KB2022-01 Cyberlogic Response to Microsoft DCOM Hardening

To address security vulnerability CVE-2021-26414, Microsoft is hardening the Distributed Component Model (DCOM) on its Windows operating systems.

The Cyberlogic OPC Server uses DCOM as its primary communication method that allows remote (over the network) OPC clients to communicate to it. Also, when exchanging data with other OPC servers, the Cyberlogic OPC Server uses the Cyberlogic OPC DA Driver Agent, which may communicate across the network over DCOM. As a result, the hardening changes may negatively impact some installations of the Cyberlogic software.

This article describes the possible problems that a user may experience following these changes and explains how to prevent disruptions and maintain full functionality of the affected Cyberlogic software.

Applies To:

Any remote OPC Client software that connects to the Cyberlogic OPC Server over DCOM. Also, any Cyberlogic OPC Server installation that uses the Cyberlogic OPC DA Driver Agent and connects to another remote OPC server over DCOM. All Cyberlogic OPC Server software suites are affected.

Overview:

To address security vulnerability (CVE-2021-26414), Microsoft implemented hardening changes in DCOM that enforce an authentication level of Packet Integrity or higher for activation. These changes are distributed by the Microsoft software updates.

In the initial update, dated June 8, 2021, the hardening changes were disabled by default but with the ability to enable them using a registry key. In the following update, scheduled for June 14, 2022, the hardening changes will be enabled by default but with the ability to disable them using a registry key. In the final update, scheduled for March 14, 2023, the hardening changes will be enabled with no ability to disable them. By this point, you must resolve any compatibility issues resulting from the hardening changes in your environment.

Prior to the hardening changes, the minimum DCOM authentication level was Connect, which authenticated the client software only during the initial connection to the server and provided no guaranty that the exchanged data had not been modified in transit. This was the most commonly used authentication level and was used by the Cyberlogic OPC Server and the Cyberlogic OPC Client when their security settings were set to Medium.

The new minimum DCOM authentication level is Packet Integrity, and it requires authentication each time a call to the OPC server is made. Also, the entire content of every packet is digitally signed. This ensures that none of the data transferred between a client

and a server has been modified. For maximum protection, the DCOM authentication level can also be set to Packet Privacy, so that all data packets are signed and encrypted.

For more information about Microsoft's DCOM hardening, see this Microsoft support article.

Issues:

The hardening changes described above will require changes to the DCOM security settings in all OPC client software that exchange data across the network with the Cyberlogic OPC Server if their current authentication level is set to less than the Packet Integrity.

Cyberlogic OPC Server:

The Cyberlogic OPC Server is the main component included with all Cyberlogic OPC Server software suites.

Prior to version 9.0 Patch 6, the OPC Server allowed three DCOM security settings: Low, Medium, and Custom. In the Low setting, any authentication level was allowed. In the Medium setting, the minimum authentication level was set to Connect, which is now below the minimum DCOM requirements. In the Custom setting, the server relied on its DCOM settings that were set by the DCOMCONFIG utility, so the authentication level could potentially be set to a level that is below Packet Integrity.

Although the minimum authentication level required by the server could be set to below Packet Integrity, the server will not be impacted by the hardening changes, unless the server is also configured to use the Cyberlogic OPC DA Driver Agent (see below). DCOM will automatically enforce an authentication level of Packet Integrity or higher from all OPC clients. Therefore, configuration for the OPC clients may be affected by the changes.

Cyberlogic OPC DA Driver Agent:

The Cyberlogic OPC DA Driver Agent is a plug-in module that allows the Cyberlogic OPC Server to communicate to other OPC DA servers. It is included with the following Cyberlogic OPC software suites:

- MBX OPC Enterprise Suite
- DHX OPC Enterprise Suite
- OPC Crosslink, OPC Crosslink Premier and OPC Crosslink Enterprise Suites
- OPC Datacenter and OPC Datacenter Premier Suites

For DCOM connections, the OPC DA Driver Agent sets its DCOM authentication level based on the security settings of the host Cyberlogic OPC Server.

Prior to version 9.0 Patch 6, the authentication level used by the driver agent was always set to Connect in both the Low and Medium security setting. In the Custom setting, the authentication level was either equal to the authentication level of the server or was set to Connect if the server's authentication level was below Connect. After the hardening changes take effect, the authentication level used in the Low, Medium and potentially some Custom settings will be below the minimum DCOM requirements.

Cyberlogic OPC Test Client:

The Cyberlogic OPC Client is a test client included with all Cyberlogic OPC Server software suites.

Prior to version 9.0 Patch 6, the OPC Client allowed three security settings: Low, Medium, and Custom. The Low setting could only be used for the local OPC server connections. In the Medium setting, the authentication level was set to Connect. In the Custom setting, the OPC Client relied on the default DCOM settings for all applications on the system. Since various applications could have different requirements, it was often unreliable and, therefore, avoided. After the hardening changes take effect, the authentication level used in the Low, Medium and some Custom settings will be below the minimum DCOM requirements.

Other OPC Clients:

Most OPC DA clients provide some mechanism for adjusting the DCOM security settings to match the requirements of the target OPC server. Refer to the software documentation or contact the manufacturer's technical support for more information on how to change the settings to be compatible with the Microsoft DCOM hardening changes.

Resolution for Version 9.0:

Due to the possible negative effect of the Microsoft DCOM hardening changes on some installations of the Cyberlogic OPC Server suites, Cyberlogic has issued a free software patch to alleviate the negative impact. To avoid possible disruptions, apply Patch 6 (or higher) prior to June 14, 2022. Patch 6 can be downloaded from the Download page of the Cyberlogic website or directly from this link.

The following sections describe the software changes included in Patch 6:

Cyberlogic OPC Server:

The authentication level in the Medium DCOM security settings will be set to Packet Integrity (rather than Connect). The upcoming DCOM hardening should not require any configuration changes. However, the DCOM security settings for all remote OPC clients connecting to the server should be reviewed to ensure that their authentication level is set to at least Packet Integrity.

Cyberlogic OPC DA Driver Agent:

For DCOM connections, the OPC DA Driver Agent sets its DCOM authentication level based on the security settings of the host Cyberlogic OPC Server.

The authentication level used by the driver agent will now be set to Packet Integrity in the Low and Medium security setting. In Custom setting, the authentication level will be either equal to the authentication level of the server or will be set to Packet Integrity if the server's

authentication level is below Packet Integrity. The upcoming DCOM hardening should not require any configuration changes.

Cyberlogic OPC Test Client:

The OPC Client now allows three security settings: Low, Medium, and High (rather than Custom). The Low setting has not changed and should only be used for the local OPC server connections. In the Medium setting, the authentication level is now set to Packet Integrity, and in the (new) High setting, it is set to Packet Privacy. Both Medium and High security settings fully comply with the upcoming DCOM hardening changes.

Resolution for Versions prior to 9.0:

If you are using any Cyberlogic OPC Server product whose version is lower than 9.0, you will have to upgrade to version 9.0. To avoid possible disruptions, upgrade your software prior to June 14, 2022.

Technical Support:

If you have any questions or need addition help, please contact Cyberlogic's Technical Support group by emailing techsupport@cyberlogic.com, or by calling 248-631-2288.

Cyberlogic's website, www.cyberlogic.com, has information on related products, news, software downloads and contact information.

Cyberlogic Technologies
755 W Big Beaver Rd
Suite 2020
Troy, Michigan 48084 USA

Sales:	248-631-2200 sales@cyberlogic.com
Technical Support:	248-631-2288 techsupport@cyberlogic.com