optimize!
softing

AUSWIRKUNGEN UND LÖSUNGEN

Informationen zur OPC Classic Kommunikation im Zusammenhang mit dem Microsoft DCOM-Sicherheitspatch KB5004442 (CVE-2021-26414)

Februar 2023

Industrial

Microsoft Update KB 5004442 – DCOM Server Security Feature Bypass (CVE-2021-26414)

Am 8. Juni 2021 hat Microsoft ein Sicherheitsupdate (KB 5004442) veröffentlicht, um Sicherheitslücken im DCOM Remote Protocol zu beheben. Die Details dieser Schwachstellen sind im CVE-2021-26414 beschrieben. Mit dem Distributed Component Object Model (DCOM) Remote Protocol werden Anwendungsobjekte mit Hilfe von Remoteprozeduraufrufen (RPCs) offengelegt. Das Protokoll dient der Kommunikation zwischen den Softwarekomponenten vernetzter Geräte.

Auswirkungen auf die OPC Classic-Kommunikation

OPC Classic-Anwendungen basieren auf der proprietären COM-Technologie (Component Object Model) von Microsoft. Windows aktiviert automatisch die Distributed COM (DCOM)-Funktionalität, wenn COM-basierte Anwendungen versuchen, über ein Netzwerk miteinander zu kommunizieren.

OPC Classic-Clients und -Server sind COM-Komponenten. Sie unterliegen den Einschränkungen des Windows DCOM-Sicherheitsframeworks. Änderungen an den Windows-Sicherheitseinstellungen, die über Betriebssystem-Updates veröffentlicht werden, können die OPC Classic-Kommunikation beeinträchtigen.

Das DCOM-Sicherheitsupdate KB 5004442 wirkt sich auf die Konnektivität von OPC-Komponenten aus. Mit der Aktivierung der neuen Sicherheitsfunktion sind nur noch DCOM-Verbindungen (Netzwerkverbindungen) zwischen OPC-Servern und Clients möglich, welche eine paketbasierte Authentifizierung unterstützen. Die Kommunikation zwischen OPC Classic-Servern und Clients, welche auf demselben Computer ausgeführt wird, ist dabei nicht beeinträchtigt.

Detaillierte Informationen über die Auswirkungen dieses KB 5004442 DCOM-Sicherheitsupdates, sind auf der Microsoft Website verfügbar.

Zeitplan der DCOM-Sicherheitsupdates

8. Juni 2021 – Phase 1

- Microsoft veröffentlich den Sicherheitspatch KB5004442.
- Änderungen sind standardmäßig deaktiviert.
- Die neuen Sicherheitsmechanismen können über Windows Registrierungsschlüssel aktiviert werden.

14. Juni 2022 – Phase 2

- Microsoft veröffentlicht ein Windows Updates, welches die Sicherheitsmechanismen standardmäßig aktiviert.
- Anwender können die Sicherheitsmechanismen mithilfe eines Windows Registrierungsschlüssels deaktivieren.

14. März 2023 – Phase 3

- Die Sicherheitsfunktionsänderungen sind standardmäßig aktiviert.
- Eine Deaktivierung ist nicht mehr möglich.
- Anwender müssen zu diesem Zeitpunkt alle Kompatibilitätsprobleme mit den Härtungsänderungen und Anwendungen in ihrer Umgebung beheben.

Ab Inkrafttreten der Phase 3 am 14. März 2023 funktioniert die auf DCOM basierende OPC-Kommunikation möglicherweise nicht mehr.

Welche Windows Versionen sind betroffen?

Aktuell gilt das DCOM-Sicherheitsupdate für die folgenden Windows-Versionen.

- Windows-Server 2019
- Windows Server 2012 R2
- Windows-Server 2016
- Windows Server 2008
- Windows 10
- Windows 8.1
- Windows 7

Betroffene Produkte von Softing Industrial

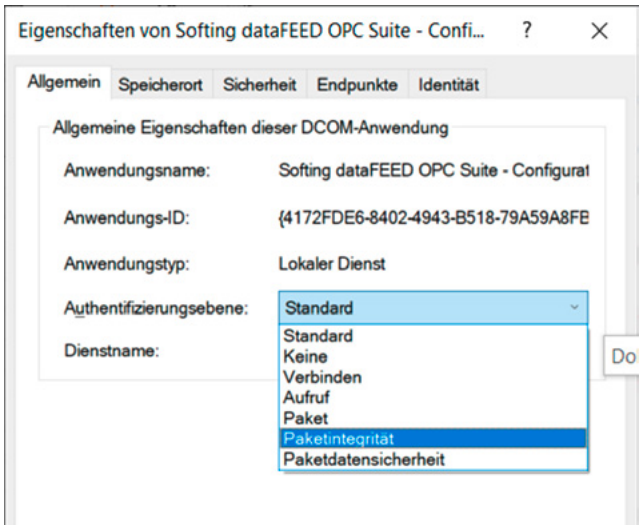
Für die unten aufgeführten OPC-Produkte empfehlen wir dringend die Verwendung eines OPC-Tunnels anstelle der DCOM-basierten OPC Classic-Netzwerkkommunikation. Andernfalls können wir nicht garantieren, dass die Produkte mit dem Microsoft-Patch korrekt funktionieren.

- dataFEED OPC Suite Version 5.19 oder älter.
- Softing S7/S5 OPC-Server
- Softing Modbus-OPC-Server
- Softing Profibus OPC-Server
- Multiprotokoll-OPC-Server (INAT Multiprotocol OPC Server)

Lösung im Falle eines Verbindungsausfalls

Wenn Ihre OPC-Verbindung nach Anwendung des obligatorischen Microsoft-Patches fehlschlägt, überprüfen Sie bitte, ob die Authentifizierungsebene auf „Paketintegrität“ oder „Paketdatenschutz“ eingestellt ist.

Der folgende Screenshot veranschaulicht, wo diese Authentifizierungsebene im Dialogfeld „Windows-Komponentendienste“ konfiguriert wird.



HINWEIS: Softing leistet keinen Support bei Problemen mit OPC Classic Remote-Netzwerkverbindungen

Falls das Problem auch bei korrekter Authentifizierungsebene nicht behoben ist, empfehlen wir die Verwendung der dataFEED OPC-Tunnel-Lösung.

Softing Industrial Empfehlung

Softing arbeitet fortlaufend daran, seine OPC Classic-Anwendungen zu verbessern, damit sie mit allen aktuellen und zukünftigen DCOM-Sicherheitsupdates weiterhin ordnungsgemäß funktionieren.

Dessen ungeachtet empfehlen wir unseren Kunden den Einsatz der dataFEED OPC Tunnel-Lösung von Softing anstelle einer DCOM-basierten OPC Classic Remote-Verbindung. Die OPC Tunnel-Lösung gewährleistet eine stabile OPC Classic Remote-Kommunikation und ist unabhängig von Microsoft Patches. Darüber hinaus sind Installation und Betrieb wesentlich einfacher als das Aufsetzen einer DCOM-basierten OPC Classic Remote-Kommunikation.

Detaillierte Informationen zur dataFEED OPC Tunnel-Lösung und eine kostenlose Testversion finden Sie unter: dataFEED OPC Tunnel

Wenn Sie Fragen haben, kontaktieren Sie uns unter: info.automation@softing.com.

optimize!
softing

https://industrial.softing.com