MONTELEKTRO

SJEDIŠTE RIJEKA
Kudeji 53
HR-51215 Kastav
rijeka@montelektro.hr
+ 385 51 54 58 10

URED ZAGREB
Marka Marulića 5
HR-10431 Sv. Nedelja
zagreb@montelektro.hr
+ 385 1 39 09 020

SECURITY ADVISORY

CVE-2021-26414 Windows DCOM Server Security Feature Bypass

Revision history:

Date	Rev.	Description
13.02.2023.	3	[DFL]: BatchMe and Siemens engineering tools status added
23.08.2022.	2	[DFL]: Aveva/Wonderware status added
01.08.2022.	1	[DFL]: Initial release

TABLE OF CONTENTS

1. INTRODUCTION

A medium vulnerability in Microsoft Windows operating systems identified by *CVE-2021-26414 Windows DCOM Server Security Feature Bypass* has been publicly disclosed by Microsoft at 8th of June 2021. This vulnerability requires that a user with an affected version of Windows access a malicious server. An attacker would have to host a specially crafted server share or website. An attacker would have no way to force users to visit this specially crafted server share or website but would have to convince them to visit the server share or website, typically by way of an enticement in an email or chat message.

Montelektro is aware of this vulnerability and of how it could, if exploited, potentially impact our customers' environments. We are continuously monitoring security advisories published by vendors and testing our own components used in IT infra and PCS (Process Control System) solutions.

Microsoft has released security patches targeting the vulnerability on Windows operating systems. Patches significantly change the functionality of part of the operating system, which can affect the functionality of the PCS solution. The activation of the Microsoft patch must therefore be delayed until the vendors of all PCS components publish patches for their components or confirm that the activation of the Microsoft patch does not affect the operation of the component.

2. VULNERABILITY METRICS

2.1. Base metrics

The Base metric group represents the intrinsic characteristics of a vulnerability that are constant over time and across user environments. It is composed of two sets of metrics: the *Exploitability metrics* and the *Impact metrics*.

The *Exploitability metrics* reflect the ease and technical means by which the vulnerability can be exploited. That is, they represent characteristics of *the thing that is vulnerable*, which we refer to formally as the **vulnerable component**. On the other hand, the *Impact metrics* reflect the direct consequence of a successful exploit and represent the consequence to *the thing that suffers the impact*, which we refer to formally as the **impacted component**.

Table 1 - Vulnerability Exploitability metrics

Metric	Value
Attack Vector This metric reflects the context by which vulnerability exploitation is possible. The Base Score increases the more remote (logically, and physically) an attacker can be to exploit the vulnerable component.	**Network** The vulnerable component is bound to the network stack and the set of possible attackers extends beyond the other options listed, up to and including the entire Internet. Such a vulnerability is often termed 'remotely exploitable' and can be thought of as an attack being exploitable at the protocol level one or more network hops away (e.g., across one or more routers).
Attack Complexity This metric describes the conditions beyond the attacker's control that must exist to exploit the vulnerability. Such conditions may require the collection of more information about the target or computational exceptions. The assessment of this metric excludes any requirements for user interaction to exploit the vulnerability. If a specific configuration is required for an attack to succeed, the Base metrics should be scored assuming the vulnerable component is in that configuration.	**High** A successful attack depends on conditions beyond the attacker's control. That is, a successful attack cannot be accomplished at will, but requires the attacker to invest in some measurable amount of effort in preparation or execution against the vulnerable component before a successful attack can be expected. For example, a successful attack may require an attacker to: gather knowledge about the environment in which the vulnerable target/component exists; prepare the target environment to improve exploit reliability; or inject themselves into the logical network path between the target and the resource requested by the victim to read and/or modify network communications (e.g., a man in the middle attack).
Privileges Required This metric describes the level of privileges an attacker must possess before successfully exploiting the vulnerability.	**Low** The attacker is authorized with (i.e., requires) privileges that provide basic user capabilities that could normally affect only settings and files owned by a user. Alternatively, an attacker with Low privileges may have the ability to cause an impact only to non-sensitive resources.
User Interaction This metric captures the requirement for a user, other than the attacker, to participate in the successful compromise the vulnerable component. This metric determines whether the vulnerability can be exploited solely at the will of the attacker, or whether a separate user (or user-initiated process) must participate in some manner.	**Required** Successful exploitation of this vulnerability requires a user to take some action before the vulnerability can be exploited.
Scope Does a successful attack impact a component other than the vulnerable component? If so, the Base Score increases and the Confidentiality, Integrity	**Unchanged** An exploited vulnerability can only affect resources managed by the same security authority. In this case, the vulnerable component and

Metric	Value
and Authentication metrics should be scored relative to the impacted component.	the impacted component are either the same, or both are managed by the same security authority.

