Matrikon®
Powering Interoperability.

OPC Classic Data Connectivity Notice

2022 Microsoft Windows DCOM Security Update

Impact and Path Forward

December 2021

Executive Summary

On June 8, 2021, Microsoft released a security update that changed how the Windows operating system enforces DCOM security. This Windows update was made in response to a recently discovered vulnerability, detailed in CVE 2021 26414. As a result of this change, OPC communications relying on DCOM may stop working when the Windows changes start to be enforced in 2022.

Microsoft will deploy the complete DCOM security update in phases to give Windows users time to make adequate preparations before the update becomes mandatory. The schedule and phase details are described in this paper.

Users wishing to continue to use their OPC Classic infrastructure in architectures that rely on DCOM-based communications are strongly advised to implement one of the following:

- **Solution:** Eliminate DCOM dependency by shifting to a solution like Matrikon OPC UA Tunneller (UAT), which is not affected by this or future DCOM updates and does not require changes to existing OPC applications.
- **Mitigation:** Test their systems (instructions provided below) and make the needed preparations to address this round of DCOM security updates. Future updates will most likely require further investigation and adjustments.

Windows DCOM Security Update Overview

This Windows DCOM Security update requires OPC Classic applications to support the **Packet Integrity** level authentication if they are used in architectures that still rely on DCOM.

For an OPC Classic application to support the Packet Integrity authentication level, the functionality must be implemented in the application itself. Software updates will be needed from software vendors whose applications do not support this authentication level; therefore, end-users will not be able to get around this issue via Windows security setting changes.

Once the DCOM security update is enforced:

- OPC Classic clients that do not support the Packet Integrity authentication level and rely on DCOM will not connect to remote OPC Classic servers.
- Local OPC Classic client/server communications will not be affected.
- OPC UA applications will not be affected because OPC UA does not use DCOM.

How this update affects OPC Classic Communications

COM and DCOM Backgrounder

All OPC Classic applications are based on Microsoft's proprietary Component Object Model (COM) technology. As such, Windows automatically engages Distributed COM (DCOM) functionality when COM-based applications try to communicate across a network. While DCOM will be eventually phased out, it continues to be supported in Windows because of the large install base that relies on it.

Because all OPC Classic clients and servers are COM components, their communications are subject to the constraints imposed by the Windows DCOM security framework. Therefore, changes to Windows security settings via OS updates can adversely affect OPC Classic applications' ability to communicate.

The DCOM security update discussed here may impact the connectivity of OPC components because many of these applications only authenticate upon first establishing connections with their counterparts instead of doing so on a per-packet basis.

Effect on OPC Classic Clients

Client permissions are set using a function called **CoInitializeSecurity**. This function can be called only once per instance; subsequent calls will not be executed and will return an error. If the OPC Classic client calls this function, the settings are based on the parameters included in the call. If the client does not call this function, the OS will call it on the application's behalf based on the Default DCOM settings. Any client calling this function requires changes to its source code to set the required security object (Authentication Level) to the required value (Packet Integrity). Clients that do not call CoInitializeSecurity will not be affected, assuming that the Default DCOM permissions are set appropriately.

Effect on OPC Classic Servers

Server applications may also call CoInitializeSecurity. Matrikon servers that do so specify that the permissions established in the **DCOMCNFG** utility be used. Modifying the Custom permissions therefore determines the security settings to be used. This security update will not affect servers to the same degree as clients.

How Matrikon UAT Resolves DCOM Related Issues

Matrikon UAT provides an immediate resolution to this issue because UAT components:

- make local connections to the respective 3rd party OPC Classic clients and servers
- use a secure, TCP/IP-based connection between each other. (UAT is unaffected by this DCOM security update).

By removing the dependence on the DCOM for remote OPC communications, Matrikon UAT

- eliminates issues created by this DCOM security update,
- futureproofs OPC Classic architectures from future Microsoft DCOM security updates.

Finally, UAT offers complete interoperability with all vendors' OPC Classic software. By proactively installing UAT, Matrikon customers are freed from dependence on other OPC software vendors to implement changes to their software to accommodate Microsoft DCOM security updates.

