TLP:WHITE

SICK PSIRT
Security Advisory

Bootloader mode vulnerability in Flexi Soft Gateways v3

Document ID:	SCA-2023-0001
Publication Date:	2023-02-20
CVE Identifiers:	CVE-2023-23453, CVE-2023-23452
Version:	2

Summary

The SICK PSIRT received a report about a Missing Authentication for Critical Function vulnerability in the firmware of FX0-GPNT v3 and FX0-GENT v3. This vulnerability was introduced with the hardware redesign of the v3 of FX0-GENT and FX0-GPNT as part of the implementation of the RK512 protocol. The RK512 protocol is used to configure the Flexi Soft stations via an exposed TCP port on the Ethernet based gateways.

List of Products

Product	Part Number	Affected by
SICK FX0-GENT00000 v3 with Firmware V3.04	1044072	CVE-2023-23453 Status: Known Affected Remediation: Workaround
SICK FX0-GENT00000 v3 with Firmware V3.05	1044072	CVE-2023-23453 Status: Known Affected Remediation: Workaround
SICK FX0-GENT00010 v3 with Firmware V3.04	1121596	CVE-2023-23453 Status: Known Affected Remediation: Workaround
SICK FX0-GENT00010 v3 with Firmware V3.05	1121596	CVE-2023-23453 Status: Known Affected Remediation: Workaround

SICK FX0-GPNT00000 v3 with Firmware V3.04	1044074	CVE-2023-23452 Status: Known Affected Remediation: Workaround
SICK FX0-GPNT00000 v3 with Firmware V3.05	1044074	CVE-2023-23452 Status: Known Affected Remediation: Workaround
SICK FX0-GPNT00010 v3 with Firmware V3.04	1121597	CVE-2023-23452 Status: Known Affected Remediation: Workaround
SICK FX0-GPNT00010 v3 with Firmware V3.05	1121597	CVE-2023-23452 Status: Known Affected Remediation: Workaround

Vulnerability Overview

CVE-2023-23453 Missing Authentication for Critical Function

Description: The Flexi Soft Gateways FX0-GENT00000 v3 and FX0-GENT00010 v3 use the RK512 protocol to configure the Flexi Soft stations via an exposed TCP port on the Ethernet based gateways. A remote unauthenticated attacker may craft malicious packets to the listener on TCP port 9000 and may use this vulnerability as a permanent denial of service attack. If the attacker is more sophisticated, the attacker may even achieve remote code execution.

CVE-2023-23453 has been assigned to this vulnerability.
CVSSv3.1 base score: 9.1
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H
CWE identifier: CWE-306 (Missing Authentication for Critical Function)

CVE-2023-23452 Missing Authentication for Critical Function

Description: The Flexi Soft Gateways FX0-GPNT00000 v3 and FX0-GPNT00010 v3 use the RK512 protocol to configure the Flexi Soft stations via an exposed TCP port on the Ethernet based gateways. A remote unauthenticated attacker may craft malicious packets to the listener on TCP port 9000 and may use this vulnerability as a permanent denial of service attack. If the attacker is more sophisticated, the attacker may even achieve remote code execution.

CVE-2023-23452 has been assigned to this vulnerability.
CVSSv3.1 base score: 9.1
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H
CWE identifier: CWE-306 (Missing Authentication for Critical Function)

Remediations

Workaround for CVE-2023-23453

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

Valid for:

- SICK FX0-GENT00000 v3 with Firmware V3.04
- SICK FX0-GENT00000 v3 with Firmware V3.05
- SICK FX0-GENT00010 v3 with Firmware V3.04
- SICK FX0-GENT00010 v3 with Firmware V3.05

Workaround for CVE-2023-23452

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

Valid for:

- SICK FX0-GPNT00000 v3 with Firmware V3.04
- SICK FX0-GPNT00000 v3 with Firmware V3.05
- SICK FX0-GPNT00010 v3 with Firmware V3.04
- SICK FX0-GPNT00010 v3 with Firmware V3.05

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:
http://ics-cert.us-cert.gov/content/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/2023/sca-2023-0001.json

The canonical PDF URL.:
https://www.sick.com/.well-known/csaf/white/2023/sca-2023-0001.pdf

History

Version	Release Date	Comment
1	2023-02-20	Initial Release
2	2023-02-23	Updated Advisory (only visual changes)