Doc Type	Tech Alerts
Doc Id	TA000032813
Legacy Doc Id	
Publish Date	1/14/2023

System Platform issues with Microsoft Update KB5004442 - DCOM Hardening

Affected versions

- **System Platform 2020 R2 SP1 and earlier System Platform 2020 R2 releases.**
- **System Platform 2020 P01 and all earlier System Platform 2020 releases.**
- **System Platform 2017 U3 SP1 P01 and earlier System Platform 2017 releases.**
- **System Platform 2014 R2 SP1 P02 and all earlier releases of System Platform.**
- **OI Gateway and FS Gateway**
- **AVEVA Enterprise Data Management OPC Real-Time Service (eDNA RTS)**
- **AVEVA Enterprise Data Management OPC Data Server DA/HDA (eDNA DA/HDA)**
- **AVEVA Edge 2020 R2 SP1 and earlier**
- **InduSoft Web Studio 2020 R2 and earlier**

Situation

In June 2021, Microsoft delivered a security update that included the ability to add a registry key that enables the hardening of DCOM as provided in KB5004442. The key supports setting the key value to 1 (enable). Please review the Microsoft article on KB5004442 for details and important timeline. AVEVA continues to monitor Microsoft's activities with their DCOM hardening plan. The monitoring activities include evaluating the potential impact on AVEVA's software portfolio.

NOTE: AVEVA is currently confirming details and test results of Microsoft's Nov 8th update related to KB5004442 and will update this *Tech Alert* further once the research is complete.

Known Issues

NOTE: The following behavior is observed with the registry setting enabled. No issues are observed when the setting is disabled.

- **OI Gateway** and **FS Gateway**
  - Unable to browse remote OPC server and data.
  - Local browsing to OPC data will work fine.
- **System Platform - Application Server IDE**
  - During design-time, OPC Client objects are unable to browse for OPC Servers.
  - During design-time, OPC Client objects are unable to browse for tags.
  - Browsing for local OPC servers and tags on local OPC Servers using the OPC Client Object will function properly.
  - The runtime behavior of OPC Client objects are unaffected regardless of whether the server is local or remote
  - Remote deployment *may* fail (when GR Node has monthly Microsoft Updates prior to June 2022 and the Runtime Node has monthly updates on or after June 2022).
- **AVEVA Edge and Indusoft Web Studio**
  - **Studio OPC DA Server, Studio OPC HDA Server, OPC DA 2.05 (legacy), OPC XML/DA Clients**
    - Unable to browse remote OPC server and data.
    - Unable to read/write OPC items data on the remote OPC server.
    - Local browsing and reading/writing OPC data will work fine.
- **Historian Server** remote administration from within the SMC does not work.
  - The work around is to RDP to the machine on which **Historian Server** is installed and administer it locally.
- **AVEVA Enterprise Data Management OPC Real-Time Service (eDNA RTS)** fails to connect to a remote OPC DA server.
- OPC clients fail to connect to **AVEVA Enterprise Data Management OPC Data Server DA/HDA (eDNA DA/HDA)**

Workaround

1. Install Cumulative Updates/Monthly Rollup Updates from September 2021 or later on all computers (KB5004442 is included).
2. Disable the DCOM hardening registry key. **A reboot is required** to apply the registry update. Link to Microsoft Article

Solution

1. The **OI Gateway** and **Application Server's $OPCClient** issues are fixed in the **System Platform 2023** release.
2. The **OI Gateway** issues are resolved in the **Communication Drivers Pack 2023** release.
3. Product updates / hot fixes for **OI Gateway** supported product versions, **6.0 through 2020 R3**, are now available. Please contact Customer Support for more information or to obtain a hot fix.
4. Customers using **FS Gateway** must migrate to an **OI Gateway** version where a hotfix to address this issue is available, or to **OI Gateway 2023** via **Communication Drivers Pack 2023.**
5. The issues observed with the OPC Client Object are minor and only impact design-time. Therefore, product updates and/or hot fixes to address the issues will only be made available to the latest update levels of System Platform versions still under mainstream support (see Product Life Cycle for details) as follows:

    - **System Platform 2023** and newer – The issues are resolved in all new versions starting with **System Platform 2023**.
    - **System Platform 2020 R2 SP1 P01** – The issues are resolved in Patch 01
    - **System Platform 2020 R2 SP1** – As shown above, the issues are resolved in Patch 01 and applying the patch is recommended. However, a separate hotfix is available for customers who are unable to install the patch.
    - **System Platform 2020 R2 P01** – A hotfix is available.
    - **System Platform 2020 R2** – A hotfix is available, but Patch 01 must be applied first.
    - **System Platform 2020 P01** – A hotfix is available.
    - **System Platform 2020** – A separate hotfix is available, but Patch 01 must be applied first.
    - For earlier **System Platform** versions not listed, contact Customer Support for more information on how to obtain supported versions and/or hotfixes for this issue.

6. For **System Platform** remote deployment issues, ensure GR and Runtime nodes have the same *monthly* Microsoft updates and there is no mismatch between the galaxy nodes (for example: both have the Oct 2022 updates).
7. If it is not possible for customers to upgrade to supported versions or apply the hotfixes as described in this document, AVEVA recommends that they continue to disable DCOM hardening and subscribe to this *Tech Alert* to stay informed of any changes.
8. To maintain a safe and secure environment and ensure access to important security updates, it is advisable to keep **System Platform** versions up to date as much as possible. This will help protect against current and future security threats.
9. AVEVA recommends regularly applying Microsoft Windows operating systems updates. Reference Security Central to verify if specific Microsoft updates are supported for use with **System Platform** and other products.

    NOTE: As always, AVEVA highly recommends thorough testing of all system updates or KBs in a non-production environment prior to applying the updates to your production environment.

    NOTE: AVEVA is currently confirming details and test results of Microsoft's Nov 8th update to KB5004442 and will update this *Tech Alert* further once the research is complete.

Preferred Workaround Options for the **AVEVA Enterprise Data Management (eDNA)** related products**:**

- **AVEVA Enterprise Data Management OPC Real-Time Service (eDNA RTS)**: Deploy locally on the OPC server and use data bridging or use AVEVA OI Gateway.
- **AVEVA Enterprise Data Management OPC Data Server (eDNA DA/HDA)**: Deploy locally on the same system as the OPC client.
    - Use data bridging with **AVEVA Enterprise Data Management OPC Real-Time Service**.

NOTE: AVEVA continues testing and the information in this Alert is subject to change. **Subscribe to this *Tech Alert* to be notified of future changes.**

Registry details

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:

> Path : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole\AppCompat
> Value Name: "RequireIntegrityActivationAuthenticationLevel"
> Type: dword
> Value Data: default = not defined or 0x00000000 means disabled. 0x00000001 = enabled.

Set to **0** for Disabled. This setting was the default prior to Jun 2022. After June 2022 the setting can be enabled by *default* but you can disable it using a registry key.

Registry Setting Notes:

- You must provide Value Data in hexadecimal format.
- Enabling the registry key above will make RPC servers enforce an Authentication-Level of PC_C_AUTHN_LEVEL_PKT_INTEGRITY or higher.
- **Reminder:** You must restart your device after setting this registry key for it to take effect.

Additional Information

This article will be updated again in the weeks ahead as research continues. Please continue testing the setting on your systems in non-production environments only.