TLP:WHITE

SICK PSIRT Security Advisory

SICK Products affected by Brotli Vulnerability (Broccoli2Shell)

Document ID: sca-2026-0017

Publication Date: 2026-11-06

CVE Identifier: CVE-2026-111497

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

Version: 1

Summary

SICK identified multiple products affected by the Brotli vulnerability, also known as Broccoli2Shell (CVE-2026-111497). Successful exploitation of this vulnerability could impact the confidentiality, integrity, and availability of affected systems. At the time of publication, SICK is not aware of any active exploitation of this vulnerability targeting SICK products. SICK strongly recommends that customers review and implement the remediation measures provided in this advisory to reduce potential security risks.

List of Products

Product	Details
SICK Baggage Analytics all versions	Status: Known Affected Remediation: Vendor Fix CVE IDs: CVE-2026-111497 Status: Known Affected Remediation: Workaround CVE IDs: CVE-2026-111497
SICK CorivaHub < 2026.1.3	Status: Known Affected Remediation: Vendor Fix CVE IDs: CVE-2026-111497 Status: Known Affected Remediation: Workaround CVE IDs: CVE-2026-111497

Product	Details
SICK Logistics Diagnostic Analytics all versions	Status: Known Affected Remediation: Vendor Fix CVE IDs: CVE-2026-111497 Status: Known Affected Remediation: Workaround CVE IDs: CVE-2026-111497
SICK Package Analytics all versions	Status: Known Affected Remediation: Vendor Fix CVE IDs: CVE-2026-111497 Status: Known Affected Remediation: Workaround CVE IDs: CVE-2026-111497
SICK Tire Analytics all versions	Status: Known Affected Remediation: Vendor Fix CVE IDs: CVE-2026-111497 Status: Known Affected Remediation: Workaround CVE IDs: CVE-2026-111497

Vulnerability Overview

CVE-2026-111497 Unchecked Return Value

Summary: A buffer overflow vulnerability in the Brotli decoder (c/dec/decode.c) in Google Brotli versions 1.0.3 through 1.2.0 on all platforms allows a remote unauthenticated attacker to corrupt adjacent decoder state memory, disclose sensitive memory contents, cause a denial of service, or potentially execute arbitrary code using a crafted Brotli-compressed stream. Users need to update any Brotli libraries or binaries between 1.0.3 through 1.2.0 to the latest available version: 1.0.10 or 1.1.1 or 1.2.1.

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-252 (Unchecked Return Value)

Remediations:

Product	Details
SICK CorivaHub < 2026.1.3	Vendor Fix Users are recommended to re-install or upgrade to version 2026.1.3 while setting the global.imagePullPolicy to 'IfNotPresent'.
SICK Logistics Diagnostic Analytics all versions SICK Package Analytics all versions SICK Baggage Analytics all versions SICK Tire Analytics all versions	Workaround As an immediate risk reduction measure, customers should disable the affected services on affected systems: 1.Open Windows Services. 2.Stop the following services (if present): •SICK Node-RED •SICK An Native Access •SICK An Bridge 3. Set the Startup Type for each service to Disabled. For most customers, disabling Node-RED is not expected to impact normal Process Analytics functionality, provided that Node-RED integrations are not being used to consume data from third-party systems.
SICK CorivaHub < 2026.1.3	Workaround 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/hubdocs?s=main%252F2026.1%252Fdeployment%252Fcluster%252Fconfig-values.html%2523_tile_server

Product	Details
SICK Logistics Diagnostic Analytics all versions SICK Package Analytics all versions SICK Baggage Analytics all versions SICK Tire Analytics all versions	Vendor Fix The provided fix addresses exploitation via Node-RED only. Exploitation via Bridge and native Access remains possible and must be mitigated using the documented workarounds. Customers who require Node-RED functionality may manually update the bundled Node.js runtime on each affected Process Analytics instance: 1. Stop the SICK Node-RED service. 2. Create a backup of the following directory: C:\Program Files\SICK\Analytics Solutions\node-red\runtime\nodejs 3. Download and extract Node.js 24.22.1. 4. Replace the existing nodejs directory with the extracted version. 5. Verify the installed version:node.exe -v 6. Restart the SICK Node-RED service. 7. Validate that Process Analytics and Node-RED functionality operate as expected. 8. If any issues are observed, restore the backup and revert to the previous version.

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-2026-0017.json

History

Version	Release Date	Comment
1	2026-11-06	Initial version