Content Type	Alert
Article #	000032813
Title	System Platform and related products issues with Microsoft Update KB5004442 - DCOM Hardening
Legacy DocId	
Confidence	Expert Reviewed
Published On	2/14/2023

System Platform and related product issues with Microsoft Update KB5004442 - DCOM Hardening

Affected versions

- **AVEVA System Platform – all versions**
- **AVEVA Historian – all versions**
- **AVEVA OI Gateway and FS Gateway – all versions**
- **AVEVA Enterprise Data Management (eDNA) – all versions**
- **AVEVA Edge – 2020 R2 SP1 and earlier**
- **InduSoft Web Studio – 2020 R2 and earlier**

Situation

In 2021, Microsoft acknowledged a critical security vulnerability in the DCOM protocol and announced intentions to use a phased approach to achieve DCOM security hardening with the following timeline.

- June 2021: DCOM hardening introduced but disabled by default.
- June 2022: DCOM hardening enabled by default, but with an option to disable.
- November 2022: Update including client-side patch to auto raise authentication level
- January 2023: Additional OS versions included in client-side patch updates from November 2022
- March 2023: DCOM hardening enabled by default with no option to disable.

Each date in the timeline comprises multiple KB updates. As each update was released, AVEVA performed extensive testing to evaluate impact. AVEVA continues to both monitor Microsoft's activities with the DCOM hardening plan and to do testing with each update released.

The following Operating systems are affected by KB 5004442:

- Windows Server 2008 and newer server versions
- Windows 7 and newer client OS versions

For more information on DCOM hardening related updates reference Microsoft article KB5004442.

Known Issues

As of January 2023, AVEVA has observed the following with regard to Microsoft's DCOM hardening process.

- **AVEVA System Platform and Historian 2014 R2 SP1 *and later***
  - There are no known technical issues upon enabling DCOM hardening provided the following requirements are met.
    - All nodes in a system are running **System Platform version 2014 R2 SP1 *or later*.**
    - All Microsoft updates related to DCOM hardening, which include Security-only updates and Monthly Rollup updates, up to and including those released in January 2023, have been applied to all nodes in the system.

  NOTE: It is not supported for systems to run with some of these updates, but not all, nor to run with a mismatch in monthly updates between nodes in the same system.

- **AVEVA Historian** server all versions.
  - Remote administration from within the SMC/OCMC does not work.
- **System Platform versions 2014 R2 *or earlier***
  - Because these versions are not in Mainstream nor Extended support, AVEVA has not fully tested the impact of DCOM hardening. Therefore, AVEVA cannot officially support the combination. Systems running these **System Platform versions 2014 R2 *or earlier*** versions on operating systems impacted by DCOM hardening may experience issues with deployment, OPC Server/Tag browsing and remote administration.

- **OI Gateway 5.2** ***or newer***
  - There are no known technical issues upon enabling DCOM hardening provided all updates related to DCOM hardening, which include Security-only updates and Monthly Rollup updates up to and including those released in January 2023, have been applied to all computers hosting this software.
- **OI Gateway 5.1** ***or older,*** and any version of **FS Gateway**
  - Because these versions are not in Mainstream nor Extended support, AVEVA has not fully tested the impact of DCOM hardening. Therefore, AVEVA cannot officially support the combination. Systems running these versions, or any (including newer) version, on a partially updated OS, may experience issues with OPC Client browsing and connectivity.
- **AVEVA Edge and InduSoft Web Studio**
  - AVEVA observed the following behavior when running Studio **OPC DA Server**, **Studio OPC HDA Server**, **OPC DA 2.05 (legacy)**, or **OPC XML/DA Clients** on computers where DCOM hardening is enabled.
    - An inability to browse remote OPC server and data.
    - An inability to read/write OPC items data on the remote OPC server.
    - Local browsing and reading/writing OPC data will work fine.
- **AVEVA Enterprise Data Management**
  - On computers where DCOM Hardening is enabled, the OPC Real-Time Service (eDNA RTS) fails to connect to a remote OPC DA server.

NOTE: As noted above, the **System Platform**, **OI Gateway** and **FS Gateway** issues are resolved with Microsoft's Jan 2023 Updates applied. The other products listed are still in testing and an update will be provided once results are complete.

Solution

- For systems running **System Platform 2014 R2 SP1** ***or later*****,** and/or **OI Gateway version 5.2** ***or later***
  - Apply all Microsoft updates related to DCOM hardening, including Security-only updates and Monthly Rollup updates up to and including those delivered in January 2023.
  - **IMPORTANT:** Previous versions of this *tech alert* advised users to disable DCOM hardening. However, AVEVA *now* recommends changing this to ENABLED once the updates noted above have been applied. If any technical issues occur, please report them to AVEVA immediately.
    - Enable DCOM Hardening by creating the following registry entries (if they do not exist).

      Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole\AppCompat
      Value Type: DWORD
      Value Name: "RequireIntegrityActivationAuthenticationLevel"
      Value Data: 0x00000001

    - Setting the Value Data to 0x00000000 will disable DCOM hardening, but this option will be deprecated in March 2023 and the entire key will become obsolete. The DCOM hardening will be force-enabled at that time.
    - Notes about working with Registry settings:
      - Provide Value Data in hexadecimal format.
      - Restart the device after setting this registry key for it to take effect.
      - Always take extra care when editing the Registry.

- **AVEVA Historian** server remote administration
  - The workaround is to administer the Historian Server via RDP.
- For systems running **System Platform 2014 R2** ***or earlier***,
  - As these versions are not under Mainstream or Extended support, customers are advised to update or upgrade their System Platform installations to a supported version.
- For **AVEVA Edge,** the issues are resolved in the **AVEVA Edge 2020 R2 SP2** release and customers are advised to upgrade to this version**.**
- For **AVEVA Enterprise Data Management (eDNA)** related products, the following workarounds are recommended.
  - **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**.

General Recommendations

- To maintain a safe and secure environment and ensure access to important security updates, keep **System Platform** versions as up to date as possible. This will help protect against current and future security threats.
- 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.
- 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 continues testing and the information in this Alert is subject to change. **Subscribe to this** ***Tech Alert*** **to be notified of future changes.**

Additional Information

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