ID: IN39470 | Access Levels: Everyone

Mitigating Microsoft DCOM Hardening Patch (CVE-2021-26414) for Affected Rockwell Automation Products

Document ID	IN39470
Published Date	04/14/2022

Summary

Mitigating Microsoft DCOM Hardening Patch (CVE-2021-26414) for Affected Rockwell Automation Products

Content

Table of Contents

1. What is DCOM?

Distributed Component Object Model (DCOM) is an extension of Component Object Model (COM) that allows COM components to communicate among objects on different computers. DCOM uses Remote Procedure Call (RPC) to generate standard packets that can be shared across a network. This allows COM to communicate beyond the boundaries of the local computer. DCOM is used in a wide variety of software, including Classic OPC DA server and client communications.

2. What is Microsoft changing?

To fix the issue CVE-2021-26414 , Microsoft is releasing patches for multiple Windows operating systems as described in KB5004442-Manage changes for Windows DCOM Server Security Feature Bypass (CVE-2021-26414). A complete list of the Microsoft Windows operating system patches can be found in CVE-2021-26414. Microsoft's patch raises the minimum DCOM authentication level used when establishing DCOM connections between computers. Microsoft is releasing the patch in three phases: June 2021, June 2022, and March 2023.

Microsoft Release Date	Microsoft Rollout Phase
June 2021	Windows DCOM security updates are implemented but are disabled by default
June 14, 2022	Windows DCOM security updates are enabled by default. A registry key can disable enforcement

March14, 2023	Windows DCOM security updates are enabled by default. Microsoft DCOM changes can not be disabled

Once enabled, beginning in June 2022, installing the Microsoft Windoes Cumulative update on the computers within your network may lead to compatibility issues; DCOM communication between the servers and clients not meeting Microsoft's minimum DCOM authentication level will fail. Many Rockwell Automation software products use DCOM for communication. Affected Rockwell Automation products use FactoryTalk® Services Platform, FactoryTalk® Live Data, Classic OPC-DA, or are using Windows® APIs to establish DCOM connections between two computers. Please note products using OPC UA are not affected.

Rockwell Automation products may be **directly** or **indirectly** affected by Microsoft's patch. For example,

- ThinManager® is **directly** affected because it uses DCOM between the ThinManager® server and a remote client administrating the system
- FactoryTalk® Edge Gateway™ is **directly** affected because it offers a Classic OPC-DA ingress point that uses DCOM to establish connection
- Studio 5000 Logix Designer® is **indirectly** affected because it uses FactoryTalk® Services, specifically FactoryTalk® Security, and FactoryTalk® Services uses DCOM between the FactoryTalk® Directory server and FactoryTalk® Directory client
- FactoryTalk® Product Management is **indirectly** affected because it uses FactoryTalk® ProductionCentre®, and FactoryTalk® ProductionCentre® uses FactoryTalk® Services and FactoryTalk® Live Data

A list of **directly** and **indirectly** affected Rockwell Automation products can be found in PN1581 - Product Notification 2022-01-001 - Rockwell Automation products unable to establish proper DCOM connection after installing Microsoft DCOM Hardening patch (MS KB5004442)

Tip:

- To ensure proper communication, the authentication level of both the Rockwell Automation server application and the client application should be at the same level at any time.
- The third-party Classic OPC DA server and client applications are also impacted.

3. Determining if systems are affected

Once the Microsoft DCOM hardening patch is deployed, it has been available since June 2021, the system will generate DCOM errors as various applications attempt to establish DCOM connections between two computers using too low a DCOM authentication level. Following the June 2022 Microsoft Windows cumulative update, DCOM communications between two computers will fail if low DCOM authentication level used is too low. The DCOM errors are captured in the Windows Event log. The error messages use Event ID 10036, 10037 and 10038. The content of the messages is show below:

Event ID	Message
10036	The server-side authentication level policy does not allow the user %1\%2 SID (%3) from address %4 to activate DCOM server. Please raise the activation authentication level at least to RPC_C_AUTHN_LEVEL_PKT_INTEGRITY in client application. (%1 – domain, %2 – user name, %3 – User SID, %4 – Client IP Address)
10037	Application %1 with PID %2 is requesting to activate CLSID %3 on computer %4 with explicitly set authentication level at %5. The lowest activation authentication level required by DCOM is 5 (RPC_C_AUTHN_LEVEL_PKT_INTEGRITY). To raise the activation authentication level, please contact the application vendor. (%1 – Application Path, %2 – Application PID, %3 – CLSID of the COM class the application is requesting to activate, %4 – Computer Name, %5 – Value of Authentication Level)
10038	Application %1 with PID %2 is requesting to activate CLSID %3 on computer %4 with default activation authentication level at %5. The lowest activation authentication level required by DCOM is 5 (RPC_C_AUTHN_LEVEL_PKT_INTEGRITY). To raise the activation authentication level, please contact the application vendor. (%1 – Application Path, %2 – Application PID, %3 – CLSID of the COM class the application is requesting to activate, %4 – Computer Name, %5 – Value of Authentication Level)

4. What's the solution?

Rockwell Automation products released after March 1, 2022, will raise the DCOM authentication level to match Microsoft's revised minimum. These products will not be adversely affected when Microsoft's DCOM hardening patch is applied to computers in a system.

