TLP:WHITE

SICK PSIRT
Security Advisory

Vulnerability in SICK MSC800

Document ID:	SCA-2022-0006
Publication Date:	2022-04-11
CVSSv3 Base Score:	5.4
CVSS Vector String:	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N
CVE Identifier:	CVE-2022-27577
Version:	V1.0

SUMMARY

SICK received a report about a vulnerability in the SICK MSC800.

The vulnerability 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.

AFFECTED PRODUCTS

Product	Firmware Version	Remediation available
SICK MSC800	All versions prior to 4.15	Yes

VULNERABILITY OVERVIEW

CVE-2022-27577 Predictable Exact Value from Previous Values
An attacker could compromise services on the MSC800 by a TCP sequence prediction attack if a vulnerable version of the SICK MSC800 is used.

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

General Security Practices

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.

Additional information on Industrial Security can be found at:
http://ics-cert.us-cert.gov/content/recommended-practices

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

HISTORY

Version	Release Date	Comment
V1.0	2022-04-11	Initial Release