

SICK PSIRT Security Advisory

Vulnerabilities affecting SICK TLOC100-100

Document ID: SCA-2025-0013
Publication Date: 2025-11-11
CVE Identifiers: N/A (CWE-1104), CVE-2025-59459, CVE-2025-59460, CVE-2025-59461, CVE-2025-59462, CVE-2025-59463
Version: 2

Summary

SICK has identified multiple vulnerabilities in the SICK TLOC100-100 product. The vulnerabilities could potentially affect the confidentiality, integrity and availability of the product. Therefore it is strongly recommended to apply general security practices when operating the product. SICK is currently not aware of any public exploits.

List of Products

Product	Part Number	Affected by
SICK TLOC100-100 all Firmware versions	6087307	<u>Use of Unmaintained Third Party Components</u> Status: Known Affected Remediation: Mitigation
		<u>CVE-2025-59461</u> Status: Known Affected Remediation: Mitigation
		<u>CVE-2025-59462</u> Status: Known Affected Remediation: Mitigation

		CVE-2025-59463 Status: Known Affected Remediation: Mitigation
SICK TLOC100-100 with Firmware <7.1.1	6087307	CVE-2025-59459 Status: Known Affected Remediation: Vendor fix
		CVE-2025-59460 Status: Known Affected Remediation: Vendor fix

Vulnerability Overview

Use of Unmaintained Third Party Components

Summary: The device is running an outdated operating system, which may be susceptible to known vulnerabilities.

No CVE 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-1104 (Use of Unmaintained Third Party Components)

CVE-2025-59459 Allocation of Resources Without Limits or Throttling

Summary: An attacker that gains SSH access to an unprivileged account may be able to disrupt services (including SSH), causing persistent loss of availability.

CVE-2025-59459 has been assigned to this vulnerability.

CVSSv3.1 base score: 5.5

CVSSv3.1 vector string: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

CWE identifier: CWE-770 (Allocation of Resources Without Limits or Throttling)

CVE-2025-59460 Use of Weak Credentials

Summary: The system is deployed in its default state, with configuration settings that do not comply with the latest best practices for restricting access. This increases the risk of unauthorised connections.

CVE-2025-59460 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:H/I:N/A:N

CWE identifier: CWE-1391 (Use of Weak Credentials)

CVE-2025-59461 Missing Authorization

Summary: A remote unauthenticated attacker may use the unauthenticated C++ API to access or modify sensitive data and disrupt services.

CVE-2025-59461 has been assigned to this vulnerability.

CVSSv3.1 base score: 7.6

CVSSv3.1 vector string: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H

CWE identifier: CWE-862 (Missing Authorization)

CVE-2025-59462 Uncaught Exception

Summary: An attacker who tampers with the C++ CLI client may crash the UpdateService during file transfers, disrupting updates and availability.

CVE-2025-59462 has been assigned to this vulnerability.

CVSSv3.1 base score: 6.5

CVSSv3.1 vector string: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CWE identifier: CWE-248 (Uncaught Exception)

CVE-2025-59463 Deadlock

Summary: An attacker may cause chunk-size mismatches that block file transfers and prevent subsequent transfers.

CVE-2025-59463 has been assigned to this vulnerability.

CVSSv3.1 base score: 4.3

CVSSv3.1 vector string: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

CWE identifier: CWE-833 (Deadlock)

Remediations

Mitigation for Use of Unmaintained Third Party Components

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 TLOC100-100 all Firmware versions

Vendor Fix for CVE-2025-59459

Details: Users are strongly recommended to upgrade to the latest release of TLOC100-100 ($\geq 7.1.1$).

Valid for:

- SICK TLOC100-100 with Firmware $< 7.1.1$

Vendor Fix for CVE-2025-59460

Details: Users are strongly recommended to upgrade to the latest release of TLOC100-100 ($\geq 7.1.1$).

Valid for:

- SICK TLOC100-100 with Firmware $< 7.1.1$

Mitigation for CVE-2025-59461

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 TLOC100-100 all Firmware versions

Mitigation for CVE-2025-59462

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 TLOC100-100 all Firmware versions

Mitigation for CVE-2025-59463

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 TLOC100-100 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	2025-10-27	Initial version
2	2025-11-11	Removed CVE ID