SICK
Sensor Intelligence.

TLP:WHITE

SICK PSIRT
Security Advisory

Vulnerability in SICK Flexi Soft and Flexi Classic Gateways

Document ID:	SCA-2023-0003
Publication Date:	2023-05-03
CVE Identifier:	CVE-2023-23444
CVSSv3 Base Score:	7.5
CVSSv3 Vector String:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Version:	2

Summary

SICK discovered a vulnerability in several Flexi Classic and Flexi Soft Gateways. If exploited, this potentially allows a remote unauthenticated attacker to impact the availabiltiy of the gateways.
SICK is not aware of an exploit targeting this vulnerability.

List of Products

Product	Part Number	Affected by
SICK FX0-GENT00000 FLEXISOFT EIP GATEW. all Firmware versions	1044072	CVE-2023-23444 Status: Known Affected Remediation: Workaround
SICK FX0-GENT00010 FLEXISOFT EIP GW (C) all Firmware versions	1121596	CVE-2023-23444 Status: Known Affected Remediation: Workaround
SICK FX0-GENT00030 FLEXISOFT EIP GATEW.V2 all Firmware versions	1099830	CVE-2023-23444 Status: Known Affected Remediation: Workaround
SICK FX0-GMOD00000 FLEXISOFT MOD GATEW. all Firmware versions	1044073	CVE-2023-23444 Status: Known Affected Remediation: Workaround

SICK FX0-GMOD00010 FLEXISOFT MOD GW (C) all Firmware versions	1127717	CVE-2023-23444 Status: Known Affected Remediation: Workaround
SICK FX0-GPNT00000 FLEXISOFT PNET GATEW. all Firmware versions	1044074	CVE-2023-23444 Status: Known Affected Remediation: Workaround
SICK FX0-GPNT00010 FLEXISOFT PNET GW (C) all Firmware versions	1121597	CVE-2023-23444 Status: Known Affected Remediation: Workaround
SICK FX0-GPNT00030 FLEXISOFT PNET GATEW.V2 all Firmware versions	1099832	CVE-2023-23444 Status: Known Affected Remediation: Workaround
SICK UE410-EN1 FLEXI ETHERNET GATEW. all Firmware versions	1042964	CVE-2023-23444 Status: Known Affected Remediation: Workaround
SICK UE410-EN3 FLEXI ETHERNET GATEW. all Firmware versions	1042193	CVE-2023-23444 Status: Known Affected Remediation: Workaround
SICK UE410-EN4 FLEXI ETHERNET GATEW. all Firmware versions	1044078	CVE-2023-23444 Status: Known Affected Remediation: Workaround

Vulnerability Overview

CVE-2023-23444 Missing Authentication for Critical Function

Summary: An unauthenticated remote attacker can change the IP settings of the SICK Flexi Classic and Flexi Soft Gateways by sending a broadcasted UDP packet and thereby affect the available of the gateways.

CVE description: Missing Authentication for Critical Function in SICK Flexi Classic and Flexi Soft Gateways with Partnumbers 1042193, 1042964, 1044078, 1044072, 1044073, 1044074, 1099830, 1099832, 1127717, 1121596, 1121597 allows an unauthenticated remote attacker to influence the availability of the device by changing the IP settings of the device via broadcasted UDP packets.

CVE-2023-23444 has been assigned to this vulnerability.
CVSSv3.1 base score: 7.5
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CWE identifier: CWE-306 (Missing Authentication for Critical Function)

Remediations

Workaround for CVE-2023-23444

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

Valid for:

- SICK FX0-GENT00000 FLEXISOFT EIP GATEW. all Firmware versions
- SICK FX0-GENT00010 FLEXISOFT EIP GW (C) all Firmware versions
- SICK FX0-GENT00030 FLEXISOFT EIP GATEW.V2 all Firmware versions
- SICK FX0-GMOD00000 FLEXISOFT MOD GATEW. all Firmware versions
- SICK FX0-GMOD00010 FLEXISOFT MOD GW (C) all Firmware versions
- SICK FX0-GPNT00000 FLEXISOFT PNET GATEW. all Firmware versions
- SICK FX0-GPNT00010 FLEXISOFT PNET GW (C) all Firmware versions
- SICK FX0-GPNT00030 FLEXISOFT PNET GATEW.V2 all Firmware versions
- SICK UE410-EN1 FLEXI ETHERNET GATEW. all Firmware versions
- SICK UE410-EN3 FLEXI ETHERNET GATEW. all Firmware versions
- SICK UE410-EN4 FLEXI ETHERNET GATEW. 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	2023-05-03	Initial Release
2	2023-12-04	Added self reference in CSAF