TLP:WHITE

SICK PSIRT
Security Advisory

Vulnerabilities affecting SICK Lector85x and SICK Lector83x

Document ID:	SCA-2026-0006
Publication Date:	2026-03-06
CVE Identifiers:	CVE-2026-2330, CVE-2026-2331
Version:	1

Summary

Two vulnerabilities affecting the SICK Lector85x and SICK Lector83x product families have been identified. Both vulnerabilities are caused by insufficient access restrictions in HTTP-based interfaces, which may allow unauthenticated access to sensitive device resources. Depending on the configuration, this could lead to unauthorized modification of device settings and security-relevant data. SICK recommends applying the defined remediations for both vulnerabilities. SICK is currently not aware of any public exploits.

List of Products

Product	Affected by
SICK Lector83x with firmware <2.8.0	CVE-2026-2330 Status: Known Affected Remediation: Vendor fix
SICK Lector83x with firmware >= 2.6.0 <= 2.7.0	CVE-2026-2331 Status: Known Affected Remediation: Vendor fix
SICK Lector85x with firmware <2.8.0	CVE-2026-2330 Status: Known Affected Remediation: Vendor fix

SICK
Sensor Intelligence.

TLP:WHITE

SICK Lector85x with firmware >= 2.6.0 <= 2.7.0	CVE-2026-2331 Status: Known Affected Remediation: Vendor fix

Vulnerability Overview

CVE-2026-2330 Files or Directories Accessible to External Parties

Summary: An attacker may access restricted filesystem areas on the device via the CROWN REST interface due to incomplete whitelist enforcement. Certain directories intended for internal testing were not covered by the whitelist and are accessible without authentication. An unauthenticated attacker could place a manipulated parameter file that becomes active after a reboot, allowing modification of critical device settings, including network configuration and application parameters.

CVE-2026-2330 has been assigned to this vulnerability.
CVSSv3.1 base score: 9.4
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H
CWE identifier: CWE-552 (Files or Directories Accessible to External Parties)

CVE-2026-2331 Files or Directories Accessible to External Parties

Summary: An attacker may perform unauthenticated read and write operations on sensitive filesystem areas via the AppEngine Fileaccess over HTTP due to improper access restrictions. A critical filesystem directory was unintentionally exposed through the HTTP-based file access feature, allowing access without authentication. This includes device parameter files, enabling an attacker to read and modify application settings, including customer-defined passwords. Additionally, exposure of the custom application directory may allow execution of arbitrary Lua code within the sandboxed AppEngine environment.

CVE-2026-2331 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-552 (Files or Directories Accessible to External Parties)

Remediations

Vendor Fix for CVE-2026-2330

Details: Users are strongly recommended to upgrade to release version 2.8.0.

Valid for:

- SICK Lector83x with firmware <2.8.0
- SICK Lector85x with firmware <2.8.0

Vendor Fix for CVE-2026-2331

Details: Users are strongly recommended to upgrade to release version 2.8.0.

Valid for:

- SICK Lector83x with firmware >= 2.6.0 <= 2.7.0
- SICK Lector85x with firmware >= 2.6.0 <= 2.7.0

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	2026-03-06	Initial version