optimize!
softing

IMPACT AND SOLUTIONS

Information About OPC Classic Communication in Connection with Microsoft DCOM Security Patch KB5004442 (CVE-2021-26414)

February 2023

Industrial

Microsoft Update KB 5004442 – DCOM Server Security Feature Bypass (CVE-2021-26414)

On June 8, 2021, Microsoft released a security update (KB 5004442) to address vulnerabilities in the DCOM Remote Protocol The details of these vulnerabilities are described in CVE-2021-26414. The Distributed Component Object Model (DCOM) Remote Protocol exposes application objects using Remote Procedure Calls (RPCs). The protocol is used for communication between software components of networked devices.

Effects on OPC Classic Communication

OPC Classic applications are based on Microsoft's proprietary COM (Component Object Model) technology. Windows automatically activates the Distributed COM (DCOM) functionality when COM-based applications attempt to communicate with each other over a network.

OPC Classic clients and servers are COM components that are subject to Windows DCOM security framework restrictions. Changes to Windows security settings that may be released via operating system updates can affect OPC Classic communication.

The DCOM security update KB 5004442 affects the connectivity of OPC components. With the activation of the new security functions, only DCOM connections (network connections) between the OPC server and clients that support packet-based authentication are possible. This does not affect the communication between OPC Classic servers and clients running on the same computer. Detailed information about the impact of this KB 5004442 DCOM security update, is available on the Microsoft website.

Schedule of DCOM Security Updates

June 8, 2021 - Phase 1

- Microsoft releases security patch KB5004442.
- The changes are disabled by default.
- The new security mechanisms can be activated via Windows registration keys.

June 14, 2022 - Phase 2

- Microsoft releases a Windows update which activates the security mechanisms by default.
- Users can disable the security mechanisms using a Windows registry key.

March 14, 2023 - Phase 3

- The security feature changes are enabled by default.
- Deactivation is no longer possible.
- At this point, users must resolve any compatibility issues with the hardening changes and applications in their environment.

Starting with the effective date of Phase 3 on March 14, 2023, OPC communications based on DCOM may no longer work.

Which Windows Versions are Affected?

The DCOM security update currently applies to the following Windows versions:

- Windows Server 2019
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2008
- Windows 10
- Windows 8.1
- Windows 7

Affected Products from Softing Industrial

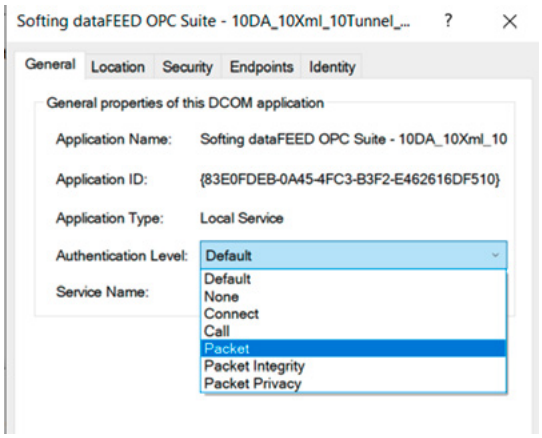
For the OPC products listed below we strongly recommend using an OPC tunnel instead of the DCOM based OPC Classic network communication. Otherwise, we cannot guarantee that the products will work correctly with the Microsoft patch.

- dataFEED OPC Suite Version 5.19 or older.
- Softing S7/S5 OPC Server
- Softing Modbus OPC Server
- Softing Profibus OPC Server
- Multiprotocol OPC Servers (INAT Multiprotocol OPC Server)

Solution in Case of Connection Failure

If your OPC connection fails after applying this mandatory Microsoft patch, please check if the authentication level is set to “Packet Integrity” or “Packet Privacy”.

The following screenshot illustrates where this authentication level is configured in the Windows Component Services dialog box.



NOTE: Softing does not provide support for problems with OPC Classic remote network connections

If the problem is not solved even with the correct authentication level, Softing recommends using the dataFEED OPC tunnel solution.

Softing Industrial Recommendation

Softing is permanently working to improve its OPC Classic applications to ensure to work properly with all current and future DCOM security updates. However, we recommend our customers to use the dataFEED OPC Tunnel solution from Softing instead of a DCOM-based OPC Classic remote connection. The OPC Tunnel solution ensures stable OPC Classic remote communication and is independent of Microsoft patches. Furthermore, installation and operation are much easier than setting up a DCOM-based OPC Classic remote communication.

Detailed information about the dataFEED OPC Tunnel solution and a free trial version can be found at: dataFEED OPC Tunnel

If you have any questions, contact us at: info.automation@softing.com.

optimize!
softing

https://industrial.softing.com