optimize!
softing

IMPACT AND SOLUTIONS

关于Microsoft DCOM 安全补丁 KB5004442 (CVE-2021-26414) 对 OPC Classic通信的影响及解决方案

2023 年 2月

Industrial

Windows更新 KB 5004442 – DCOM 服务器安全功能旁路 (CVE-2021-26414)

2021 年 6 月 8 日，Microsoft 发布了安全更新 (KB 5004442) 以解决 DCOM 远程协议中的漏洞。在 CVE-2021-26414 中描述了这些漏洞的详细信息。 分布式组件对象模型（DCOM）远程协议是一种使用远程过程调用（RPC）公开应用程序对象的协议，它支持远程过程调用，并且可用于网络设备的软件组件之间的通信。

对 OPC Classic通信的影响

OPC Classic 应用程序使用了基于 Microsoft 专有的 COM（Component Object Model 组件对象模型）技术。 当基于 COM 的应用程序尝试通过网络相互通信时，Windows 会自动激活分布式 COM (DCOM) 功能。

OPC Classic 客户端和服务器是受到Windows DCOM 安全框架限制的 COM 组件。 随着操作系统更新，微软发布的安全设置的更改可能会影响OPC Classic通信。

DCOM 安全更新 KB 5004442 将影响 OPC 组件的连接。新的安全功能激活之后，OPC服务器和那些支持基于数据包的身份验证的客户端之间只能建立 DCOM 连接（网络连接）。 这不会影响在同一台计算机上运行的 OPC Classic 服务器和客户端之间的通信。有关此 KB 5004442 DCOM 安全更新影响的详细信息，请访问 Microsoft 网站。

DCOM 安全更新时间线

2021 年 6 月 8 日 - 第一阶段

- Microsoft 发布安全补丁 KB5004442。
- 默认情况下禁用更改。
- 可以通过 Windows 注册表项激活新的安全机制。

2022 年 6 月 14 日 - 第二阶段

- Microsoft 发布了在默认情况下激活安全机制的 Windows 更新。
- 用户可以使用 Windows 注册表项禁用安全机制。

2023 年 3 月 14 日 - 第三阶段

- 默认情况下启用安全功能更改。
- 不可停用。
- 此时，用户必须解决其环境中强化更改和应用程序的任何兼容性问题。

© Copyright 2023 Softing Industrial Automation GmbH

从第 3 阶段的生效日期 （2023 年 3 月 14 日）开始，基于 DCOM 的 OPC 网络通信可能不再生效。

哪些Windows版本会受到影响?

DCOM安全更新目前会影响以下Windows版本:

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

受影响的Softing 工业自动化产品

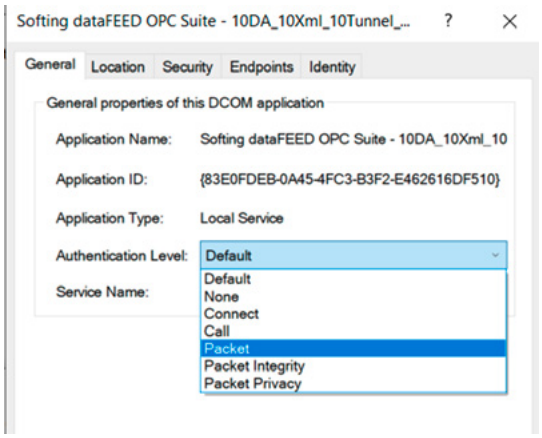
对于下面列出的 OPC 产品，我们强烈建议使用 OPC Tunnel 而不是基于 DCOM 的 OPC Classic网络通信。 我们无法确保以下产品可以在 Microsoft 安全补丁下正常工作。

- dataFEED OPC Suite Version 5.19 及更早版本
- Softing S7/S5 OPC Server
- Softing Modbus OPC Server
- Softing Profibus OPC Server
- Multiprotocol OPC Servers (INAT Multiprotocol OPC Server)

连接失败的解决方法

dataFEED OPC Suite 5.20 及以上版本提供Windows安全更新补丁KB5004442（CVE-2021-26414）所需的身份验证级别“数据包完整性（Packet Integrity）”和“数据包保密性（Packet Privacy）”，并支持安全更新后的 OPC Classic 远程网络通信。
如果在应用此强制性 Microsoft 补丁后您的 OPC 应用连接失败，请检查应用DCOM配置中身份验证级别是否设置为“数据包完整性（Packet Integrity）”或“数据包保密性（Packet Privacy）”。以下截图显示了在 Windows 组件服务对话框中配置此身份验证级别的位置。

© Copyright 2023 Softing Industrial Automation GmbH



请注意：Softing 不提供对 OPC Classic 远程网络连接问题的支持。

如果使用正确的身份验证级别仍无法解决问题，Softing 推荐使用 dataFEED OPC Tunnel解决方案。

Softing 的建议

Softing 一直致力于改进 OPC Classic 应用程序，以确保其与所有当前和未来的 DCOM 安全更新一起正常工作。 但是，我们建议我们的客户使用 Softing 的 dataFEED OPC Tunnel 解决方案，而不是基于 DCOM 的 OPC Classic 远程连接。 OPC Tunnel 解决方案确保稳定的 OPC Classic 远程通信，并且不会受到 Microsoft 补丁的影响。 此外，其安装和配置比设置基于 DCOM 的 OPC Classic 远程通信要容易得多。有关 dataFEED OPC Tunnel解决方案和免费试用版的详细信息，请访问: dataFEED OPC Tunnel

如果您有任何问题，请联系我们： info@softingchina.com

© Copyright 2023 Softing Industrial Automation GmbH

optimize!
softing

https://industrial.softing.com