

SICK PSIRT Security Advisory

Vulnerabilities Affecting SICK CorivaHub

Document ID: sca-2026-0016

Publication Date: 2026-10-16

CVE Identifier: CVE-2026-65637, CVE-2026-85061

Version: 1

Summary

SICK CorivaHub includes the third-party components Apache Tomcat and MapLibre GL, which are affected by two known vulnerabilities. These vulnerabilities include an improper input validation issue in Apache Tomcat and a vulnerability in MapLibre GL that could allow malicious behavior through custom GUIs. Under certain conditions, successful exploitation could affect the confidentiality, integrity and availability of the affected system. The attack surface associated with the Apache Tomcat vulnerability is significantly reduced by the default product configuration. Nevertheless, SICK recommends updating to CorivaHub 2026.1.2 to remediate both vulnerabilities.

List of Products

Product	Details
SICK CorivaHub <=2026.1.1	<u>Status:</u> Known Affected <u>Remediation:</u> Vendor Fix <u>CVE IDs:</u> CVE-2026-65637, CVE-2026-85061 <u>Status:</u> Known Affected <u>Remediation:</u> Workaround <u>CVE IDs:</u> CVE-2026-85061

Vulnerability Overview

CVE-2026-65637 Improper Input Validation

Summary: Improper Input Validation vulnerability in Apache Tomcat due to incomplete fix for CVE-2026-32990. This issue affects Apache Tomcat: from 11.0.20 through 11.0.24, from 10.1.53 through 10.1.57, from 9.0.115 through 9.0.120. Users are recommended to upgrade to version 11.0.25, 10.1.58 or 9.0.121, which fix the issue.

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-20 (Improper Input Validation)

Remediations:

Product	Details
SICK CorivaHub <=2026.1.1	<u>Vendor Fix</u> Users are recommended to upgrade to version 2026.1.2.

CVE-2026-85061 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Summary: MapLibre GL JS is an interactive vector tile map library for web browsers. Prior to 6.4.1, DOM.sanitize() in src/util/dom.ts iterates elem.attributes as a live NamedNodeMap while removeAttributes() removes attributes from the same collection, shifting indexes and skipping an adjacent dangerous attribute. An attacker who controls untrusted third-party style attribution strings or user-supplied custom attributions can supply consecutive dangerous attributes, causing an attribute such as onload or ontoggle to survive sanitization and execute when the attribution control inserts the content into innerHTML. A victim must render the affected map content for the script to execute. This issue is fixed in version 6.4.1.

CVSSv3.1 base score: 10

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

CWE identifier: CWE-79 (Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'))

Remediations:

Product	Details
SICK CorivaHub <=2026.1.1	<u>Vendor Fix</u> Users are recommended to upgrade to version 2026.1.2.
SICK CorivaHub <=2026.1.1	<u>Workaround</u> Customers may disable the offline map functionality by setting corivaHubOfflineMap.enabled to false in the CorivaHub configuration. This prevents the affected MapLibre GL component from being loaded and mitigates the vulnerability. The workaround is not expected to have a significant impact on normal production operations. Detailed configuration instructions are available in the CorivaHub documentation: https://portal.coriva.io/portal/app/hub-docs?s=main%252F2026.1%252Fdeployment%252Fcluster%252Fconfig-values.html%2523_tile_server

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>

The canonical URL.:

<https://www.sick.com/.well-known/csaf/white/2026/sca-2026-0016.json>

CorivaHub documentation:

https://portal.coriva.io/portal/app/hub-docs?s=main%252F2026.1%252Fdeployment%252Fcluster%252Fconfig-values.html%2523_tile_server

History

Version	Release Date	Comment
1	2026-10-16	Initial version