ID: PN1581 | Access Levels: Everyone

Product Notification 2022-01-001 - Rockwell Automation products unable to establish proper DCOM connection after installing Microsoft DCOM Hardening patch (CVE-2021-26414)

Document ID	PN1581
Published Date	07/19/2022

Summary

Product Notification 2022-01-001 - Rockwell Automation products unable to establish proper DCOM connection after installing Microsoft DCOM Hardening patch (CVE-2021-26414)

Reference

2022-01-001

Revision History

Revision Number

G

Revision History

Revision G / July 2022 – This notification has been revised to provide clarification that FactoryTalk® EnergyMetrix™ is indirectly affected in the Product Identification section and to remove FactoryTalk® EnergyMetrix™ from the Correction section. Please read this revised notification in its entirety.

Introduction

This Product Notice informs you of a potential anomaly that exists with Rockwell Automation® products that will be unable to establish proper DCOM connection after installing Microsoft® DCOM Hardening patch to address CVE-2021-26414 as described in MS KB5004442 - Manage changes for Windows DCOM Server Security Feature Bypass (CVE-2021-26414). Microsoft is releasing multiple Windows cumulative updates to address CVE-2021-26414. CVE-2021-26414 lists the individual patches. The Microsoft patch addresses a vulnerability in DCOM. The Microsoft patch increases the minimum authentication level used when establishing DCOM connections. The affected Rockwell Automation products use FactoryTalk® Services Platform, FactoryTalk® Live Data, OPC-DA, or are using Windows® APIs to establish DCOM connections between two computers.

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® UI and a remote ThinServer™ service
- 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

Product Identification

The **Active** and **Active Mature** products listed below are **directly** affected by the Microsoft DCOM Hardening patch:

Directly Affected Products

• FactoryTalk® Services • RSLinx® Classic • FactoryTalk® Linx • FactoryTalk® Linx Gateway • FactoryTalk® Linx Data Bridge • FactoryTalk® View Site Edition • FactoryTalk® ViewPoint • FactoryTalk® Batch	• ThinManager® • FactoryTalk® ProductionCentre® • FactoryTalk® Transaction Manager	• FactoryTalk® VantagePoint® • Pavilion8® • Emonitor® Condition Monitoring Software • KEPServer Enterprise • AADvance® OPC Portal • AADvance® OPC Standalone • Trusted® OPC Portal

The **Active** and **Active Mature** products listed below are **indirectly** affected by the Microsoft DCOM Hardening patch:

Indirectly Affected Products		
• FactoryTalk® Policy Manager • FactoryTalk® System Services • FactoryTalk® Linx CommDTM • ControlFLASH™ • ControlFLASH Plus™ • Studio 5000 Logix Designer® • Studio 5000 View Designer® • Studio 5000® Logix Emulate™ • Studio 5000 Architect® • FactoryTalk® Logix Echo • FactoryTalk® AssetCentre • FactoryTalk® Historian SE • Application Code Manager • FactoryTalk® View Machine Edition	• RSNetWorx™ • RSLogix 5000® • RSLogix 500® • RSLogix™ 5 • FactoryTalk® Metrics • FactoryTalk® Production Management • FactoryTalk® Quality Management • FactoryTalk® Warehouse Management • FactoryTalk® EI Hub • FactoryTalk® PharmaSuite® • FactoryTalk® AutoSuite • FactoryTalk® CPGSuite®	• FactoryTalk® Analytics™ EdgeML • FactoryTalk® Analytics™ DataView • FactoryTalk® Analytics™ DataFlowML • FactoryTalk® Analytics™ AugmentedModeler • FactoryTalk® Historian - ThingWorx Connector • FactoryTalk® EnergyMetrix™

The **Active** and **Active Mature** products listed below are unaffected by the Microsoft DCOM Hardening patch:

Unaffected Products

• FactoryTalk® Activation Manager • FactoryTalk® Updater • Studio 5000® Add On Profiles	• PanelView™ Plus 6 / 7 • PlantPAx® MPC • PlantPAx® Process Object Online Configuration Tool	• Connected Components Workbench™ • FactoryTalk® Historian ME

The following products' lifecycle state is **End of Life** or **Discontinued**. No action is planned to address the Microsoft DCOM Hardening patch, regardless of the effect on the product, based on the lifecycle state:

End of Life or Discontinued Products		
• FactoryTalk® Performance Management	• RSView®32 (Active Display)	• GuardPLC™ OPC Server

