SICK PSIRT
Security Advisory

Vulnerability in SICK Overall Equipment Effectiveness (OEE)

Document ID:	SCA-2022-0005
Publication Date:	2022-04-11
CVE Identifier:	CVE-2022-27578
CVSSv3 Base Score:	8.4
CVSSv3 Vector String:	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N
Version:	2

Summary

SICK received a report about a vulnerability in the SICK Overall Equipment Effectiveness (OEE). The services under the OEE application are started in the context of system privileges.
An attacker can perform a privilege escalation if the application is installed in a directory, where non authenticated or low privilege users can modify the content of the OEE application.
SICK recommends implementing the mitigations below.

List of Products

Product	Part Number	Affected by
SICK Overall Equipment Effectiveness (OEE) 0.5.1	1613866	CVE-2022-27578 Status: Fixed Remediation: Vendor fix

Vulnerability Overview

CVE-2022-27578 Execution with Unnecessary Privileges

CVE Description: An attacker can perform a privilege escalation through the SICK OEE if the application is installed in a directory where non authenticated or low privilege users can modify its content.

CVE-2022-27578 has been assigned to this vulnerability.
CVSSv3.1 base score: 8.4
CVSSv3.1 vector string: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N
CWE identifier: CWE-250 (Execution with Unnecessary Privileges)

References:
CVE Entry:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27578

Remediations

Vendor Fix for CVE-2022-27578

Details: SICK recommends installing the application in a directory, that is only modifiable by system or administrator users. The default installation path of the SICK OEE application is %ProgramFiles% [i.e. “C:\Program Files” or “C:\Programme” depending on the installation language], which is by default only modifiable by system or administrator users.

Valid for:

- SICK Overall Equipment Effectiveness (OEE) 0.5.1

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:
http://ics-cert.us-cert.gov/content/recommended-practices

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

History

Version	Release Date	Comment
1	2022-04-11	Initial Release
2	2023-02-10	Updated Advisory (only visual changes)