HPS Technical Support

Knowledge Sharing Mail	Ref: KSM2022-001

Version: 005	Last Updated: Feb 18, 2022	Applicable Systems: Experion OPC Classic Clients	Releases: R5xx	Author: HPS Technical Support

Experion OPC Classic Clients & Microsoft Windows DCOM Security Update 2022 Changes

*** Microsoft postponed the DCOM Hardening dates – updated table ****

On June 8, 2021, Microsoft released a security update that changed how the Windows operating system enforces DCOM security. This Windows update was made in response to a recently discovered vulnerability, detailed in CVE 2021 26414. As a result of this change, OPC communications relying on DCOM may stop working when the Windows changes start to be enforced in 2022.

Microsoft will deploy the complete DCOM security update in phases to give Windows users time to make adequate preparations before the update becomes mandatory.

The table below outlines the schedule this phased Windows DCOM security update will follow

Date	Update Rollout Phase	Actions
June 2021	• Windows DCOM security updates are implemented but are disabled by default. • MSFT provides a registry key to enable new features.	• Users update Windows with the latest security update. • Use the MSFT-provided registry key to enable new security features. • Users can test their systems to assess the impact of the new security features.
June 2022	• New security features are enabled by default. • Users can disable these features using the registry key.	• During this time, customers can disable new security features to allow vendors to implement required software changes in OPC Classic client applications.
March 2023	• New DCOM security features are enabled by default. • These features can no longer be disabled.	• OPC Classic client applications that do not implement the new security features can no longer create remote connections to OPC Classic servers.

Experion Release Impacted by the Microsoft DCOM Hardening

DCOM Hardening is being deployed to multiple Windows versions, as a consequence Experion R5xx & R43x with ESU OPC Classic DA, AE, HDA connections are impacted by the Microsoft DCOM hardening (Experion Servers, EAS, EAPP, ACE OPCG).

Experion OPC Classic Clients - Updates:

Experion OPC Classic Clients (OPC Scada Channel, OPC Advanced, OPC Display, OPC Integrator, OPC Gateway) will be updated to accommodate the DCOM change on the following Experion supported releases.

Experion Updates details:

- R500.2 SP9 HF – May 2022

- R501.6 SP6 HF – May 2022

- R510.2 SP7HP6 HF – May 2022

- R511.3 SP9HP8 HF - May 2022

- R511.4 SP4HP3 – May 2022

- R511.5 SHU2 HF – May 2022

- R520 SHU2 HF – May 2022

- R520 FU3 HF – May 2022

Impact for 3rd Party OPC Classic Clients

3rd Party OPC Classic Clients (OPC DA, AE, HDA) would likely require an update to accommodate the upcoming Windows DCOM hardening, it is up to the customer to contact the 3rd party vendor and assess the impact for their configurations.

DVM Impact

Investigations are currently under way. We believe that communications to Database Servers Camera Servers and EBI and Experion servers might be impacted by the Microsoft DCOM change.

This may affect status reporting, client operations and Multi-monitor displays. DVM may require updates to accommodate the DCOM change on the following supported DVM releases (May 2022):

- R620.1 SP1

- R700.1 SP1

- R710.1

Older DVM releases that are no longer supported will not receive any software updates. (e.g. DVM R600, DVM R500)

EBI Impact

Investigations are currently under way. We believe that OPC DA, AE, HDA connections might be impacted by the Microsoft DCOM change. EBI OPC Clients (OPC Scan Task and OPC Data Transfer) may require updates to accommodate the DCOM change on the following supported EBI releases (May 2022):

- R500.1 CU5

- R600.1 CU3

- R610.1

Older EBI releases that are no longer supported will not receive any software updates. (e.g. EBI R430, EBI R410)

Experion OPC UA

OPC UA is not impacted by the upcoming DCOM changes, therefore, transitioning to OPC UA might be a future proof alternative.

- Experion OPC UA Clients is available from Experion R510.2

- Experion OPC UA Server is available from Experion R511.3

OPC UA Data Access support in R511x and R520x:

- Read
- Write
- Subscription
- Browse

OPC UA Historical Access support in R520x:

- Data only
- Raw history values read
- History aggregates : Average, Interpolative, Maximum and Minimum

GTAC guide and video for configuring an OPC UA connection can be found here.

Registry change to temporally disable DCOM hardening:

During the timeline phases in which you can enable or disable the hardening changes for CVE-2021-26414, you can use the following registry key to temporally disable the DCOM hardening:

- Path : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole\AppCompat
- Value Name: "RequireIntegrityActivationAuthenticationLevel"
- Type: dword
- Value Data: default = 0x00000000 means disabled.

   Note You must enter Value Data in hexadecimal format. **Important** You must restart your device after setting this registry key for it to take effect.

It is recommended to implement the registry change on Experion OPC Servers nodes, and 3rd party OPC Client nodes

Experion System Impact assessment:

What are these new Windows log DCOM message after installing recent Security Updates?

Microsoft has introduced new logging that enables you to determine if an OPC client requires an application/code update. Refer to the article CVE-2021-26414 for details on the new logging.

How do I know if my OPC Client application is compatible with DCOM Hardening changes?

Only the vendor developing the OPC client application would be able to answer this question. The DCOM Hardening change would require a code change on the OPC Client application.

You might also inspect the Experion OPC Server node for the new Windows events that would enable to identify which application would require update.

Would it work if the OPC Clients runs an old/unpatched OS?

In a scenario where the OPC client runs on an older or unpatched OS, the OPC connection would fail as it would be blocked by the OS DCOM hardening on the OPC Server side.

Questions and Answers

Where can I learn more details on the upcoming Windows changes and impact?

There are various articles online, for example here.

Is it enough to update the Experion nodes?

Experion updates would only cover the scenario where Experion Server is the OPC Classic Client (OPC Scada Channel, OPCI, OPC Adv, etc.). For configurations where an OPC Client application is acquiring from Experion (Server, EAPP), the Experion update would not help, an update of the OPC Client application would be required.

Would updating RDM be "necessary" to mitigate the problem?

RDM is also impacted, it would require an update. The updates would be delivered for the list of Experion release above.

What will be the impact for other Honeywell products using OPC?

Honeywell Products using OPC Classic client technology would require an update, the respective technology groups are assessing the impact and similar notification would be released by the respective support team.

What configuration change can I apply to my system to mitigate the issue?

There is no DCOM configuration change that would mitigate the problem, the OPC Client application needs to be updated to use an increased level of authentication at connection time. The change requires a code change in the application

Is the DCOM Change already deployed by Microsoft in their monthly security updates?

Yes, the Microsoft changes have been introduced in the MS Security June 2021 and later, but not activated.

Can I deploy security updates on my system?

Yes, it is safe to install security update, DCOM Changes are not enforced, extra logging is expected, refer to this article for details.

My OPC Client node is on a different Windows domain than Experion will it continue to work?

We are investigating with Microsoft if this configuration would continue to work, noting that OPC UA might be a better option for cross domain configuration.

Will Honeywell qualify 3rd OPC Client for Experion use?

There is no plan to qualify 3rd party OPC Client application, it is up to the customer to confirm with its vendor that their OPC Classic client is compliant with the Windows DCOM changes.

Where can I find the configuration best practices for OPC Classic Client application:

The GTAC configuration guidelines for OPC Classic clients can be found on this article.

Where can I find update of this article?

This article will be updated once we get more details from Microsoft, the article can be found online on this link.

If you have any questions concerning this Knowledge Sharing Mail,
then please contact HPS Technical Support