DCOM Policies Hardening by Microsoft® | Impact on 3rd Party DCS Communication

Overview

Microsoft has issued guidance in hardening of the DCOM technology via a new patch which may impact some customers. This advisory is in reference to the information provided via the GE Knowledge Base article published via the Customer Dashboard, and is accessible at the following link with a GE customer login: KB0030779.

Background

Distributed Component Object Model (popularly known as DCOM) is a Microsoft proprietary technology for communication between software components on networked computers.

DCOM extends Microsoft's COM and provides the communication substrate under Microsoft's COM+ application server infrastructure. This protocol is supported natively in all versions of Windows starting from Windows 95, and all versions of Windows Server since Windows NT. The DCOM Remote Protocol communication (RPC) is useful and appropriate when a distributed object-based architecture is required exchanging data across the network.

To allow the DCOM communication, it is required to perform certain configuration changes to the HMI computer (as outlined in GEI 100621) that might pose some security challenges and may not be the right solution when traversing across network segments for the following reasons:

- Does not provide a secure means of transport and authentication to segmented networks
- Requires multiple firewall ports to be opened which reduces security posture
- Not considered appropriate for "high speed" real-time communication
- Does not operate well on unreliable networks which could be the case for third party networks
- Generates additional data overhead during the transmission which slows the communication

To mitigate the security challenges, GE standardized using Tunneling software as a solution for 3rd party DCS communication for exchange of data. This Tunneller software simplifies DCOM configuration and has a client / server component that exchanges data between servers providing necessary data for DCS system. In addition, this helps secure this communication and avoids the data overhead during the transmission.

What is changing now:

To address the security concerns with DCOM configurations mentioned above, Microsoft will be hardening DCOM policies that would impact existing applications relying on DCOM / RPC for communication. When the latest Microsoft patch, KB5004442 is applied, this will harden the security policies on the HMI and impact the communication between GE OPC Server and 3rd Party DCS system that use DCOM configuration.

However, this impacts the system that were connected online or using any HMI patching program such as PPVP from GE to regularly update the Windows Operating system with latest patches released by Microsoft from time to time.

How to Identify if site communicates with 3rd Party DCS using DCOM settings:

If the site has the DCS system and is exchanging data over the OPC DA protocol, and if the Gateway Servers interfacing with DCS Systems were not loaded with any tunneling software (ex: Tunneller software on Gateway HMIs like ONB from Integration Objects, TMW gateway from Triangle Microworks etc.), the system will be utilizing standard Microsoft DCOM settings for exchange of this OPC DA data.

Alternatively, this can also be verified by checking if DCOM settings were enabled on the GE Gateway servers by reviewing the **Configuring DCOM** Section of **GEH-6808** and checking if the mentioned settings were applied to the Gateway Servers at site to allow DCOM communication.

Remediation

As highlighted in the Background section, using Tunneling software is a standard offering from GE and there is no impact when the DCS communication is established using this software. Also, in cases where the site does not use DCS communication, no action is required.

However, if site does have DCS communication and has implemented DCOM communication by way of configuring the DCOM settings, and site HMIs are updated regularly with Microsoft Windows monthly patches, the site may need to review the below possible alternatives:

- Using Tunneller Software that avoids need for DCOM configurations on the Gateway Servers and applications continue to work with no impact. This method avoids any changes to application code, however requires additional software procurement and configuration.

- Alternatively, sites can implement this communication using OPC UA instead of OPC DA. OPC UA is an enhanced communication protocol that has built in security features with mutual certificate exchange for trusting the client and server that does not require DCOM configuration. This solution requires changes to application code to enable communication from OPC DA to OPC UA protocol.

Both these alternatives require study of current systems to understand the impact and deploy the modification required; thus, these should be routed through CM&U request.

GE Power Product Security Incident Response Team (PSIRT)

Providing secure and reliable products and solutions is vital to the operations of GE Gas Power. Our products are engineered with security as a key principle. We have implemented and will maintain reasonable and appropriate technical and organizational measures, internal controls, and information security routines intended to help protect our products and customers.

Contact Information

Contact your local GE Services representative for assistance or for additional information or submit an ER case for assistance in making configuration changes to your environment.
For Product Security issues or incident/vulnerability reporting: www.ge.com/power/cybersecurity

Document History

Version	Release Date	Purpose
1.0	March 28th, 2023	Initial release