TLP:WHITE

SICK PSIRT
Security Advisory

Critical vulnerabilities in SICK DL100-2xxxxxxx

Document ID:	SCA-2025-0004
Publication Date:	2025-03-14
CVE Identifiers:	CVE-2025-27593, CVE-2025-27594, CVE-2025-27595
Version:	2

Summary

Critical vulnerabilities have been found in the SICK device DL100-2xxxxxxx. If exploited, this potentially allows an attacker to impact availabiltiy, integrity and confidentaility of the products. Currently, SICK is not aware of any public exploits specifically targeting these vulnerabilities. As a mitigation, SICK strongly recommends operating the system within a secure infrastructure to minimize risk.

List of Products

Product	Part Number	Affected by

SICK DL100-2xxxxxxx all firmware versions	1052684 1052685 1052686 1052687 1052688 1052689 1052690 1052691 1052692 1052693 1052694 1052695 1052696 1052697 1052698 1052699 1052700 1052701 1058164 1058165 1058166 1058167 1058168 1058169 1060386 1060387 1060388 1060389 1060390 1060391 1060948 1060949 1060950 1060951 1060952 1060953 1064835 1066423 1066425 1066426 1066427 1066428 1066429 1066438 1086984 1086985 1086986 1086987 1086988 1092652 1095769 1095770 1095771 1095772 1096493	CVE-2025-27593 Status: Known Affected Remediation: Workaround

		CVE-2025-27594 Status: Known Affected Remediation: Workaround
		CVE-2025-27595 Status: Known Affected Remediation: Workaround

Vulnerability Overview

CVE-2025-27593 Download of Code Without Integrity Check

Summary: The product can be used to distribute malicious code using SDD Device Drivers due to missing download verification checks, leading to code execution on target systems.

CVE-2025-27593 has been assigned to this vulnerability.
CVSSv3.1 base score: 9.3
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:N
CWE identifier: CWE-494 (Download of Code Without Integrity Check)

CVE-2025-27594 Cleartext Transmission of Sensitive Information

Summary: The device uses an unencrypted, proprietary protocol for communication. Through this protocol, configuration data is transmitted and device authentication is performed. An attacker can thereby intercept the authentication hash and use it to log into the device using a pass-the-hash attack.

CVE-2025-27594 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-319 (Cleartext Transmission of Sensitive Information)

CVE-2025-27595 Use of Weak Hash

Summary: The device uses a weak hashing alghorithm to create the password hash. Hence, a matching password can be easily calculated by an attacker. This impacts the security and the integrity of the device.

CVE-2025-27595 has been assigned to this vulnerability.
CVSSv3.1 base score: 9.8
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CWE identifier: CWE-328 (Use of Weak Hash)

Remediations

Workaround for CVE-2025-27593

Details: Please make sure that you apply general security practices when operating the products. The following General Security Practices and Operating Guidelines could mitigate the associated security risk.

Valid for:

- SICK DL100-2xxxxxxx all firmware versions

Workaround for CVE-2025-27594

Details: Please make sure that you apply general security practices when operating the products. The following General Security Practices and Operating Guidelines could mitigate the associated security risk.

Valid for:

- SICK DL100-2xxxxxxx all firmware versions

Workaround for CVE-2025-27595

Details: Please make sure that you apply general security practices when operating the products. The following General Security Practices and Operating Guidelines could mitigate the associated security risk.

Valid for:

- SICK DL100-2xxxxxxx 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

Security Advisory of Deutsche Telekom Security GmbH:
https://github.security.telekom.com/2025/03/multiple-vulnerabilities-in-sick-dl100.html

Acknowledgments

Thanks to Leonard Lewedei from Deutsche Telekom Security GmbH for executing penetration testing and reporting the vulnerabilities.

History

Version	Release Date	Comment
1	2025-03-14	Initial version
2	2025-07-30	Updated Advisory: URL for SICK Operating Guidelines has been updated