Sensor Intelligence.

TLP:WHITE

SICK PSIRT
Security Advisory

CodeMeter vulnerablity affects SICK CODE-LOC and SICK LIDAR-LOC

Document ID:	SCA-2025-0014
Publication Date:	2025-11-03
CVE Identifier:	CVE-2025-47809
CVSSv3 Base Score:	7.7
CVSSv3 Vector String:	CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:H
Version:	1

Summary

A vulnerability in the CodeMeter runtime affects the SICK products SICK CODE-LOC and SICK LIDAR-LOC. This could potentially affect the integrity, confidentiality and availability of the products. Only systems running on Microsoft Windows are affected. Furthermore, the systems are only affected when running the installation and keeping the Control Center component open. As soon as the system has been restarted, it is no longer affected by the vulnerability. Nevertheless, SICK strongly recommends to upgrade to the latest version of the products to mitigate the risk. Currently, SICK is not aware of any public exploits.

List of Products

Product	Affected by
SICK CODE-LOC with Firmware <LLS-2.8.1.24092R	CVE-2025-47809 Status: Known Affected Remediation: Vendor fix
SICK LIDAR-LOC with Firmware <LLS-2.8.1.24092R	CVE-2025-47809 Status: Known Affected Remediation: Vendor fix

SICK
Sensor Intelligence.

TLP:WHITE

Vulnerability Overview

CVE-2025-47809 Improper Privilege Management

Summary: Wibu CodeMeter before 8.30a sometimes allows privilege escalation immediately after installation (before a logoff or reboot). For exploitation, there must have been an unprivileged installation with UAC, and the CodeMeter Control Center component must be installed, and the CodeMeter Control Center component must not have been restarted. In this scenario, the local user can navigate from Import License to a privileged instance of Windows Explorer.

CVE-2025-47809 has been assigned to this vulnerability.
CVSSv3.1 base score: 7.7
CVSSv3.1 vector string: CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:H
CWE identifier: CWE-269 (Improper Privilege Management)

Remediations

Vendor Fix for CVE-2025-47809

Details: On Microsoft Windows systems, it is strongly recommended to upgrade to the latest version (LLS-2.8.1.24092R).

Valid for:

- SICK CODE-LOC with Firmware <LLS-2.8.1.24092R
- SICK LIDAR-LOC with Firmware <LLS-2.8.1.24092R

General Security Practices

General Security Measures

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.

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://www.sick.com/media/docs/9/19/719/special_information_sick_operating_guidelines_cybersecurity_by_sick_en_im0106719.pdf

ICS-CERT recommended practices on Industrial Security:
https://www.cisa.gov/resources-tools/resources/ics-recommended-practices

CVSS v3.1 Calculator:
https://www.first.org/cvss/calculator/3.1

History

Version	Release Date	Comment
1	2025-11-03	Initial version