ID: IN39472 | Access Levels: Everyone

Minimizing the system impact during Rockwell Automation DCOM patch application

Document ID	IN39472
Published Date	03/22/2022

Feedback

Summary

Minimizing the system impact during Rockwell Automation DCOM patch application

Content

How can I minimize the disruption caused by differences in DCOM authentication levels between patched and unpatched systems and/or applications while applying Rockwell

Automation's monthly **Patch Rollup for CPR9 SRx**?

If the customer has deployed Microsoft's Windows cumulative update June 2022 through February 2023, the following set of steps assume the customer has disabled Microsoft's enforcement of DCOM Hardening at the operating system level using the Microsoft registry key as described in Microsoft KB5004442.

Follow these steps to minimize disruption when an entire system can't be patched simultaneously resulting in a mix of patched and unpatched systems and/or applications on each computer:

1. Disable Microsoft's DCOM Hardening enforcement using the methods described in IN39470 - Mitigating Microsoft DCOM Hardening Patch (CVE-2021-26414) for Affected Rockwell Automation Products. Please review Section 7 to use Rockwell Automation's **Manage Microsoft DCOM Hardening Change** utility, or Section 9 for specific directions to use Microsoft's registry key. Set the registry key to 0.
2. Deploy Rockwell Automation's May 2022, or later, monthly Patch Rollup for CPR9 SRx to the **FactoryTalk Directory Server.**
3. Before rebooting, set the Rockwell Automation registry keys to lower the DCOM Authentication Level used by Rockwell Automation software products using the methods described in IN39470 - Mitigating Microsoft DCOM Hardening Patch (CVE-2021-26414) for Affected Rockwell Automation Products. Please review Section 8 to use Rockwell Automation's **FactoryTalk DCOM Auth Level** utility, or Section 9 for specific directions to use Rockwell Automation's registry keys. Set the registry key to 1.
4. Reboot the computer.
5. Repeat steps 1, 2, and 3 for other servers (Ex. FTAssetCentre, FTView SE Server); ensure each computer is rebooted.
6. Repeat steps 1, 2, and 3 for AssetCentre Agents; ensure each computer is rebooted.
7. Repeat steps 1, 2, and 3 for clients (ex. FTAssetCentre Client, FTView SE Client); ensure each computer is rebooted.

Feedback

Following the steps outlined above, all computers are now running the Rockwell Automation DCOM patches but not using the new minimum DCOM Authentication Level.

When the customer is ready to enforce Microsoft DCOM Hardening, make the following change to the registry on all computers.

All computers must be using the same DCOM Authentication Level, as documented above. To elevate the DCOM Authentication Level in the system follow these steps on each computer:

1. Enable Microsoft's DCOM Hardening enforcement using the methods described in IN39470 - Mitigating Microsoft DCOM Hardening Patch (CVE-2021-26414) for Affected Rockwell Automation Products. Please review Section 7 to use Rockwell Automation's **Manage Microsoft DCOM Hardening Change** utility, or Section 9 for specific directions to use Microsoft's registry key. Set the registry key to 1.
2. Set the Rockwell Automation registry keys to raise the DCOM Authentication Level used by Rockwell Automation software products using the methods described in IN39470 - Mitigating Microsoft DCOM Hardening Patch (CVE-2021-26414) for Affected Rockwell Automation Products. Please review Section 8 to use Rockwell Automation's **FactoryTalk DCOM Auth Level** utility, or Section 9 for specific directions to use Rockwell Automation's registry keys. Set the registry key to 5.
3. Reboot the computer; ensure each computer in the system is rebooted

Once a computer's DCOM Authentication Level is elevated it cannot connect to any computer that is still using the lower DCOM Authentication Level that is attained by following steps 1-7 above.

Upon completion of this second set of steps, all computers are now using the new minimum DCOM Authentication Level required by Microsoft.

Windows Group Policy can be used to set these registry values and coordinate the

Feedback

computer reboot when implementing either set of steps.

Feedback

DISCLAIMER

This knowledge base web site is intended to provide general technical information on a particular subject or subjects and is not an exhaustive treatment of such subjects. Accordingly, the information in this web site is not intended to constitute application, design, software or other professional engineering advice or services. Before making any decision or taking any action, which might affect your equipment, you should consult a qualified professional advisor.

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

Copyright © 2022 Rockwell Automation, Inc. All Rights Reserved.

Feedback