Table 2 - Vulnerability Impact metrics

Metric	Value
Confidentiality impact This metric measures the impact to the confidentiality of the information resources managed by a software component due to a successfully exploited vulnerability. Confidentiality refers to limiting information access and disclosure to only authorized users, as well as preventing access by, or disclosure to, unauthorized ones.	**None** There is no loss of confidentiality within the impacted component.
Integrity impact This metric measures the impact to integrity of a successfully exploited vulnerability. Integrity refers to the trustworthiness and veracity of information.	**High** There is a total loss of integrity, or a complete loss of protection. For example, the attacker can modify any/all files protected by the impacted component. Alternatively, only some files can be modified, but malicious modification would present a direct, serious consequence to the impacted component.
Availability impact This metric measures the impact to the availability of the impacted component resulting from a successfully exploited vulnerability. It refers to the loss of availability of the impacted component itself, such as a networked service (e.g., web, database, email). Since availability refers to the accessibility of information resources, attacks that consume network bandwidth, processor cycles, or disk space all impact the availability of an impacted component.	**None** There is no impact to availability within the impacted component.
Scope Does a successful attack impact a component other than the vulnerable component? If so, the Base Score increases and the Confidentiality, Integrity and Authentication metrics should be scored relative to the impacted component.	**Unchanged** An exploited vulnerability can only affect resources managed by the same security authority. In this case, the vulnerable component and the impacted component are either the same, or both are managed by the same security authority.

2.2. Vulnerability Temporal metrics

The *Temporal metric* group reflects the characteristics of a vulnerability that may change over time but not across user environments. For example, the presence of a simple-to-use exploit kit would increase the CVSS score, while the creation of an official patch would decrease it.

Table 3 - Vulnerability Temporal metrics

Metric	Value
Exploit Code Maturity This metric measures the likelihood of the vulnerability being attacked and is typically based on the current state of exploit techniques, exploit code availability, or active, 'in-the-wild' exploitation.	**Unproven** No exploit code is available, or an exploit is theoretical.
Remediation Level The Remediation Level of a vulnerability is a key factor for prioritization. The typical vulnerability is unpatched when initially published. Workarounds or hotfixes may offer interim remediation until an official patch or upgrade is issued. Each of these respective stages adjusts the temporal score downwards, reflecting the decreasing urgency as remediation becomes final.	**Official fix** A complete vendor solution is available. Either the vendor has issued an official patch, or an upgrade is available.
Report Confidence This metric measures the degree of confidence in the existence of the vulnerability and the credibility of the known technical details. Sometimes only the existence of vulnerabilities is publicized, but without specific details. For example, an impact may be recognized as undesirable, but the root cause may not be known. The vulnerability may later be corroborated by research which suggests where the vulnerability may lie, though the research may not be certain. Finally, a vulnerability may be confirmed through acknowledgement by the author or vendor of the affected technology. The urgency of a vulnerability is higher when a vulnerability is known to exist with certainty. This metric also suggests the level of technical knowledge available to would-be attackers.	**Confirmed** Detailed reports exist, or functional reproduction is possible (functional exploits may provide this). Source code is available to independently verify the assertions of the research, or the author or vendor of the affected code has confirmed the presence of the vulnerability.

3. PCS COMPONENT DEPENDENCY AND STATUS MATRIX

The PCS component dependency matrix is designed for users of our PCS solutions so that they can monitor the exposure status and plan system components patching in timely fashion. For each PCS solution in the matrix, you can find on which components the solution depends and which component requires patch deployment.

The installation of security patches should be postponed until each dependent component can be updated or is declared as unaffected by the component vendor.

