TLP:WHITE

SICK PSIRT
Security Advisory

Vulnerabilities in SICK EventCam App

Document ID:	SCA-2023-0005
Publication Date:	2023-06-19
CVE Identifiers:	CVE-2023-31410, CVE-2023-31411
Version:	2

Summary

SICK discovered vulnerabilities in the SICK EventCam App, that can be accessed via Ethernet. If exploited, this potentially allows a remote unauthenticated attacker to impact availabiltiy, integrity and confidentaility of the EventCam App. SICK recommends making sure to run the product in a secure environment. SICK is not aware of an exploit targeting this vulnerability.

List of Products

Product	Part Number	Affected by
SICK EventCam App all versions	1616071 1615765	CVE-2023-31410 Status: Known Affected Remediation: Workaround
		CVE-2023-31411 Status: Known Affected Remediation: Workaround

SICK
Sensor Intelligence.

TLP:WHITE

Vulnerability Overview

CVE-2023-31410 Cleartext Transmission of Sensitive Information

Description: A remote unprivileged attacker can intercept the communication via e.g. Man-In-The-Middle, due to the absence of Transport Layer Security (TLS) in the SICK EventCam App. This lack of encryption in the communication channel can lead to the unauthorized disclosure of sensitive information. The attacker can exploit this weakness to eavesdrop on the communication between the EventCam App and the Client, and potentially manipulate the data being transmitted.

CVE-2023-31410 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-319 (Cleartext Transmission of Sensitive Information)

CVE-2023-31411 Improper Authorization

Description: A remote unprivileged attacker can modify and access configuration settings on the EventCam App due to the absence of API authentication. The lack of authentication in the API allows the attacker to potentially compromise the functionality of the EventCam App.

CVE-2023-31411 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-285 (Improper Authorization)

Remediations

Workaround for CVE-2023-31410

Details: Please make sure that you apply general security practices when operating the EventCam App. The following General Security Practices and Operating Guidelines could mitigate the associated security risk.

Valid for:

- SICK EventCam App all versions

Workaround for CVE-2023-31411

Details: Please make sure that you apply general security practices when operating the EventCam App. The following General Security Practices and Operating Guidelines could mitigate the associated security risk.

Valid for:

- SICK EventCam App all versions

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://cdn.sick.com/media/docs/1/11/411/Special_information_CYBERSECURITY_BY_SICK_en_IM0084411.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	2023-06-19	Initial Release
2	2023-12-04	Added self reference in CSAF