TLP:WHITE

SICK PSIRT
Security Advisory

Vulnerability in SICK Logistics Analytics Products and SICK Field Analytics

Document ID:	SCA-2024-0001
Publication Date:	2024-01-29
CVE Identifier:	CVE-2023-46604
CVSSv3 Base Score:	9.8
CVSSv3 Vector String:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Version:	2

Summary

A critical vulnerability in Apache ActiveMQ affects the SICK products Field Analytics 1.2 and Logistics Analytics products 4.5.
The Java OpenWire protocol marshaller that is used in ActiveMQ Classic and ActiveMQ Artemis is vulnerable to Remote Code execution. This vulnerability may allow a remote attacker with network access to either a Java-based OpenWire broker or client to run arbitrary shell commands by manipulating serialized class types in the OpenWire protocol to cause either the client or the broker (respectively) to instantiate any class on the classpath.
Therefore it is strongly recommended to upgrade both Logistics Analytics products 4.5 and Field Analytics 1.2 to the latest release.
Prior versions of Logistics Analytics products are not affected.

List of Products

Product	Affected by
SICK Baggage Analytics 4.5	CVE-2023-46604 Status: Known Affected Remediation: Vendor fix
SICK Field Analytics 1.2	CVE-2023-46604 Status: Known Affected Remediation: Vendor fix
SICK Logistics Diagnostic Analytics 4.5	CVE-2023-46604 Status: Known Affected Remediation: Vendor fix
SICK Package Analytics 4.5	CVE-2023-46604 Status: Known Affected Remediation: Vendor fix
SICK Tire Analytics 4.5	CVE-2023-46604 Status: Known Affected Remediation: Vendor fix

Vulnerability Overview

CVE-2023-46604 Deserialization of Untrusted Data

Summary: The Java OpenWire protocol marshaller is vulnerable to Remote Code Execution. This vulnerability may allow a remote attacker with network access to either a Java-based OpenWire broker or client to run arbitrary shell commands by manipulating serialized class types in the OpenWire protocol to cause either the client or the broker (respectively) to instantiate any class on the classpath. Users are recommended to upgrade both Apache ActiveMQ Classic and Apache ActiveMQ Legacy brokers and clients to version 5.15.16, 5.16.7, 5.17.6, or 5.18.3 which fixes this issue.

CVE-2023-46604 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-502 (Deserialization of Untrusted Data)

References:
Active MQ Notification:
https://activemq.apache.org/news/cve-2023-46604

Remediations

Vendor Fix for CVE-2023-46604

Details: Customers who use the version 1.2 are strongly recommended to upgrade to the latest release 1.2.2.

Valid for:

- SICK Field Analytics 1.2

Details: Customers who use the version 4.5 are strongly recommended to upgrade to the latest release 4.5.1. Prior versions of Logistics Analytics products are not affected.

Valid for:

- SICK Baggage Analytics 4.5
- SICK Logistics Diagnostic Analytics 4.5
- SICK Package Analytics 4.5
- SICK Tire Analytics 4.5

General Security Practices

General Security Measures

As general security measures, SICK recommends to minimize network exposure of the devices, restrict network access and follow 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://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	2024-01-29	Initial version
2	2025-07-30	Updated Advisory: URL for SICK Operating Guidelines has been updated