Table 4 - PCS component dependency and status matrix

PCS Solution	BatchMe	GE Digital	ProLeiT	Rockwell	Siemens	Windows	Aveva
BatchMe ArchestrA Rockwell PLC	●	–	–	●[1]	–	●	●
BatchMe ArchestrA Siemens PLC	●	–	–	–	●	●	●
BatchMe FactoryTalk Rockwell PLC	●	–	–	●	–	●	–
BatchMe iFix Siemens PLC	●	●	–	–	●	●	–
BatchMe InTouch Rockwell PLC	●	–	–	●[1]	–	●	●[2]
BatchMe InTouch Siemens PLC	●	–	–	–	●	●	●[2]
BatchMe WinCC Siemens PLC	●	–	–	–	●	●	–
ProLeiT brewmaxx Siemens PLC	–	–	●	–	●	●	–
ProLeiT brewmaxx Rockwell PLC	–	–	●	●	–	●	–

– solution does not depend on the component

◌ component status currently unknown

● component patching required

● patching required for some component versions

● component patching not required

[1] Only if engineering tools are used
[2] Only if Historian is used

4. PCS COMPONENTS

4.1. Montelektro BatchMe

Vulnerability exposure status of Montelektro components in PCS solutions.

Table 5 - Montelektro BatchMe components vulnerability exposure status

Component	Version	Status
Control Module Configurator	CmCfg v3.3.2	Unaffected
Control Module Configuration Downloader	CmCfgDL v3.4.0.1	Unaffected
Control Recipe Editor	CREditor v3.0.1.6654	Unaffected
Configuration Downloader	DownloadMe v3.2.3	Unaffected
Interlock Editor	ILCKEditor v2.3.0	Unaffected
Material Editor	MaterialMe v3.3.4	Unaffected
Recipe Editor	MBatchManager v3.5.1	Unaffected
OPC Connector	OPCConn v3.5.1	Unaffected
OPC Connector UA	OPCConnUA v4.2.13	Unaffected
Production Scheduler	ServeMe v3.1.13	Unaffected
Time-Table Editor	TTEditor v1.0.0.6	Unaffected

4.2. Microsoft Windows

Vulnerability exposure status of Microsoft Windows components used in Montelektro PCS solutions.

Table 6 - Microsoft Windows vulnerability exposure status

Product	Version	Security advisory	Status
Windows 10 Enterprise	Windows 10 Enterprise 2019 LTSC Windows 10 Enterprise and Education, version 1909 Windows 10 Enterprise, version 1909	KB5004442 - Manage changes for Windows DCOM Server Security Feature Bypass (CVE-2021-26414)	Affected
Windows 10 IoT	Windows 10 IoT Core 2019 LTSC Windows 10 IoT Enterprise 2019 LTSC Windows 10 IoT Enterprise, version 1909	KB5004442 - Manage changes for Windows DCOM Server Security Feature Bypass (CVE-2021-26414)	Affected
Windows 10	Windows 10, version 1607, all editions Windows 10, version 2004, all editions Windows 10, version 20H2, all editions Windows 10, version 21H1, all editions	KB5004442 - Manage changes for Windows DCOM Server Security Feature Bypass (CVE-2021-26414)	Affected
Windows 7/8	Windows 7 Windows 8.1	KB5004442 - Manage changes for Windows DCOM Server Security Feature Bypass (CVE-2021-26414)	Affected
Windows Embedded	Windows Embedded 8 Standard Windows Embedded 8.1 Industry Enterprise Windows Embedded 8.1 Industry Pro Windows Embedded POSReady 7 ESU Windows Embedded Standard 7 ESU	KB5004442 - Manage changes for Windows DCOM Server Security Feature Bypass (CVE-2021-26414)	Affected
Windows Server	Windows Server 2008 Windows Server 2008 R2 Windows Server 2012 Windows Server 2012 R2 Windows Server 2016, all editions Windows Server 2019 Windows Server 2022 Windows Server version 2004 Windows Server, version 20H2, all editions	KB5004442 - Manage changes for Windows DCOM Server Security Feature Bypass (CVE-2021-26414)	Affected

4.3. ProLeiT

Vulnerability exposure status of ProLeiT components used in Montelektro PCS solutions.