Description

A potential anomaly exists with Rockwell Automation products that will be unable to establish proper DCOM connection after installing Microsoft DCOM Hardening patch to address CVE-2021-26414 as described in MS KB5004442 - Manage changes for Windows DCOM Server Security Feature Bypass (CVE-2021-26414). Microsoft is releasing multiple Windows cumulative updates to address CVE-2021-26414. CVE-2021-26414 lists the individual patches. The Microsoft patch addresses a vulnerability in DCOM. The Microsoft patch increases the minimum authentication level used when establishing DCOM connections. The affected Rockwell Automation products use FactoryTalk® Services Platform, FactoryTalk® LiveData, OPC-DA, or are using Windows APIs to establish DCOM connections between two computers. 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® UI and a remote ThinServer™ service
- Studio 5000 Logix Designer® is indirectly affected because it uses FactoryTalk® Services, specifically FactoryTalk® Security, and FactoryTalk® Services uses DCOM for communication 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® LiveData

Classic OPC-DA communications utilizes DCOM communications to pass information between workstations. FactoryTalk® Services include an OPC-DA client interface that enables many FactoryTalk-enabled software products to exchange data with third-party OPC-DA servers. Similarly, FactoryTalk® Linx Gateway and RSLinx® Classic function as an OPC-DA server. The DCOM authentication level elevation impacts all OPC-DA communications from these products and any third-party OPC-DA clients and servers running on different workstations (Note OPC-DA communication within one workstation or OPC UA communication are not affected). OPC-DA Clients and Servers must utilize the same DCOM authentication level. Once the FactoryTalk-enabled software DCOM authentication level is changed the DCOM authentication level used by third-party clients and servers on remote workstations must also be updated.

Temporary Workaround

Following application of Microsoft's June 14, 2022, Windows cumulative update, and until Rockwell Automation product patches are available, use the temporary workaround Microsoft describes in MS KB5004442 to disable the Microsoft DCOM Hardening patch.

Important: This mitigation can only be employed until Microsoft releases the final patch update to address CVE-2021-26414 on March 14, 2023. After deploying Microsoft's March 14, 2023, final update it is no longer possible to disable Microsoft's DCOM Hardening patch. After deploying Microsoft's March 14, 2023, update the only mitigation available is to apply Rockwell Automation patches to affected products.

For Classic OPC-DA communications consider moving clients and servers to operate on the same workstation or migrate the system to replace Classic OPC-DA with OPC UA.

Correction

Correcting operation of affected products may require:

- Adjusting the product's DCOM Authentication Level configuration, OR
- Updating affected products either by applying patches or installing a newer unaffected version. Rockwell Automation is working on product patches for affected

products. Rockwell Automation will release the patches on the Rockwell Automation Product Compatibility and Download Center (PCDC) in the future.

The operation of KEPServer Enterprise, AADvance OPC Portal, AADvance OPC Standalone, and Trusted OPC Portal can be corrected by adjusting the DCOM Authentication Level of the application service using the Windows DCOM configuration utility (DCOMCNFG.EXE). Set the **DCOM Authentication Level** to **Default**, **Packet Integrity**, or **Packet Security**. No patch is required.

Following Rockwell Automation's version lifecycle policy patches will be produced for **Preferred** and **Managed** versions of **directly** affected products. **Indirectly** affected products operation can be corrected by applying the FactoryTalk® Services and RSLinx® Classic patches. Systems employing Rockwell Automation product versions released before January 1, 2017 must update to a newer product version to avoid the behavior described in this Product Notice. When available, patches may be downloaded from the PCDC site:

Affected Product	Versions
FactoryTalk® Services	6.21, 6.20, 6.11, 6.10, 3.00, 2.90
FactoryTalk® Linx	6.21, 6.20, 6.11, 6.10, 6.00, 5.90
FactoryTalk® Linx Gateway	6.21, 6.20, 6.11, 6.10, 6.00,3.90
FactoryTalk® Linx Data Bridge	6.21.01, 6.20, 6.11
RSLinx® Classic	4.21, 4.20, 4.12, 4.11, 4.10, 4.00.01
FactoryTalk® View Site Edition	12.00, 11.00, 10.00, 9.00
FactoryTalk® ViewPoint	12.00, 11.00, 10.00, 9.00
FactoryTalk® Batch	15.00, 14.00, 13.00.02
ThinManager®	12.01, 12.00, 11.02, ** 11.01, ** 11.00
FactoryTalk® Transaction Manager	13.10, 13.00, 12.10, 12.00
** Emonitor® Condition Monitoring Software	4.00
** FactoryTalk® ProductionCentre®	10.04, 10.03, 10.02, 10.01
** FactoryTalk® VantagePoint®	8.31, 8.30, 8.20, 8.10, 8.00, 7.00
** Pavilion 8®	5.17.01, 5.17.00, 5.16, 5.15.01, 5.15

Patches for all software products will be included in the Rockwell Automation monthly patch rollup; excepting products preceded with '**' these products do not participate in the Rockwell Automation monthly patch rollup.