Rockwell Automation will produce patches for **directly** affected products. The patches will raise the DCOM authentication level to match Microsoft's revised minimum. Once patches are applied to Rockwell Automation products they will no longer be adversely affected when Microsoft's DCOM hardening patch is applied to computers in a system. Please refer to the PN1581 - Product Notification 2022-01-001 - Rockwell Automation products unable to establish proper DCOM connection after installing Microsoft DCOM Hardening patch (MS KB5004442) for a listing of product versions that will receive patches.

To avoid the DCOM compatibility issues make sure all Rockwell Automation applications you use are updated or patched.

5. What Rockwell Automation products must be patched to mitigate the effect?

The following table details the dependencies affected Rockwell Automation products. You must patch the directly affected products used by the indirectly affected products to mitigate the effects of Microsoft's DCOM Hardening patch.

Affected Product Name	Affected product requires patching	FactoryTalk Services Platform	FactoryTalk Linx	RSLinx Classic	FactoryTalk Transaction Manager	FactoryTalk ProductionCentre
FactoryTalk Service Platform	X					
FActoryTalk Linx	X	X				
FactoryTalk Linx Gateway	X	X				
FactoryTalk Linx DataBridge	X	X				
FactoryTalk View Site Edition	X	X	X	X		

FactoryTalk View Machine Edition		X	X	X		
FactoryTalk ViewPoint	X	X	X	X		
FactoryTalk Batch	X	X	X	X		
FactoryTalk Edge Gateway	X	X				
FactoryTalk Analytics EdgeML	X	X	X	X		
FactoryTalk VantagePoint	X	X	X			
FactoryTalk Transaction Manager	X	X	X	X		
FactoryTalk ProductionCentre	X	X	X			
Pavilion8	X	X	X			
Emonitor Condition Monitoring	X					
ThinManager	X					
FactoryTalk Policy Manager		X				
FactoryTalk System Services		X				
FactoryTalk Linx CommDTM			X			
ControlFlash		X				
ControlFlash Plus		X				
Studio 5000 Logix Designer		X				
Studio 5000 View Designer		X				
Studio 5000 Logix Emulate		X				
Studio 5000 Architect		X				
Application Code Manager		X				
FactoryTalk Echo		X	X			
FactoryTalk AssetCentre		X				
FactoryTalk Historian Site Edition		X	X			
RSLogix 5		X				
RSLogix 500		X				
RSNetworx		X				
FactoryTalk Metrics		X	X	X	X	
FactoryTalk Production Management		X				X
FactoryTalk Warehouse Management		X				X
FactoryTalk Quality Management		X				X
FactoryTalk EI Hub		X				X
FactoryTalk PharmaSuite		X				X
FactoryTalk CPGSuite		X				X
FactoryTalk AutoSuite		X				X
FactoryTalk Analytics DataView		X	X			
FactoryTalk Analytics DataFlowML		X	X			

FactoryTalk Analytics AugmentedModeler		X	X			
Historian-Thingworx Connector		X	X			
FactoryTalk EnergyMetrix		X		X		
RSLogix 5000		X				

6. Maintaining compatibility in a mixed system

Rockwell Automation products released March 2022, and thereafter, and product patches released to address Microsoft's DCOM hardening patch raise the DCOM authentication level used by Rockwell Automation products to Microsoft revised minimum. **This DCOM authentication level elevation occurs, whether Microsoft's DCOM hardening patch is deployed or not, when installing new software or applying patches**. Elevating the DCOM authentication level affects interoperability between current and patched products, and previously released unpatched products. Use the following guidance to maintain interoperability:

Microsoft Cumulative Update	Recommend action in systems mixing current or patched Rockwell Automation products with previously released unpatched product
Not deployed	Lower the DCOM authentication level used by Rockwell Automation March2022 releases and patched products to maintain interoperability with previously released unpatched product by doing one of the following: • Use Rockwell Automation's *FactoryTalk DCOM Auth Level* utility, as described below • Use the registry editor, as described below • Use domain group policy, as described below

