

# SICK PSIRT Security Advisory

## Vulnerability Affecting Sick\_Safetyscanners\_Base CPP Driver

Document ID: sca-2026-0015

Publication Date: 2026-10-15

CVE Identifier: CVE-2026-101290

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 out-of-bounds read vulnerability exists in the open-source repository sick\_safetyscanners\_base ([https://github.com/SICKAG/sick\\_safetyscanners\\_base](https://github.com/SICKAG/sick_safetyscanners_base)), a standalone C++ driver library for SICK safety laser scanners. A specially crafted network packet could cause the library to read data beyond the bounds of the received buffer. If exploited, this vulnerability could potentially affect the availability of applications using the affected library. SICK recommends applying the defined remediations for this vulnerability.

### List of Products

| Product                                      | Details                                                                                            |
|----------------------------------------------|----------------------------------------------------------------------------------------------------|
| Sick_Safetyscanners_Base CPP Driver <= 1.0.4 | <u>Status:</u> Known Affected<br><u>Remediation:</u> Vendor Fix<br><u>CVE IDs:</u> CVE-2026-101290 |

### Vulnerability Overview

#### CVE-2026-101290 Out-of-bounds Read

**Summary:** A remote attacker may send a specially crafted network packet that causes the affected application to perform an out-of-bounds memory read due to insufficient validation of packet length. This may result in an application crash and a denial-of-service condition.

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-125 (Out-of-bounds Read)

**Remediations:**

| Product                                         | Details                                                                 |
|-------------------------------------------------|-------------------------------------------------------------------------|
| Sick_Safetyscanners_Base CPP<br>Driver <= 1.0.4 | <u>Vendor Fix</u><br>Users are recommended to upgrade to version 1.0.5. |

## General Security Practices

---

### General Security Measures

---

As general security measures, SICK recommends minimizing network exposure of the devices, restricting network access and following 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://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](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-2026-0015.json>

Affected Repository:

[https://github.com/SICKAG/sick\\_safetyscanners\\_base](https://github.com/SICKAG/sick_safetyscanners_base)

## Acknowledgments

---

Thanks to kta1kri for reporting this issue in a coordinated manner (URL:

<https://github.com/kta1kri>).

## History

---

| Version | Release Date | Comment         |
|---------|--------------|-----------------|
| 1       | 2026-10-15   | Initial version |