

Introduzione

Questa Tech Alert illustra come risolvere e/o prevenire le problematiche sorte con l'aggiornamento KB5004442 di Microsoft.

Nel Giugno del 2021 Microsoft ha rilasciato un aggiornamento di sicurezza che aggiunge una chiave di registro (registry key) che abilita l'hardening delle DCOM come riportato da KB5004442. La chiave supporta l'impostazione del valore a 1 (enable).

Mentre Microsoft ha posticipato la prossima fase di questi cambiamenti ([Articolo di Microsoft](#)), AVEVA continua a monitorare le attività di Microsoft riguardo al piano di potenziamento delle DCOM. Le attività di monitoraggio includono la valutazione del potenziale impatto sul portfolio software di AVEVA.

Note: AVEVA sta attualmente confermando i dettagli e i risultati dei test dell'aggiornamento dell'8 novembre di Microsoft relativo a KB5004442 e aggiornerà questo avviso tecnico ulteriormente una volta completata la ricerca.

Versioni

Quanto descritto in questa TA si applica alle seguenti versioni:

- **System Platform 2020 R2 SP1 e versioni precedenti di System Platform 2020 R2**
- **System Platform 2020 P01 e tutte le versioni precedenti di System Platform 2020.**
- **System Platform 2017 U3 SP1 P01 e versioni precedenti di System Platform 2017.**
- **System Platform 2014 R2 SP1 P02 e tutte le versioni precedenti di 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**
- **InduSoft Web Studio 2020 R2 e precedenti**

Problemi Conosciuti

Note: Le seguenti problematiche sono state riscontrate solo mentre la chiave di registro è nello stato "enabled". Non ci sono problematiche riscontrate quando lo stato della chiave è "disabled" (0).

- **OI Gateway e FS Gateway**
 - Impossibile navigare OPC Server remoti e dati
 - La navigazione locale verso i dati OPC funzionerà correttamente.
- **System Platform - Application Server IDE**
 - In fase di design, gli OPC Client Objects non sono in grado di cercare gli OPC Server.
 - In fase di design, gli OPC Client Objects non sono in grado di cercare i tag.

- La ricerca di OPC server e tags su OPC Servers locali utilizzando l'OPC Client Object funzionerà correttamente.
 - Il comportamento di runtime degli OPC Client Objects non viene influenzato indipendentemente dal fatto che il server sia locale o remoto.
 - Il deploy remoto potrebbe non riuscire (quando il nodo GR dispone di aggiornamenti Microsoft mensili precedenti a giugno 2022 e il nodo di runtime dispone di aggiornamenti mensili a partire da giugno 2022).
- **AVEVA Edge and Indusoft Web Studio**
 - **Studio OPC DA Server, Studio OPC HDA Server, OPC DA 2.05 (legacy), OPC XML/DA Clients**
 - Impossibile navigare OPC Server remoti e dati
 - Impossibile leggere/scrivere i dati degli elementi OPC su un OPC Server remoto
 - La navigazione locale e la lettura/scrittura dei dati OPC funzioneranno correttamente.
 - **Historian Server:** l'amministrazione remota interna del SMC non funziona.
 - Il workaround è connettersi via Remote Desktop (RDP) sulla macchina su cui è installato il server Historian e amministrarlo localmente
 - **AVEVA Enterprise Data Management OPC Real-Time Service** non riesce a connettersi al server remoto OPC DA
 - Il client OPC non riesce a connettersi a **AVEVA Enterprise Data Management OPC Data Server DA/HDA (eDNA DA/HDA)**

Workaround

1. Installare gli aggiornamenti cumulativi o gli aggiornamenti mensili da settembre 2021 o successivi su tutte le macchine (compreso l'aggiornamento KB5004440).
2. Disabilitare la chiave di registro per l'hardening delle DCOM. È necessario riavviare la macchina per applicare la modifica dello stato della registry key.

Soluzione

1. I problemi di **OI Gateway** e di **Application Server's \$OPCCClient** sono stati risolti nella **System Platform 2023**.
2. I problemi dell'**OI Gateway** sono stati risolti nel **Communication Drivers Pack 2023**.
3. Sono ora disponibili aggiornamenti di prodotto/hotfix per le versioni dei prodotti supportati da **OI Gateway, dalla 6.0 alla 2020 R3**. Si prega di contattare l'assistenza clienti per ulteriori informazioni o per ottenere un HotFix.
4. I clienti che utilizzano **FS Gateway** devono migrare a una versione di **OI Gateway** in cui è disponibile un hotfix per risolvere questo problema o a **OI Gateway 2023** tramite **Communication Drivers Pack 2023**.
5. I problemi osservati con l'OPC Client Object sono minori e hanno un impatto solo in fase di design. Pertanto, gli aggiornamenti di prodotto e/o le hot fixes mirate al problema, saranno rese disponibili solo per gli ultimi livelli di aggiornamento delle versioni della System Platform ancora sotto il supporto mainstream (vedi la [Product Life Cycle](#) per i dettagli) come segue:
 - **System Platform 2023** e versioni successive: i problemi sono stati risolti in tutte le nuove versioni a partire da **System Platform 2023**.
 - **System Platform 2020 R2 SP1 P01** – I problemi sono stati risolti nella patch 01
 - **System Platform 2020 R2 SP1** – Come mostrato sopra, i problemi sono stati risolti nella Patch 01 e si consiglia di applicare la patch. Tuttavia, è disponibile un hotfix separato per i clienti che non sono in grado di installare la patch.

