Windows DCOM Hardening

There is much confusion concerning Microsoft DCOM hardening. It's intention isn't to shut down the use of DCOM but instead insure OPC client to OPC server connections are legitimate. This is accomplished by not allowing DCOM authentication levels below packet security. Note that Microsoft Windows DCOM software handles the details of authentication. It's not any code implemented within a given OPC DA server or OPC client. DCOM hardening doesn't affect most OPC DA servers including RoviSys OPC90 DA OPC server. The reason is these OPC servers don't dictate what authentication level they require but instead work with whatever is setup within DCOM. Specially, the settings are default authentication level is "Packet Integrity" and default impersonation level is "Impersonate" or "Delegate".

This is not the case for most OPC DA client products. OPC DA client software sets up a connection with an OPC DA server with a single call to Windows. That call identifies the OPC server it wishes to connect with and what authentication level it wants to use. Most OPC DA client software has hardcoded the authentication level it requests to be something less than packet security. This causes OPC DA client software to not be able to connect with an OPC DA server after the Microsoft DCOM hardening patch is enforced.

OPC client vendors that have hardcoded the authentication level below packet security will have to issue a patched version that hard codes packet security or allows the user to specify an authentication level it should use for the connection. The RoviSys BridgeMaster product is a two side OPC DA client. By default, the latest version of this product utilizes packet security authentication, but the user can specify another level too.

For those who want to dig in deeper, this article provides even more details:

https://techcommunity.microsoft.com/t5/windows-it-pro-blog/dcom-authentication-hardening-what-you-need-to-know/ba-p/3657154