TLP:WHITE

SICK PSIRT
Security Advisory

Vulnerability in SICK MSC800

Document ID:	SCA-2022-0006
Publication Date:	2022-04-11
CVE Identifier:	CVE-2022-27577
CVSSv3 Base Score:	5.4
CVSSv3 Vector String:	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N
Version:	3

Summary

SICK received a report about a vulnerability in the SICK MSC800. An attacker could compromise services on the MSC800 by a TCP sequence prediction attack if a vulnerable version is used.

List of Products

Product	Part Number	Affected by
SICK MSC800 with Firmware <4.15	1040571	CVE-2022-27577 Status: Known Affected Remediation: Vendor fix

SICK
Sensor Intelligence.

TLP:WHITE

Vulnerability Overview

CVE-2022-27577 Predictable Exact Value from Previous Values

CVE Description: The vulnerability in the MSC800 in all versions before 4.15 allows for an attacker to predict the TCP initial sequence number. When the TCP sequence is predictable, an attacker can send packets that are forged to appear to come from a trusted computer. These forged packets could compromise services on the MSC800.
SICK has released a new firmware version of the SICK MSC800 and recommends updating to the newest version.

CVE-2022-27577 has been assigned to this vulnerability.
CVSSv3.1 base score: 5.4
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N
CWE identifier: CWE-342 (Predictable Exact Value from Previous Values)

References:
CVE Entry:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27577

Remediations

Vendor Fix for CVE-2022-27577

Details: SICK has released a new firmware version of the SICK MSC800 and recommends updating to the newest version.

Valid for:

- SICK MSC800 with Firmware $<$4.15

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

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

Additional Product Information

SICK MSC800 with Firmware <4.15	Product on sick.com: https://www.sick.com/de/de/p/p354746

History

Version	Release Date	Comment
1	2022-04-11	Initial Release
2	2023-02-10	Updated Advisory (only visual changes)
3	2025-07-30	Updated Advisory: URL for SICK Operating Guidelines has been updated