TLP:WHITE

SICK PSIRT
Security Advisory

Vulnerabilities affecting SICK LMS1000 and SICK MRS1000

Document ID:	SCA-2026-0005
Publication Date:	2026-02-27
CVE Identifiers:	CVE-2026-1626, CVE-2026-1627
Version:	1

Summary

Two vulnerabilities affect the SICK LMS1000 and SICK MRS1000 product families. The vulnerabilities allow the use of weak cryptographic configurations in the SSH service, which may enable an attacker with network access to observe, manipulate, or compromise the integrity of SSH communications. SICK recommends applying the defined remediations for both vulnerabilities.

List of Products

Product	Part Number	Affected by
SICK LMS1000 with firmware <=2.4.0	1092445	CVE-2026-1626 Status: Known Affected Remediation: Vendor fix
		CVE-2026-1627 Status: Known Affected Remediation: Vendor fix
SICK MRS1000 with firmware <=2.4.0	1075367 1081208 1112242 1131433 1106288 1104278	CVE-2026-1626 Status: Known Affected Remediation: Vendor fix

		CVE-2026-1627 Status: Known Affected Remediation: Vendor fix

Vulnerability Overview

CVE-2026-1626 Use of a Broken or Risky Cryptographic Algorithm

Summary: An attacker may exploit the use of weak CBC-based cipher suites in the device's SSH service to potentially observe or manipulate parts of the encrypted SSH communication, if they are able to intercept or interact with the network traffic.

CVE-2026-1626 has been assigned to this vulnerability.
CVSSv3.1 base score: 6.5
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N
CWE identifier: CWE-327 (Use of a Broken or Risky Cryptographic Algorithm)

CVE-2026-1627 Use of a Broken or Risky Cryptographic Algorithm

Summary: An attacker may exploit the use of outdated and weak MAC algorithms in the device's SSH service to potentially compromise the integrity of the SSH session, allowing manipulation of transmitted data if the attacker can interact with the network traffic.

CVE-2026-1627 has been assigned to this vulnerability.
CVSSv3.1 base score: 6.5
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N
CWE identifier: CWE-327 (Use of a Broken or Risky Cryptographic Algorithm)

Remediations

Vendor Fix for CVE-2026-1626

Details: Users are strongly recommended to upgrade to release version 2.4.1.

Valid for:

- SICK LMS1000 with firmware <=2.4.0
- SICK MRS1000 with firmware <=2.4.0

Vendor Fix for CVE-2026-1627

Details: Users are strongly recommended to upgrade to release version 2.4.1.

Valid for:

- SICK LMS1000 with firmware <=2.4.0
- SICK MRS1000 with firmware <=2.4.0

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

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	2026-02-27	Initial version