

# SICK PSIRT Security Advisory

## Microsoft vulnerability affects multiple SICK IPCs with SICK MEAC

Document ID: SCA-2022-0004  
Publication Date: 2022-04-11  
CVSSv3 Base Score: 4.8  
CVSSv3 Vector String: CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:N/I:H/A:N  
CVE Identifier: CVE-2021-26414  
Version: V1.0

### SUMMARY

The CVE-2021-26414 “Windows DCOM Server Security Feature Bypass” was issued by Microsoft, that may affect the functionality of the SICK MEAC software installed on SICK IPCs.

**Interpretation:** The vulnerability allows a remote attacker to bypass the Windows DCOM Server authentication process.

**Limitation:** The vulnerability can only be exploited if a user operates on a CVE-2021-26414 affected Windows version and tries to access a malicious server, hosted by an attacker. The attacker would have to host a specially crafted server share or website. It is not possible for an attacker to force the user to visit this specially crafted server share or website. Only by convincing them, typically by way of an enticement in an email or chat message, an exploitation is possible.

### AFFECTED PRODUCTS

MEAC modules potentially affected by activating the patch for this vulnerability include:

Product / Part number	Version	Remediation available
OPC Client / 1614631	all versions	Yes
OPC Server / 1614636	all versions	Yes

Operators may update Windows operating system on which MEAC runs at their own discretion. MEAC operators should therefore check for installation of any of the following Windows version:

Windows Version	Patch Version	Remediation available
Windows 7	for 32-bit Systems Service Pack 1, for x64-based Systems Service Pack 1	Yes
Windows 8.1	for 32-bit systems, for x64-based systems	Yes
Windows 10	20H2, 21H1, 1607, 1809, 1909, 2004 for 32-bit Systems, ARM64-based Systems, x64-based Systems	Yes
Windows RT 8.1		Yes
Windows Server 2008	R2 for x64-based Systems Service Pack 1, R2 for x64-based Systems Service Pack 1	Yes

	(Server Core installation), for 32-bit Systems Service Pack 2, for 32-bit Systems Service Pack 2 (Server Core installation), for x64-based Systems Service Pack 2, for x64-based Systems Service Pack 2 (Server Core installation)	
Windows Server 2012	(GUI), (Server Core installation), R2, R2 (Server Core installation)	Yes
Windows Server 2016	(GUI), (Server Core installation)	Yes
Windows Server 2019	(GUI), (Server Core installation)	Yes
Windows Server	20H2 (Server Core Installation)	Yes
Windows Server	2004 (Server Core installation)	Yes

## SOLUTION

Microsoft is addressing this vulnerability in a phased rollout of Windows security updates. Under the current schedule, the hardening changes can be disabled until March 14, 2023:

Update release	Behavior change
June 8, 2021	Hardening changes <b>disabled by default</b> but with the ability to enable them using a registry key.
June 14, 2022	Hardening changes <b>enabled by default</b> but with the ability to disable them using a registry key.
March 14, 2023	Hardening changes <b>enabled by default with no ability to disable them.</b> By this point, you must resolve any compatibility issues with the hardening changes and applications in your environment.

Prior to the March 2023 release, the hardening change will be disabled if the registry key "HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Ole\AppCompat\RequireIntegrityActivationAuthenticationLevel" is undefined or 0, and enabled, if set to 1. A reboot is required after making any changes to the registry key.

**Recommended measures:** Given the moderate risk (a user having to deliberately access a malicious server), SICK recommends deactivating the hardening by using the above registry key, until it has been confirmed that the hardening does not adversely affect the MEAC functionality. SICK will then inform customers in an updated version of this security advisory.

In a subset of Windows versions with release dates newer than between August 2021 and October 2021, depending on the Windows version, customers can identify vulnerable installations by checking the Windows event log for messages.

## General Security Practices

As general security measures, SICK recommends to minimize network exposure of the devices, restrict network access and follow recommended security practices in order to run the devices in a protected IT environment.

Additional information on Industrial Security can be found at:  
<http://ics-cert.us-cert.gov/content/recommended-practices>

## VULNERABILITY CLASSIFICATION

---

SICK performs vulnerability classification by using the CVSS scoring system (CVSS v3.1). The environmental score is dependent on the customer's environment and can affect the overall CVSS score. SICK recommends that customers individually evaluate the environmental score to achieve final scoring.

## RESOURCES

---

SICK PSIRT Security Advisories

<https://sick.com/psirt>

SICK Operating Guidelines

[https://cdn.sick.com/media/docs/1/11/411/Special\\_information\\_CYBERSECURITY\\_BY\\_SICK\\_en\\_IMO084411.PDF](https://cdn.sick.com/media/docs/1/11/411/Special_information_CYBERSECURITY_BY_SICK_en_IMO084411.PDF)

Microsoft, CVE-2021-26414 "Windows DCOM Server Security Feature Bypass"

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26414>

Bypass of the Windows DCOM Server authentication process by CVE-2021-2614

<https://www.cybersecurity-help.cz/vdb/SB2021060835>

Track DCOM error events

<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>

## HISTORY

---

Version	Release Date	Comment
V1.0	2022-04-11	Initial Release