- **System Platform 2020 R2 P01** – È disponibile un hotfix.
 - **System Platform 2020 R2** – È disponibile un hotfix, ma prima deve essere applicata la Patch 01.
 - **System Platform 2020 P01** – È disponibile un hotfix.
 - **System Platform 2020** – È disponibile un hotfix separato, ma è necessario applicare prima la Patch 01.
 - Per le versioni precedenti della **System Platform** non elencate, contattare il Supporto Tecnico per ulteriori informazioni su come ottenere le versioni supportate e/o hotfix per questo problema.
6. Per i problemi di deployment remoto di **System Platform**, assicurarsi che i nodi GR e Runtime dispongano degli stessi aggiornamenti Microsoft mensili e che siano presenti nessuna discrepanza tra i nodi della Galaxy (ad esempio: entrambi hanno gli aggiornamenti di ottobre 2022).
 7. Se non è possibile per i clienti eseguire l'aggiornamento alle versioni supportate o applicare gli hotfixes come descritto in questo documento, AVEVA consiglia di continuare a disabilitare l'hardening delle DCOM e di iscriversi a questo TechAlert per rimanere informati su eventuali modifiche.
 8. Per mantenere un ambiente sicuro e protetto e garantire l'accesso a importanti aggiornamenti di sicurezza, è consigliabile mantenere le versioni della **System Platform** aggiornate il più possibile. Ciò contribuirà a proteggere dalle minacce alla sicurezza attuali e future.
 9. AVEVA consiglia di applicare regolarmente gli aggiornamenti dei sistemi operativi Microsoft Windows. Fare riferimento al [Security Central](#) per verificare se specifici aggiornamenti Microsoft sono supportati per l'utilizzo con **System Platform** e altri prodotti.

NOTA: come sempre, AVEVA consiglia vivamente di testare tutti gli aggiornamenti di sistema o KB in un ambiente non di produzione prima di applicare gli aggiornamenti all'ambiente di produzione.

NOTA: AVEVA sta attualmente confermando i dettagli e i risultati dei test dell'aggiornamento dell'8 novembre di Microsoft a KB5004442 e aggiornerà questo avviso tecnico ulteriormente una volta completata la ricerca.

Opzioni di Workaround consigliate per i prodotti relativi all' **AVEVA Enterprise Data Management (eDNA)**:

- **AVEVA Enterprise Data Management OPC Real-Time Service (eDNA RTS):** Fare il deploy localmente sul server OPC e usare il data bridging o il Gateway OI AVEVA.
- **AVEVA Enterprise Data Management OPC Data Server (eDNA DA/HDA):** Fare il deploy sullo stesso sistema dell'OPC Client.
 - Usare il data bridging con **AVEVA Enterprise Data Management OPC Real-Time Service**.

NOTA: AVEVA continuerà i test quindi le informazioni in questa Tech Alert saranno soggette a cambiamento. Iscriviti a Tech Alert per essere notificato di successive modifiche

Dettaglio Registro

Durante la fase in cui è possibile abilitare o disabilitare i cambiamenti per il potenziamento di CVE-2021-26414, puoi usare la seguente chiave di registro:

Path: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole\AppCompat

Value Name: "RequireIntegrityActivationAuthenticationLevel"

Type: dword

Value Data: Default = not defined o 0x00000000 significa "disabled". 0x00000001 = "enabled".

Imposta a 0 per "disabled" (di default fino a Giugno 2022. Dopo questa data potrebbe essere "enabled" di default ma con la possibilità di essere disattivata usando una chiave di registro).

Note di impostazione registro:

- È necessario fornire "Value Data" in formato esadecimale.
- Abilitare la chiave di registro di cui sopra porterà il server RPC ad avere un Authentication-Level di "PC_C_AUTHN_LEVEL_PKT_INTEGRITY" o superiore.
- Ricorda: è necessario riavviare la macchina dopo l'impostazione della chiave di registro perché questa abbia effetto.

Informazioni Aggiuntive

Questo articolo verrà aggiornato nel momento in cui la ricerca sarà completata. Continuare a testare i cambiamenti in un ambiente non produttivo.

Referenze

- Per il download del seguente documento in lingua inglese, fare riferimento a questo link [TA000032813](#)
- Microsoft Web Site

Autore: C.Tessitore

Disclaimer

Il presente documento è fornito a scopo di esempio e non sostituisce la documentazione AVEVA. L'applicazione di quanto contenuto, in un preciso ambito applicativo, deve essere sempre validata da un tecnico Wonderware. La documentazione rilasciata da AVEVA resta il riferimento tecnico ufficiale da seguire: softwaresupport.aveva.com. Wonderware Italia non si assume la responsabilità di un'applicazione scorretta di questo documento.