SICK
Sensor Intelligence.

TLP:WHITE

SICK PSIRT
Security Advisory

Vulnerability in SICK OLM

Document ID:	SCA-2024-0007
Publication Date:	2024-12-31
CVE Identifier:	N/A (CWE-200)
CVSSv3 Base Score:	8.8
CVSSv3 Vector String:	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Version:	3

Summary

SICK received a report about a vulnerability in the SICK Support Portal supportportal.sick.com, which was hosted and operated by a third-party service provider. Due to a misconfiguration, the access restriction of a NFS (Network File System) storage system has failed, which resulted in temporary unauthorized access to the file share. SICK initiated remediating measures immediately after becoming aware of the security incident. SICK requested all available log data and carried out a comprehensive analysis. The SICK incident response team analysed the data and found product related files that could enable an attacker to potentially impact the availabilty, integrity and confidentiality of the affected products. To reduce the risk to our customers, SICK provided mitigations for the affected products.
It is highly recommended to upgrade the affected products to the latest release or implement the suggested workarounds.

List of Products

Product	Affected by
SICK OLM all Firmware versions	Exposure of Sensitive Information to an Unauthorized Actor Status: Known Affected Remediation: Workaround

SICK
Sensor Intelligence.

TLP:WHITE

Vulnerability Overview

Exposure of Sensitive Information to an Unauthorized Actor

Summary: Due to a misconfiguration in the SICK Support Portal supportportal.sick.com, the access restriction of a NFS (Network File System) storage system has failed, which resulted in temporary unauthorized access to the file share. The service password of the SICK OLM got leaked, that could enable an attacker to potentially impact the availabilty, integrity and confidentiality.

No CVE has been assigned to this vulnerability.
CVSSv3.1 base score: 8.8
CVSSv3.1 vector string: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CWE identifier: CWE-200 (Exposure of Sensitive Information to an Unauthorized Actor)

Remediations

Workaround for Exposure of Sensitive Information to an Unauthorized Actor

Details: The password of the OLM is not changeable. Please make sure that you apply general security practices when operating the products. The following General Security Practices and Operating Guidelines could mitigate the associated security risk.

Valid for:

- SICK OLM all Firmware versions

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	2024-12-31	Initial version
2	2025-01-02	Updated titel and description.
3	2025-07-30	Updated Advisory: URL for SICK Operating Guidelines has been updated