SICK Sensor Intelligence

TLP:WHITE

SICK PSIRT Security Advisory

Vulnerability Affecting sick_scan_xd Driver

Document ID: sca-2026-0018

Publication Date: 2026-11-18

CVE Identifier: CVE-2026-123123

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

Version: 1

Summary

An integer overflow vulnerability exists in the open-source repository sick_scan_xd (https://github.com/SICKAG/sick_scan_xd), a ROS 2 driver library and software development kit for SICK LiDAR and RADAR devices. A specially crafted network packet could cause an integer overflow during packet size validation, potentially bypassing boundary checks and resulting in out-of-bounds reads. If exploited, this vulnerability could affect the availability of applications using the affected library. SICK recommends applying the defined remediation for this vulnerability.

If exploited, the vulnerability could potentially allow an unauthenticated attacker to compromise the availability of the product.

As general security measures, SICK recommends minimizing network exposure of the devices, restricting network access, and following recommended security practices in order to operate the devices in a protected IT environment.

SICK recommends ensuring that the product operates within a secure environment.

List of Products

Product	Details
SICK sick_scan_xd < 3.10.0	Status: Known Affected Remediation: Vendor Fix CVE IDs: CVE-2026-123123

Vulnerability Overview

CVE-2026-123123 Integer Overflow or Wraparound

Summary: An attacker that is able to send a crafted network packet to the affected component may trigger an integer overflow during module size validation. This may cause insufficient bounds checking and result in out-of-bounds memory reads, potentially leading to a denial of service condition due to process termination.

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-190 (Integer Overflow or Wraparound)

Remediations:

Product	Details
SICK sick_scan_xd < 3.10.0	Vendor Fix Users are recommended to upgrade to version 3.10.0.

Resources

SICK PSIRT Security Advisories:
https://www.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

The canonical URL:
https://www.sick.com/.well-known/csaf/white/2026/sca-2026-0018.json

Affected Repository:
https://github.com/SICKAG/sick_scan_xd

Acknowledgments

Thanks to kta1kri for reporting this issue in a coordinated manner (URL: https://github.com/kta1kri).

History

Version	Release Date	Comment
1	2026-11-18	Initial version