Sensor Intelligence.

TLP:WHITE

SICK PSIRT
Security Advisory

Sudo vulnerability affects SICK SID products

Document ID:	SCA-2025-0012
Publication Date:	2025-10-27
CVE Identifier:	CVE-2025-32463
CVSSv3 Base Score:	9.3
CVSSv3 Vector String:	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
Version:	1

Summary

SICK SID products are affected by the sudo vulnerability CVE-2025-32463. SICK strongly recommends to update to the latest version to mitigate the risk.

List of Products

Product	Affected by
SICK SID121 LFT with Firmware <4.2.7	CVE-2025-32463 Status: Known Affected Remediation: Vendor fix
SICK SID121 with Firmware <4.2.7	CVE-2025-32463 Status: Known Affected Remediation: Vendor fix
SICK SID71 LFT with Firmware <4.2.7	CVE-2025-32463 Status: Known Affected Remediation: Vendor fix
SICK SID71 with Firmware <4.2.7	CVE-2025-32463 Status: Known Affected Remediation: Vendor fix

SICK
Sensor Intelligence.

TLP:WHITE

Vulnerability Overview

CVE-2025-32463 Inclusion of Functionality from Untrusted Control Sphere

Summary: Sudo before 1.9.17p1 allows local users to obtain root access because /etc/nsswitch.conf from a user-controlled directory is used with the --chroot option.

CVE-2025-32463 has been assigned to this vulnerability.
CVSSv3.1 base score: 9.3
CVSSv3.1 vector string: CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
CWE identifier: CWE-829 (Inclusion of Functionality from Untrusted Control Sphere)

Remediations

Vendor Fix for CVE-2025-32463

Details: It is strongly recommended to upgrade to the latest version (4.2.7)

Valid for:

- SICK SID121 LFT with Firmware <4.2.7
- SICK SID121 with Firmware <4.2.7
- SICK SID71 LFT with Firmware <4.2.7
- SICK SID71 with Firmware <4.2.7

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	2025-10-27	Initial version