SICK PSIRT
Security Advisory

Critical vulnerability in multiple SICK products

Document ID:	sca-2024-0003
Publication Date:	2024-10-17
CVE Identifier:	CVE-2024-10025
CVSSv3 Base Score:	9.1
CVSSv3 Vector String:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H
Version:	1

Summary

A critical vulnerability has been discovered in the .sdd files of several SICK products. This vulnerability could allow a remote, unauthenticated attacker to gain access to the ”Authorized Client” user role, potentially impacting the availability and integrity of the affected SICK products. Users are strongly urged to change their default passwords immediately.

List of Products

Product	Affected by
SICK CLV6xx all Firmware versions	CVE-2024-10025 Status: Known Affected Remediation: Vendor fix
SICK Lector6xx all Firmware versions	CVE-2024-10025 Status: Known Affected Remediation: Vendor fix
SICK RFx6xx all Firmware versions	CVE-2024-10025 Status: Known Affected Remediation: Vendor fix

Vulnerability Overview

CVE-2024-10025 Use of Hard-coded Credentials

Summary: A vulnerability in the .sdd file allows an attacker to read default passwords stored in plain text within the code. By exploiting these plaintext credentials, an attacker can log into affected SICK products as an “Authorized Client” if the customer has not changed the default password.

CVE-2024-10025 has been assigned to this vulnerability.
CVSSv3.1 base score: 9.1
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H
CWE identifier: CWE-798 (Use of Hard-coded Credentials)

Remediations

Vendor Fix for CVE-2024-10025

Details: Customers are strongly advised to change their default passwords.

Valid for:

- SICK CLV6xx all Firmware versions
- SICK Lector6xx all Firmware versions
- SICK RFx6xx 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://cdn.sick.com/media/docs/1/11/411/Special_information_CYBERSECURITY_BY_SICK_en_IM0084411.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	2024-10-17	Initial version