Table 7 - ProLeiT components vulnerability exposure status

Product	Version	Security advisory	Status
Entire portfolio	All versions	Received a statement from ProLeiT Helpdesk service: *ProLeiT's system software is certainly not affected by the changes to the DCOM settings published by Microsoft in the above <security notice>. There are also no known project solutions that have used DCOM for customer installations.* Subject: Proposal for solution for your request "Windows DCOM Server Security Feature Bypass (CVE-2021-26414)" // # 92184392 - [ref:_00DA0abSm._5008V1NbF3f:ref] Smoke test for ***Microsoft update June 14, 2022*** listed as ***passed*** at ProLeiT Web site. MS Patches Plant iT / brewmaxx V9.80 (Results) 15/07/2022 MS Patches Plant iT / brewmaxx V9.70 (Results) 15/07/2022 MS Patches Plant iT / brewmaxx V9.60 (Results) 15/07/2022	Unaffected

4.4. GE Digital

Vulnerability exposure status of GE Digital components used in Montelektro PCS solutions.

Table 8 - GE Digital components vulnerability exposure status

Product	Version	Security advisory	Status
iFix	iFix 2022	Microsoft Windows DCOM Server Security Feature Bypass Patch for CVE-2021-26414	Unaffected
	iFix 6.5 iFix 6.1 iFix 6.0 iFix 5.9 iFix 5.8	Microsoft Windows DCOM Server Security Feature Bypass Patch for CVE-2021-26414	Affected
Historian	Historian 2022	Microsoft Windows DCOM Server Security Feature Bypass Patch for CVE-2021-26414	Unaffected
	Historian 9.1 Historian 9.0 Historian 8.1 Historian 8.0 Historian 7.2 Historian 7.1 Historian 7.0	Microsoft Windows DCOM Server Security Feature Bypass Patch for CVE-2021-26414	Affected
Industrial Gateway Server (IGS)	All versions	Microsoft Windows DCOM Server Security Feature Bypass Patch for CVE-2021-26414	Unaffected

4.5. Siemens

Vulnerability exposure status of Siemens components used in Montelektro PCS solutions.

Table 9 - Siemens components vulnerability exposure status

Product	Version	Security advisory	Status
SIMATIC WinCC	WinCC V7.3 Upd 9 WinCC V7.4 SP1 WinCC V7.5	Which Microsoft patches are recommended for operating SIMATIC WinCC V7 ("Security Updates", "Critical Updates" and "Definition Updates")?	Unaffected
	WinCC V7.3 prior to Upd 9 WinCC V7.4 prior to SP1	Which Microsoft patches are recommended for operating SIMATIC WinCC V7 ("Security Updates", "Critical Updates" and "Definition Updates")?	Affected

4.6. Rockwell

Affected Rockwell Automation products use *FactoryTalk Services Platform*, *FactoryTalk Live Data*, *OPC-DA*, or are using *Windows APIs* to establish DCOM connections between two computers.

Rockwell Automation products may be *directly* or *indirectly* affected by Microsoft's patch. For example:

- *ThinManager* is **directly** affected because it uses DCOM between the *ThinManager UI* and a remote *ThinServer service*
- *Studio 5000 Logix Designer* is **indirectly** affected because it uses *FactoryTalk Services*, specifically *FactoryTalk Security*, and *FactoryTalk Services* uses DCOM between the *FactoryTalk Directory server* and *FactoryTalk Directory client*
- *FactoryTalk Product Management* is **indirectly** affected because it uses *FactoryTalk ProductionCentre*, and *FactoryTalk ProductionCentre* uses *FactoryTalk Services* and *FactoryTalk Live Data*

Table 10 – Directly affected Rockwell components

Product	Version	Security advisory
FactoryTalk Services	6.21, 6.20, 6.11, 6.10, 3.00, 2.90	Product Notification 2022-01-001 - Rockwell Automation products unable to establish proper DCOM connection after installing Microsoft DCOM Hardening patch (CVE-2021-26414)
RSLinx Classic	4.21, 4.20, 4.12, 4.11, 4.10, 4.00.01	
FactoryTalk Linx	6.21, 6.20, 6.11, 6.10, 6.00, 5.90	
FactoryTalk Linx Gateway	6.21, 6.20, 6.11, 6.10, 6.00, 3.90	
FactoryTalk Linx Data Bridge	6.21.01, 6.20, 6.11	
FactoryTalk View Site Edition	12.00, 11.00, 10.00, 9.00	
FactoryTalk ViewPoint	12.00, 11.00, 10.00, 9.00	
FactoryTalk Batch	15.00, 14.00, 13.00.02	
ThinManager	12.01, 12.00, 11.02, 11.01, 11.00	
FactoryTalk ProductionCentre	10.01, 10.02, 10.03, 10.04	
FactoryTalk Transaction Manager	13.10, 13.00, 12.10, 12.00	
FactoryTalk VantagePoint	8.31, 8.30, 8.20, 8.10, 8.00, 7.00	
Pavilion8	5.17.01, 5.17.00, 5.16, 5.15.01, 5.15	
Emonitor Condition Monitoring Software	4.00	
KEPServer Enterprise	All versions	
AADvance OPC Portal	All versions	
AADvance OPC Standalone	All versions	
Trusted OPC Portal	All versions	

