TLP:WHITE

SICK PSIRT
Security Advisory

Vulnerability in SICK MSC800

Document ID:	sca-2024-0002
Publication Date:	2024-09-11
CVE Identifier:	CVE-2024-8751
CVSSv3 Base Score:	7.5
CVSSv3 Vector String:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Version:	1

Summary

SICK found a security vulnerability in the SICK MSC800. This vulnerability allows an unauthenticated attacker to modify the IP address of the product through the SopasET interface, potentially leading to Denial of Service. Currently SICK is not aware of any public exploits specifically targeting the vulnerability. SICK has released a new version of the SICK MSC800 firmware and recommends updating to the newest version.

List of Products

Product	Affected by
SICK MSC800 <=S2.93.19	CVE-2024-8751 Status: Fixed Remediation: Vendor fix
SICK MSC800 <=V4.25	CVE-2024-8751 Status: Fixed Remediation: Vendor fix

SICK
Sensor Intelligence.

TLP:WHITE

Vulnerability Overview

CVE-2024-8751 Missing Authentication for Critical Function

Summary: A vulnerability in the MSC800 allows an unauthenticated attacker to modify the product's IP address over Sopas ET. This can lead to Denial of Service. Users are recommended to upgrade both MSC800 and MSC800 LFT to version V4.26 and S2.93.20 respectively which fixes this issue.

CVE-2024-8751 has been assigned to this vulnerability.
CVSSv3.1 base score: 7.5
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CWE identifier: CWE-306 (Missing Authentication for Critical Function)

Remediations

Vendor Fix for CVE-2024-8751

Details: Customers who use the version <=V4.25 are strongly recommended to upgrade to the latest release V4.26

Valid for:

- SICK MSC800 <=V4.25

Details: Customers who use the version <=S2.93.19 are strongly recommended to upgrade to the latest release S2.93.20.

Valid for:

- SICK MSC800 <=S2.93.19

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	2024-09-11	Initial version