Anzahl von Anwendern darauf angewiesen ist.

Da es sich bei allen OPC Classic Clients und Servern um COM-Komponenten handelt, unterliegt ihre Kommunikation den Beschränkungen, die der Windows DCOM-Sicherheitsrahmen vorgibt. Daher können Änderungen an den Windows-Sicherheitseinstellungen durch Betriebssystem-Updates die Kommunikationsfähigkeit von OPC Classic-Anwendungen beeinträchtigen.

Das hier besprochene DCOM-Sicherheitsupdate kann sich auf die Konnektivität von OPC Komponenten auswirken, da viele dieser Anwendungen sich nur beim ersten Verbindungsaufbau mit ihren Gegenstücken authentifizieren.

## Auswirkung auf OPC Classic Clients

Client-Berechtigungen werden mit dem Funktionsaufruf **CoInitializeSecurity** gesetzt. Diese Funktion kann nur einmal pro Instanz aufgerufen werden; nachfolgende Aufrufe werden nicht ausgeführt und geben einen Fehler zurück. Wenn der OPC Client diese Funktion aufruft, basieren die Einstellungen auf den im Aufruf enthaltenen Parametern. Wenn der Client diese Funktion nicht aufruft, wird das Betriebssystem, basierend auf den Einstellungen in den DCOM-Standardeinstellungen, diese im Namen der Anwendung aufrufen. Jeder Client, der diese Funktion aufruft, benötigt Änderungen an seinem Quellcode, um das erforderliche Sicherheitsobjekt (Authentifizierungsstufe) auf den erforderlichen Wert (Paketintegrität) zu setzen. Clients, die CoInitializeSecurity nicht aufrufen, sind davon nicht betroffen, vorausgesetzt, die Standard-DCOM-Berechtigungen sind entsprechend eingestellt.

## Auswirkungen auf OPC Classic Server

Server-Anwendungen können auch CoInitializeSecurity aufrufen. Matrikon Server, die das tun, legen fest, dass die im **DCOMCNFG** Dienstprogramm festgelegten Berechtigungen zu verwenden sind. Die Änderung der benutzerdefinierten Berechtigungen bestimmt daher die zu verwendenden Sicherheitseinstellungen. Dieses Sicherheitsupdate betrifft Server nicht im gleichen Maße wie Clients

## Wie Matrikon UAT DCOM-bezogene Probleme löst

Matrikon UAT bietet eine sofortige Lösung zu diesem Problem, weil UAT-Komponenten:

- lokale Verbindungen zu den jeweiligen 3rd-Party OPC Clients und Servern herstellen
- eine sichere, TCP/IP-basierte Verbindung untereinander nutzen. (UAT ist von diesem DCOM-Sicherheitsupdate nicht betroffen).

Durch die Entfernung der Abhängigkeit von DCOM für Remote OPC Kommunikation

- beseitigt Matrikon UAT die Probleme, die durch dieses DCOM-Sicherheitsupdate entstehen
- und sichert OPC Classic-Architekturen vor zukünftigen Microsoft-DCOM-Sicherheitsupdates.

Schließlich bietet UAT vollständige Interoperabilität mit der OPC Software aller Hersteller. Durch die proaktive Installation von UAT sind Matrikon Kunden nicht mehr von anderen OPC Softwareanbietern abhängig, die Änderungen an ihrer Software vornehmen müssen, um die Microsoft-Sicherheitsupdates zu unterstützen.

## DCOM-Sicherheitsupdate Ablauf

In der folgenden Tabelle ist der Zeitplan für dieses schrittweise Windows DCOM-Sicherheitsupdate dargestellt:

| Datum | Update-Einführungsphase | Maßnahmen |
|---|---|---|
| Juni 2021 | • Windows DCOM-Sicherheitsupdates sind implementiert, werden aber standardmäßig deaktiviert.<br>• MSFT stellt einen Registrierungsschlüssel zur Verfügung, um neue Funktionen zu aktivieren. | • Benutzer aktualisieren Windows mit dem neuesten Sicherheitsupdate.<br>• Verwenden Sie den von MSFT zur Verfügung gestellten Registrierungsschlüssel, um neue Sicherheitsfunktionen zu aktivieren.<br>• Benutzer können ihre Systeme testen, um die Auswirkungen der neuen Sicherheitsfunktionen zu beurteilen. |
| 14 Juni 2022 | • Die neuen Sicherheitsfunktionen sind standardmäßig aktiviert.<br>• Die Benutzer können diese Funktionen mithilfe des Registrierungsschlüssels deaktivieren. | • Während dieser Zeit können die Kunden neue Sicherheitsfunktionen deaktivieren, um den Anbietern die Möglichkeit zu geben, die erforderlichen Softwareänderungen in den OPC Client-Anwendungen zu implementieren. |
| 14. März 2023 | • Die neuen DCOM-Sicherheitsfunktionen sind standardmäßig aktiviert.<br>• Diese Funktionen können nicht mehr deaktiviert werden. | • OPC Client-Anwendungen, welche die neuen Sicherheitsfunktionen nicht implementieren, können keine Remote-Verbindungen zu OPC Servern mehr herstellen. |

# Welche Systeme sind betroffen?

Microsoft stellt im folgenden Knowledge Base Artikel Informationen darüber bereit, wie Benutzer die Auswirkungen dieses DCOM-Sicherheitsupdates einschätzen können: KB 5004442

## Betroffene Windows-Versionen

Zum Zeitpunkt der Erstellung dieses Dokumentes gilt das DCOM-Sicherheitsupdate für die folgenden Windows-Versionen.

