

SICK PSIRT Security Advisory

AppEngine vulnerability affects SICK InspectorP6xx devices

Document ID: sca-2026-0010
Publication Date: 2026-07-28
CVE Identifier: CVE-2026-11841
CVSSv3 Base Score: 9.4
CVSSv3 Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L
Version: 1

Summary

Multiple internal virtual filesystem paths are unintentionally accessible remotely in the SICK InspectorP6xx devices. If exploited, this vulnerability could potentially allow an unauthenticated attacker to compromise the availability, integrity, and confidentiality of the devices.

List of Products

Product	Part Number	Affected by
SICK InspectorP61x with firmware <5.4.0	1124942 1124949 1124943 1124948 1142000 1124947 1142001 1124946 1143233 1143232 1114809 1116350	<u>CVE-2026-11841</u> Status: Known Affected Remediation: Vendor fix

SICK InspectorP62x with firmware <5.4.0	1111871 1110848 1130942 1154202 1110849 1111870 1110847 1154203 1121695 1121694 1156218 1118465 1118466 1156219	<u>CVE-2026-11841</u> Status: Known Affected Remediation: Vendor fix
SICK InspectorP63x all firmware versions	1082298 1082299 1082300 1082301 1101157 1101640	<u>CVE-2026-11841</u> Status: Known Affected Remediation: Mitigation
SICK InspectorP64x all firmware versions	1075507 1082302	<u>CVE-2026-11841</u> Status: Known Affected Remediation: Mitigation
SICK InspectorP65x all firmware versions	1073669 1073670 1082303 1082304 1082305 1082306	<u>CVE-2026-11841</u> Status: Known Affected Remediation: Mitigation

Vulnerability Overview

CVE-2026-11841 Files or Directories Accessible to External Parties

Summary: A vulnerability has been identified in the SOPAS FileSystemAccess method that allows unintended remote access to internal virtual filesystem paths. Due to insufficient access restrictions, an attacker with network access can query and modify internal storage locations, configuration files, and system-related application directories. This exposure may lead to the Denial of Service, unauthorized change of device configuration or disclosure of sensitive system information that could facilitate further attacks or compromise of the device.

CVE-2026-11841 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:H/I:H/A:L

CWE identifier: CWE-552 (Files or Directories Accessible to External Parties)

Remediations

Vendor Fix for CVE-2026-11841

Details: Users are recommended to upgrade to version 5.4.0.

Valid for:

- SICK InspectorP61x with firmware <5.4.0
- SICK InspectorP62x with firmware <5.4.0

Mitigation for CVE-2026-11841

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 InspectorP63x all firmware versions
- SICK InspectorP64x all firmware versions
- SICK InspectorP65x all firmware versions

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	2026-07-28	Initial version