Table 11 - Indirectly affected Rockwell components

Product list		
• FactoryTalk Policy Manager	• Application Code Manager	• FactoryTalk EI Hub
• FactoryTalk System Services	• FactoryTalk View Machine Edition	• FactoryTalk PharmaSuite
• FactoryTalk Linx CommDTM	• RSNetWorx	• FactoryTalk AutoSuite
• ControlFLASH	• RSLogix 5000	• FactoryTalk CPGSuite
• ControlFLASH Plus	• RSLogix 500	• FactoryTalk Analytics EdgeML
• Studio 5000 Logix Designer	• RSLogix 5	• FactoryTalk Analytics DataView
• Studio 5000 View Designer	• FactoryTalk Metrics	• FactoryTalk Analytics DataFlowML
• Studio 5000 Logix Emulate	• FactoryTalk Production Management	• FactoryTalk Analytics AugmentedModeler
• Studio 5000 Architect	• FactoryTalk Quality Management	• FactoryTalk Historian - ThingWorx Connector
• FactoryTalk Logix Echo	• FactoryTalk Warehouse Management	• FactoryTalk EnergyMetrix
• FactoryTalk AssetCentre		
• FactoryTalk Historian SE		

Table 12 - Unaffected Rockwell components

Product list		
• FactoryTalk Activation Manager	• PanelView Plus 6 / 7	• Connected Components Workbench
• FactoryTalk Updater	• PlantPAx MPC	• FactoryTalk Historian ME
• Studio 5000 Add On Profiles	• PlantPAx Process Object Online Configuration Tool	

Table 13 - End of Life or Discontinued Rockwell components

Product list		
• FactoryTalk Performance Management	• RSView 32 (Active Display)	• GuardPLC OPC Server

4.7. Aveva/Wonderware

Vulnerability exposure status of Aveva/Wonderware components used in Montelektro PCS solutions.

Table 14 – Aveva/Wonderware components vulnerability exposure status

Product	Program	Security advisory	Status
System Platform 2023	Application server Common services Communication drivers Historian 2023 Historian Client 2023 InTouch HMI 2023 Licensing services	System Platform issues with Microsoft Update KB5004442 - DCOM Hardening	Unaffected
System Platform 2020	Application server Historian	System Platform issues with Microsoft Update KB5004442 - DCOM Hardening	Affected
	Historian Client InTouch HMI		Unaffected
System Platform 2017	Application server Historian	System Platform issues with Microsoft Update KB5004442 - DCOM Hardening	Affected
	Historian Client InTouch		Unaffected
System Platform 2014	Application server Historian	System Platform issues with Microsoft Update KB5004442 - DCOM Hardening	Affected
	Historian Client InTouch		Unaffected

4.8. Engineering tools

Windows patches on systems using engineering tools like Simatic Manager, RS Logix and similar should not be deployed and activated unless engineering tools are patched or declared as unaffected.

Siemens engineering tools (Simatic Manager, TIA portal) are not affected.

Rockwell engineering tools are confirmed as indirectly affected; users must make sure patches for used product version are deployed prior to activating the Windows patch.

5. AVAILABLE MITIGATIONS AND FIXES

5.1. Montelektro BatchMe

Montelektro BatchMe components are not affected and considered safe to patch.

5.2. Microsoft Windows

Windows patch should be deployed and enabled only after all other affected components are patched.

5.3. ProLeiT

ProLeiT systems based on Rockwell PLC use Rockwell components for PLC communication. Rockwell patches for affected components must be deployed before the Windows patch is deployed and enabled.

Microsoft Windows in ProLeiT systems based on Siemens PLC are considered safe to patch.