- Windows Server 2019 (Server Core Installation)
- Windows Server 2019
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2008 R2 für x64-basierte Systeme Service Pack 2
- Windows Server 2008 für 32-bit Systeme Service Pack 2
- Windows 10 für x64-basierte Systeme
- Windows 10 für 32-bit Systeme
- Windows 8.1 für x64-basierte Systeme
- Windows 8.1 für 32-bit Systeme
- Windows RT 8.1
- Windows 7 für x64-basierte Systems Service Pack 1
- Windows Server 7 für 32-bit Systeme Service Pack 1

Eine vollständige Liste der Updatetypen und Windows-Builds, die von diesem Update betroffen sind, finden Sie im Microsoft Update Guide.

# Anpassung

OPC Nutzer, die beabsichtigen, DCOM weiterhin in ihren OPC Classic-Architekturen zu verwenden, müssen die Details und den Zeitplan der unten beschriebenen Phasen sorgfältig beachten. Wenn die DCOM-Sicherheitsänderungen nicht angemessen angepasst werden, kann dies zum Verlust der Datenkonnektivität führen.

## Vor dem 14 Juni 2022 Update

Während dieser Zeit werden die neuen DCOM-Sicherheitsupdates in Windows installiert, sind aber standardmäßig deaktiviert. Zu Testzwecken können sie jedoch mit einem von Microsoft bereitgestellten Registrierungsschlüssel aktiviert werden.

Um die Auswirkungen dieses DCOM-Sicherheitsupdates auf einem nicht produktiven System zu testen, können Benutzer Folgendes tun:

1. Aktivieren Sie die Sicherheitsfunktionen mithilfe des Registrierungsschlüssels.
2. Setzen Sie die Standardauthentifizierungsebene in den benutzerdefinierten DCOM-Einstellungen auf **Packet Integrity**.
3. Setzen Sie die Standardauthentifizierungsebene in den benutzerdefinierten DCOM-Einstellungen für jedes OPC Serverobjekt auf Paketintegrität.
4. Überprüfen Sie die Konnektivität von allen Client-Anwendungen zu allen Server-Anwendungen auf der Grundlage ihrer Systemkonfiguration und -topologie.

Jede OPC Client-Anwendung, die sich nicht mehr mit ihren konfigurierten OPC Servern verbinden kann, ruft höchstwahrscheinlich selbst CoInitializeSecurity auf und stellt nicht die angemessene Authentifizierungsstufe ein. Wenden Sie sich an den Anbieter der Anwendung, um sich über geplante Updates für die Anwendungsumgebung zu informieren.

## Vor dem 14. März 2023 Update

Stellen Sie sicher, dass alle OPC Verbindungen erforderlich funktionieren. Wenn es noch Probleme gibt, verwenden Sie den Registrierungsschlüssel, um die Sicherheitsfunktionen zu deaktivieren, und stellen Sie sicher, dass die verbleibenden Probleme behoben sind, bevor die DCOM-Sicherheitsänderungen dauerhaft aktiviert werden.

## Nach dem 14. März 2023 Update

Mit dem für 14. März 2023 geplanten Sicherheitsupdate werden Administratoren nicht mehr die Möglichkeit haben, die Sicherheitsfunktionen zu deaktivieren.  Zu diesem Zeitpunkt gibt es nur noch folgende Möglichkeiten:

- Besorgen Sie sich aktualisierte Versionen der betroffenen Anwendungen der Softwareanbieter
- Verwenden Sie andere Lösungen wie Matrikon UAT, welche den Einsatz von DCOM eliminieren
- Wechseln Sie zu anderen Kommunikationsmethoden wir OPC UA

Zu diesem Zeitpunkt wird es keine Konfigurationsumgebungen geben, um dieses Sicherheitsproblem zu beheben.

## Matrikon Verbesserung

Zum Zeitpunkt der Erstellung dieses Dokuments aktualisiert Matrikon aktiv seine OPC Classic-Anwendungen, um sicherzustellen, dass sie auch nach der Anwendung des DCOM-Sicherheitsupdates korrekt funktionieren.

Kunden, die diese und zukünftige DCOM-Sicherheitsprobleme in ihren OPC Classic-basierten Architekturen durch den Einsatz von OPC UA Tunneller lösen möchten, können Folgendes tun:

- Eine kostenlose Testversion von Matrikon OPC UA Tunneller herunterladen.


- Ihren Ansprechpartner bei der MTK Software GmbH zwecks Informationen zur Lizenzierung kontaktieren.

## Haftungsausschluss

Es wurden alle Bemühungen unternommen, um die Richtigkeit der in diesem Dokument enthaltenen Informationen zu Problemen im Zusammenhang mit dem Microsoft Windows DCOM Security Update zu gewährleisten.  Die Details zu diesem Update beruhen auf Informationen, die aus verschiedenen Microsoft-Quellen recherchiert wurden. Die Leser sollten die aktuellsten Informationen von Microsoft zu diesem und zukünftigen Windows-Updates verfolgen. Die Leser werden auch daran erinnert, ihre unternehmenseigenen IT- und OT-Best-Practices zu befolgen.

Alle Informationen in diesem Dokument werden in gutem Glauben zur Verfügung gestellt. Matrikon gibt jedoch keinerlei ausdrückliche oder implizite Zusicherungen oder Gewährleistungen in Bezug auf die Richtigkeit, Angemessenheit, Gültigkeit, Zuverlässigkeit, Verfügbarkeit oder Vollständigkeit der in diesem Dokument enthaltenen Informationen.

## Weitere Informationen

Um mehr über Matrikon zu erfahren,

besuchen Sie http://www.MatrikonOPC.com

oder kontaktieren Sie Ihren Ansprechpartner bei der MTK Software GmbH.

## Kontaktinformationen

info@mtk-software.de

Tel. +49(0)2238/478630-0