Microsoft Cumulative Update	Recommend action in systems mixing current or patched Rockwell Automation products with previously released unpatched product
Deployed after June 2022, but before March 2023 update	Disable enforcement of Microsoft's DCOM hardening patch using one of the following methods: • Use Rockwell Automation's *Manage Microsoft DCOM Hardening Change* utility, as described below • Use the registry editor to change the Microsoft registry key, as described below • Use domain group policy, as described below **Additionally,** you must lower the DCOM authentication level used by Rockwell Automation March2022 releases and patched products to maintain interoperability with previously released unpatched product by doing one of the following: • Use Rockwell Automation's *FactoryTalk DCOM Auth Level* utility, as described below • Use the registry editor, as described below • Use domain group policy, as described below
Deployed after March 2023	Microsoft no longer permits the DCOM hardening changes to be disabled. The only mitigation available is to upgrade or patch **directly** affected Rockwell Automation products If you lowered the DCOM authentication level used by Rockwell Automation March2022 releases and patched products to maintain interoperability with previously released unpatched product prior to deploying Microsoft's June 2022 update you must **raise** the DCOM authentication level to meet Microsoft's new minimum level, Packet Integrity (5). To raise the authentication level, do one of the following: • Use Rockwell Automation's *FactoryTalk DCOM Auth Level* utility, as described below • Use the registry editor, as described below Use domain group policy, as described below

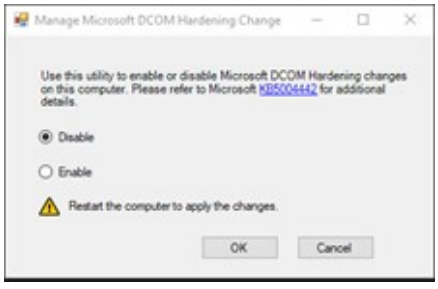
7. Using Rockwell Automation's utility to change Microsoft DCOM hardening enforcement

To use Rockwell Automation's Manage Microsoft DCOM Hardening Change utility to disable Microsoft DCOM hardening enforcement, do the following

- Open **Manage Microsoft DCOM Hardening Change** (MSDCOMHardeningManagement.EXE), select **Disable** to turn off Microsoft's DCOM hardening enforcement. Select **Enable** to turn on Microsoft's DCOM hardening enforcement

Tip: Once the March 2023 Microsoft Windows cumulative update is deployed this mitigation is no longer possible

To download Rockwell Automation's Manage Microsoft DCOM Hardening Change utility please use this link, https://download.rockwellautomation.com/esd/download.aspx?downloadid=MSDCOMHardeningManagement



8. Using Rockwell Automation's utility to adjust the authentication level used by Rockwell Automation products

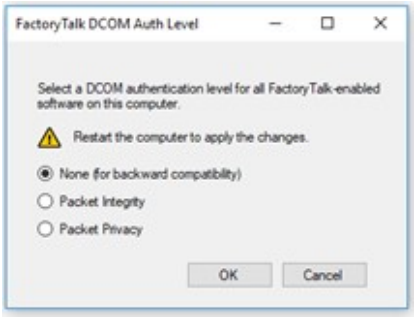
To use Rockwell Automation's FactoryTalk DCOM Auth Level utility to adjust the DCOM authentication level used in Rockwell Automation products released March 2022, and thereafter, or patched versions of product(s) **directly** affected by Microsoft DCOM hardening patch, do the following

- Open **FactoryTalk DCOM Auth Level**, select **None (for backward compatibility)**, and then click *OK*. Select **Packet Integrity**, the new default, to meet Microsoft's new minimum DCOM authentication level rules.

Tip: Using a DCOM authentication level lower than Packet Integrity (5) will not be supported after deploying the March 2023 Microsoft Windows cumulative update.

Tip: Once the March 2023 Microsoft Windows cumulative update is deployed remember to use the utility to raise the DCOM authentication level used by Rockwell Automation products to at least Packet Integrity so that Microsoft's new minimum authentication level is met

To download Rockwell Automation's FactoryTalk DCOM Auth Level utility please use this link, https://download.rockwellautomation.com/esd/download.aspx?downloadid=FactoryTalkDCOMAuthLevel



9. Using the Windows registry editor

To use the Registry Editor to enable or disable enforcement of the Microsoft DCOM hardening patch, do the following:

- Open **Registry Editor**,

  For FactoryTalk-enabled product, such as FactoryTalk Services Platform or FactoryTalk Linx, select **HKEY_LOCAL_MACHINE->SOFTWARE->Microsoft->OLE->AppCompat**, right-click **RequireIntegrityActivationAuthenticationLevel->Modify**, and then edit the **Value data** to 0 to disable and 1 to enable.

To use the Registry Editor to adjust the DCOM authentication level used by Rockwell Automation products, do the following:

On a 64-bit operating system

- Open **Registry Editor**,

  For FactoryTalk-enabled product, such as FactoryTalk Services Platform or FactoryTalk Linx, select **HKEY_LOCAL_MACHINE->SOFTWARE->WOW6432Node-**

>Rockwell Software->FactoryTalk->Platform, right-click **DCOMAuthLevel->Modify**, and then edit the **Value data** to 1. The default value after upgrading the Rockwell Automation application is 5 and the former value is 1.