For Classic OPC-DA communications consider moving clients and servers to operate on the same workstation.

If you would like to receive a notice when the patches or newer versions are released, a link is provided at the end of the Knowledgebase article for this Product Notice.

Important: Correction requires a customer to install patches or newer versions that will be available from the PCDC site.

Request Customer Action

Rockwell Automation requests you take the following actions:

- Check if you have a product affected by this Product Notice. Refer to the Product Identification and Description sections of this document for product identification assistance.
- Review Rockwell Automation Knowledgebase articles related to Rockwell Automation's response to the DCOM changes Microsoft is making to address CVE-2021-26414. For convenience all Rockwell Automation articles are being collated on a single Table of Content article IN39461 - Microsoft DCOM Hardening Information TOC.
- Review the following guidance related to Microsoft's phased delivery of the DCOM Hardening patch

Microsoft Release Date	Microsoft Rollout Phase	Recommended Action

June 2021	• Windows DCOM security updates are implemented but are disabled by default	• No action necessary • Inventory the Rockwell Automation products and versions in use to understand the future actions may be required

June 14, 2022	• Windows DCOM security updates are enabled by default
	• A Microsoft registry key can disable these Microsoft changes
		Take one or more of the following actions:
		• Disable the Microsoft DCOM security updates as described in Microsoft KB5004442
		• As described in the **Correction** section
		  ◦ Adjust the DCOM Authentication Leve of specific **directly** affected products for which no patch is necessary
		  ◦ Install Rockwell Automation patches for all **directly** affected products; or update all Rockwell Automation **directly** affected products to the most current version released after February 2022
		  ◦ **Indirectly** affected product users must install Rockwell Automation patches for the directly affected product upon which they are dependent, typically FactoryTalk® Services and RSLinx® Classic; or update all Rockwell Automation **indirectly** affected products to the most current version released after February 2022
		• If necessary, move Classic OPC-DA clients and servers to the same workstation

March 14, 2023	• Windows DCOM security updates are enabled by default
	• Microsoft DCOM changes can no longer be disabled
		• As described in the **Correction** section
		  ◦ Adjust the DCOM Authentication Leve of specific **directly** affected products for which no patch is necessary
		  ◦ Install Rockwell Automation patches for all **directly** affected products; or update all Rockwell Automation **directly** affected products to the

		most current version released after February 2022 ○ **Indirectly** affected product users must install Rockwell Automation patches for the directly affected product upon which they are dependent, typically FactoryTalk® Services and RSLinx® Classic; or update all Rockwell Automation **indirectly** affected products to the most current version released after February 2022 • If necessary, move Classic OPC-DA clients and servers to the same workstation

- Customers under support contract are automatically eligible for software updates. Customers not under a support contract should contact Rockwell Automation for further instructions.
- If you need additional assistance, please contact Rockwell Automation Technical Support. See Appendix A [Refer to the attached document for appendices] for local telephone numbers. Customers without TechConnect℠ support contracts should reference this Product Notice when calling.
- Customers with TechConnect support contracts may be able to chat online with support representatives. Reference this Product Notice when connected to a support engineer.

Click here to be notified when the patches or newer versions are released;

Attachments

File	
	PN_2022-01-001_RevG.pdf

ROCKWELL AUTOMATION DOES NOT WARRANT THE COMPLETENESS, TIMELINESS OR ACCURACY OF ANY OF THE DATA CONTAINED IN THIS WEB SITE AND MAY MAKE CHANGES THERETO AT ANY TIME IN ITS SOLE DISCRETION WITHOUT NOTICE. FURTHER, ALL INFORMATION CONVEYED HEREBY IS PROVIDED TO USERS "AS IS." IN NO EVENT SHALL ROCKWELL BE LIABLE FOR ANY DAMAGES OF ANY KIND INCLUDING DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, LOSS PROFIT OR DAMAGE, EVEN IF ROCKWELL AUTOMATION HAVE BEEN ADVISED ON THE POSSIBILITY OF SUCH DAMAGES.

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