SICK
Sensor Intelligence.

TLP:WHITE

SICK PSIRT
Security Advisory

Vulnerability in multiple SICK Flexi Soft Gateways

Document ID:	SCA-2023-0011
Publication Date:	2023-10-23
CVE Identifier:	CVE-2023-5246
CVSSv3 Base Score:	8.8
CVSSv3 Vector String:	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Version:	2

Summary

The SICK PSIRT received a report about a vulnerability in several Flexi Soft Gateways that could allow an attacker to login to the gateways by sending specially crafted packets and potentially impact the availabilty, integrity and confidentiality of the devices.
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 FX0-GENT00000 all Firmware versions	1044072	CVE-2023-5246 Status: Known Affected Remediation: Workaround
SICK FX0-GENT00010 all Firmware versions	1121596	CVE-2023-5246 Status: Known Affected Remediation: Workaround
SICK FX0-GENT00030 all Firmware versions	1099830	CVE-2023-5246 Status: Known Affected Remediation: Workaround

SICK FX0-GETC00000 all Firmware versions	1051432	CVE-2023-5246 Status: Known Affected Remediation: Workaround
SICK FX0-GETC00010 all Firmware versions	1127487	CVE-2023-5246 Status: Known Affected Remediation: Workaround
SICK FX0-GMOD00000 all Firmware versions	1044073	CVE-2023-5246 Status: Known Affected Remediation: Workaround
SICK FX0-GMOD00010 all Firmware versions	1127717	CVE-2023-5246 Status: Known Affected Remediation: Workaround
SICK FX0-GMOD00030 all Firmware versions	1130282	CVE-2023-5246 Status: Known Affected Remediation: Workaround
SICK FX0-GPNT00000 all Firmware versions	1044074	CVE-2023-5246 Status: Known Affected Remediation: Workaround
SICK FX0-GPNT00010 all Firmware versions	1121597	CVE-2023-5246 Status: Known Affected Remediation: Workaround
SICK FX0-GPNT00030 all Firmware versions	1099832	CVE-2023-5246 Status: Known Affected Remediation: Workaround
SICK FX3-GEPR00000 all Firmware versions	1069070	CVE-2023-5246 Status: Known Affected Remediation: Workaround
SICK FX3-GEPR00010 all Firmware versions	1112296	CVE-2023-5246 Status: Known Affected Remediation: Workaround

Vulnerability Overview

CVE-2023-5246 Authentication Bypass by Capture-replay

CVE Description: Authentication Bypass by Capture-replay in SICK Flexi Soft Gateways with Part-numbers 1044073, 1127717, 1130282, 1044074, 1121597, 1099832, 1051432, 1127487, 1069070, 1112296, 1044072, 1121596, 1099830 allows an unauthenticated remote attacker to potentially impact the availabilty, integrity and confidentaility of the gateways via an authentication bypass by capture-replay.

CVE-2023-5246 has been assigned to this vulnerability.
CVSSv3.1 base score: 8.8
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
CWE identifier: CWE-294 (Authentication Bypass by Capture-replay)

Remediations

Workaround for CVE-2023-5246

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

Valid for:

- SICK FX0-GENT00000 all Firmware versions
- SICK FX0-GENT00010 all Firmware versions
- SICK FX0-GENT00030 all Firmware versions
- SICK FX0-GETC00000 all Firmware versions
- SICK FX0-GETC00010 all Firmware versions
- SICK FX0-GMOD00000 all Firmware versions
- SICK FX0-GMOD00010 all Firmware versions
- SICK FX0-GMOD00030 all Firmware versions
- SICK FX0-GPNT00000 all Firmware versions
- SICK FX0-GPNT00010 all Firmware versions
- SICK FX0-GPNT00030 all Firmware versions
- SICK FX3-GEPR00000 all Firmware versions
- SICK FX3-GEPR00010 all Firmware 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	2023-10-23	Initial Release
2	2023-12-04	Added self reference in CSAF