Tip: Using a DCOM authentication level lower than Packet Integrity (5) will not be supported after deploying the March 2023 Microsoft Windows cumulative update.

For RSLinx Classic, the path is **HKEY_LOCAL_MACHINE->SOFTWARE->WOW6432Node->Rockwell Software->RSLinx**, right-click **DCOMAuthLevel->Modify**, and then edit the **Value data** to 1. The default value after upgrading the Rockwell Automation application is 5 and the former value is 1.

Tip: Using a DCOM authentication level lower than Packet Integrity (5) will not be supported after deploying the March 2023 Microsoft Windows cumulative update.

On a 32-bit operating system

- Open **Registry Editor**,

  For FactoryTalk-enabled product, such as FactoryTalk Services Platform or FactoryTalk Linx, select **HKEY_LOCAL_MACHINE->SOFTWARE->Rockwell Software->FactoryTalk->Platform**, right-click **DCOMAuthLevel->Modify**, and then edit the **Value data** to 1. The default value after upgrading the Rockwell Automation application is 5 and the former value is 1.

Tip: Using a DCOM authentication level lower than Packet Integrity (5) will not be supported after deploying the March 2023 Microsoft Windows cumulative update.

For RSLinx Classic, the path is **HKEY_LOCAL_MACHINE->-SOFTWARE->WOW6432Node->Rockwell Software->RSLinx**, right-click **DCOMAuthLevel->Modify**, and then edit the **Value data** to 1. The default value after upgrading the Rockwell Automation application is 5 and the former value is 1.

Tip: Using a DCOM authentication level lower than Packet Integrity (5) will not be supported after deploying the March 2023 Microsoft Windows cumulative update.

If it is not desirable to run a utility or change registry settings computer by computer, in a domain, domain administrators can use Windows Group Policy to set registry key values on selected computers centrally.

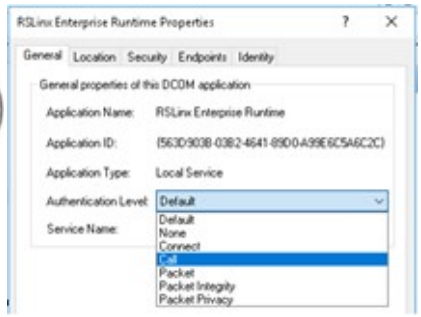
10. Using the Windows Group Policy to set registry values

If it is not desirable to run a utility or change registry settings computer by computer, in a domain, domain administrators can use Windows Group Policy to set registry key values on selected computers centrally.

11. Using Windows DCOM Configuration utility

Microsoft Windows operating systems include a utility for configuring the DCOM properties of software services. One of these properties is the DCOM Authentication Level. Most Rockwell Automation products do not use this property setting; Rockwell Automation products use a fixed DCOM Authentication Level.

Tip: Using DCOMCNFG.EXE to set Rockwell Automation software products DCOM Authentication Level is not a valid mitigation.



Rockwell Automation products that do support adjusting the DCOM Authentication Level using the Windows DCOM Configuration utility (DCOMCNFG.EXE) include: FactoryTalk EnergyMetrix, AADvance OPC Portal, AADvance OPC Standalone, and Trusted OPC Portal. Please review IN39473 - Adjusting a product's DCOM Authentication Level to mitigate Microsoft DCOM Hardening (CVE-2021-26414) using DCOMCNFG.EXE.

12. About Classic OPC DA communication

Classic OPC DA servers and clients use DCOM to communicate; the same compatibility issue may also manifest following deployment of Microsoft's DCPOM hardening patch. Do one of the following to mitigate the issue:

- The Classic OPC DA interface for FactoryTalk Linx Gateway, FactoryTalk Live Data, and RSLinx Classic must be configured to utilize the appropriate DCOM authentication level to work with or without the Microsoft patch (described earlier).
- Set the authentication level of third-party Classic OPC DA server or client to the same level as the Rockwell Automation applications.
- Lower the authentication level on computers that are installed with the patch as mentioned above.
- Deploy the Classic OPC DA server and client on the same computer.
- Change the communication method from Classic OPC DA to OPC UA.

ROCKWELL AUTOMATION DISCLAIMS ALL WARRANTIES WHETHER EXPRESSED OR IMPLIED IN RESPECT OF THE INFORMATION (INCLUDING SOFTWARE) PROVIDED HEREBY, INCLUDING THE IMPLIED WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, AND NON-INFRINGEMENT. Note that certain jurisdictions do not countenance the exclusion of implied warranties; thus, this disclaimer may not apply to you.

www.rockwellautomation.com