5.4. GE Digital

Detailed patching guidelines are available at GE website: Microsoft Windows DCOM Server Security Feature Bypass Patch for CVE-2021-26414

5.5. Siemens

Detailed patching guidelines are available at Siemens website: Which Microsoft patches are recommended for operating SIMATIC WinCC V7 ("Security Updates", "Critical Updates" and "Definition Updates")?, chapter *Notes on Windows DCOM Server hardening measures (KB5004442)*.

5.6. Rockwell

Detailed patching guidelines are available at Rockwell website: Microsoft DCOM Hardening Information TOC.

5.7. Aveva

Workaround for affected Aveva products available at Aveva website: System Platform issues with Microsoft Update KB5004442 - DCOM Hardening. AVEVA continues testing and the information in this Alert is subject to change.

6. MITIGATION RECOMMENDATIONS

As a general security measure, Montelektro strongly recommends protecting network access to devices with appropriate mechanisms.

Patch planning and administration guidelines from Process Control System – IT maintenance and security Whitepaper should be considered during the patch deployment.

Since available Windows patch significantly affects multiple PCS components, Windows patch should not be activated until all affected components are fully patched according to the vendor guidelines.

An active SLA contract can be used to support the installation of the patch on components supplied by Montelektro.

7. REFERENCES

AVEVA. (2022, Jume 29). *System Platform issues with Microsoft Update KB5004442 - DCOM Hardening*. Retrieved from Knowledge and Support center: https://softwaresupportsp.aveva.com/#/okmimarticle/docid/ta000032813

FIRST. (2021, July 25). *Common Vulnerability Scoring System v3.0: Specification Document*. Retrieved from Forum of Incident Response and Security Teams: https://www.first.org/cvss/v3.0/specification-document

GE. (2022, June 09). *Microsoft Windows DCOM Server Security Feature Bypass Patch for CVE-2021-26414*. Retrieved from GE Customer Center: https://digitalsupport.ge.com/communities/en_US/Article/Microsoft-Windows-DCOM-Server-Security-Feature-Bypass-Patch-for-CVE-2021-26414

Microsoft. (2022, June 24). *KB5004442 - Manage changes for Windows DCOM Server Security Feature Bypass (CVE-2021-26414)*. Retrieved from Windows support: https://support.microsoft.com/en-us/topic/kb5004442-manage-changes-for-windows-dcom-server-security-feature-bypass-cve-2021-26414-f1400b52-c141-43d2-941e-37ed901c769c

Microsoft. (2022, June 28). *Security Vulnerability CVE-2021-26414 Windows DCOM Server Security Feature Bypass*. Retrieved from Microsoft Security Response Center (MSRC): https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26414

Montelektro. (2019, July). *Process Control System – IT maintenance and security Whitepaper.* Retrieved from Montelektro Web site: https://www.montelektro.hr/wp-content/uploads/2022/07/KB1007-Process-Control-System-IT-maintenance-and-security-.pdf

ProLeiT. (2022, July 27). *Recommended Microsoft Patches*. Retrieved from ProLeiT Web site: https://www.proleit.com/support/mspatches/

Rockwell Automation. (2022, June 06). *Mitigating Microsoft DCOM Hardening Patch (CVE-2021-26414) for Affected Rockwell Automation Products*. Retrieved from Rockwell Automation Web site: https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1134040/~/mitigating-microsoft-dcom-hardening-patch-(cve-2021-26414)-for-affected

Rockwell Automation. (2022, July 19). *Product Notification 2022-01-001 - Rockwell Automation products unable to establish proper DCOM connection after installing Microsoft DCOM Hardening patch (CVE-2021-26414)* . Retrieved from Rockwell Automation Web site: https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1133982

Rockwell Automation. (2022, June 20). *Rockwell Automation Product Patches for Microsoft DCOM Hardening (CVE-2021-26414) TOC* . Retrieved from Rockwell Automation Web site: https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1134041/~/rockwell-automation-product-patches-for-microsoft-dcom-hardening

Siemens. (2022, February 16). *Which Microsoft patches are recommended for operating SIMATIC WinCC V7 ("Security Updates", "Critical Updates" and "Definition Updates")?* Retrieved from Industry online support - Product support: https://support.industry.siemens.com/cs/document/18752994/which-microsoft-patches-are-recommended-for-operating-simatic-wincc-v7-(-security-updates-critical-updates-and-definition-updates-)-?dti=0&lc=en-US