TLP:WHITE

SICK PSIRT
Security Advisory

Vulnerabilities in SICK Flexi Compact

Document ID:	SCA-2025-0005
Publication Date:	2025-04-28
CVE Identifiers:	CVE-2025-32470, CVE-2025-32471
Version:	2

Summary

SICK has found two vulnerabilities that affect the SICK Flexi Compact. The vulnerabilities may affect the availability and confidentiality of the products. SICK is currently not aware of any public exploits.

List of Products

Product	Affected by
SICK FLX0-GPNT100 all firmware versions	CVE-2025-32470 Status: Known Affected Remediation: Workaround
SICK FLX3-CPUC200 all firmware versions	CVE-2025-32470 Status: Known Affected Remediation: Workaround
	CVE-2025-32471 Status: Known Affected Remediation: -

Vulnerability Overview

CVE-2025-32470 Improper Access Control

Summary: A remote unauthenticated attacker may be able to change the IP adress of the device, and therefore affecting the availability of the device.

CVE-2025-32470 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-284 (Improper Access Control)

CVE-2025-32471 Use of Weak Credentials

Summary: The device's passwords have not been adequately salted, making them vulnerable to password extraction attacks.

CVE-2025-32471 has been assigned to this vulnerability.
CVSSv3.1 base score: 3.7
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N
CWE identifier: CWE-1391 (Use of Weak Credentials)

Remediations

Workaround for CVE-2025-32470

Details: Please make sure that only trusted entities have access to the device. Furthermore, you should apply the following General Security Measures when operating the product to mitigate the associated security risk. The collected resources "SICK Operating Guidelines" and "ICS-CERT recommended practices on Industrial Security" could help to implement the general security practices.

Valid for:

- SICK FLX0-GPNT100 all firmware versions
- SICK FLX3-CPUC200 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://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:
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	2025-04-28	Initial version
2	2025-07-30	Updated Advisory: URL for SICK Operating Guidelines has been updated