DCOM Security Update Schedule

The table below outlines the schedule this phased Windows DCOM security update will follow:

Date	Update Rollout Phase	Actions
June 2021	• Windows DCOM security updates are implemented but are disabled by default. • MSFT provides a registry key to enable new features.	• Users update Windows with the latest security update. • Use the MSFT-provided registry key to enable new security features. • Users can test their systems to assess the impact of the new security features.
Q1 2022	• New security features are enabled by default. • Users can disable these features using the registry key.	• During this time, customers can disable new security features to allow vendors to implement required software changes in OPC Classic client applications.
Q2 2022	• New DCOM security features are enabled by default. • These features can no longer be disabled.	• OPC Classic client applications that do not implement the new security features can no longer create remote connections to OPC Classic servers.

What systems are affected?

Microsoft provides information about how users can assess what effects this DCOM security update will have in the following knowledge base article: KB 5004442

Affected Windows versions

As of this writing, the DCOM security update applies the following Windows versions.

- Windows Server 2019 (Server Core installation)
- Windows Server 2019
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2008 R2 for x64-based Systems Service Pack 2
- Windows Server 2008 for 32-bit Systems Service Pack 2
- Windows 10 for x64-based Systems
- Windows 10 for 32-bit Systems
- Windows 8.1 for x64-based systems
- Windows 8.1 for 32-bit systems
- Windows RT 8.1
- Windows 7 for x64-based Systems Service Pack 1
- Windows 7 for 32-bit Systems Service Pack 1

Please refer to the Microsoft Update Guide for a complete list of update types and Windows builds that are affected by this update.

Mitigation

OPC Classic users who intend to continue to rely on DCOM in their OPC Classic architectures will need to pay careful attention to the details and timing of the phases described below. Failure to adequately mitigate the DCOM security changes may lead to data connectivity loss.

Before the Q1 2022 Update

During this period, the new DCOM security updates are installed in Windows but are disabled by default. However, for testing purposes, they can be enabled using a Microsoft-supplied Registry Key.

To test the effect of this DCOM security update on a non-production system, users can:

1. Enable the security features using the Registry Key.
2. Set the Default Authentication Level in the Default DCOM settings to **Packet Integrity**.
3. Set the Default Authentication Level in the Custom DCOM settings for each OPC server object to Packet Integrity.
4. Verify connectivity from all client applications to all server applications based on their system configuration and topology.

Any OPC Classic client application that ceases to connect to its configured OPC Classic servers most likely calls CoInitializeSecurity itself and does not set the appropriate Authentication Level. Contact the application vendor for planned updates to deal with the hardened environment.

Before the Q2 2022 Update

Ensure that all OPC connectivity is functioning as required. If there are remaining issues, use the Registry Key to disable the security features and make sure the remaining issues are resolved before the DCOM security changes are enabled permanently.

After the Q2 Update

With the security update planned for Q2 2022, administrators will no longer have the capability to disable the security features. The only options at this point will be to:

- Get updated versions of the affected applications from the software vendors
- Shift to using solutions like Matrikon UAT, which eliminate DCOM use
- Migrate to other communication methods like OPC UA

At this time, there will be no configuration workarounds to resolve this security issue.

Matrikon Remediation

As of this writing, Matrikon is actively updating its OPC Classic applications to ensure they continue to work correctly with the DCOM security update applied.

Customers wishing to resolve this and future DCOM security related issues in their OPC Classic based architectures by using Matrikon OPC UA Tunneller can:

- Download a free trial version of Matrikon OPC UA Tunneller.

- Contact their Matrikon Sales representative for licensing information.

Disclaimer

Every effort has been made to ensure the accuracy of the information provided in this paper about issues related to the Microsoft Windows DCOM Security update. Details about this update are based on information researched from various Microsoft sources. Readers should follow the most current information available from Microsoft about this and future Windows updates. Readers are also reminded to follow their corporate IT and OT best practices.

All information in this paper is provided in good faith. However, Matrikon makes no representation or warranty of any kind, express or implied, regarding the accuracy, adequacy, validity, reliability, availability, or completeness of the information in this paper.

More Information

To learn more about Matrikon,

visit http://www.MatrikonOPC.com

or contact your Matrikon account manager.

Contact Information

sales@matrikonopc.com