SICK
Sensor Intelligence.

TLP:WHITE

SICK PSIRT
Security Advisory

Vulnerability in SICK Flexi Soft PROFINET IO Gateway FX0-GPNT and SICK microScan3 PROFINET

Document ID:	SCA-2022-0009
Publication Date:	2022-04-29
CVE Identifier:	N/A (CWE-400)
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:	V2.0

Summary

The PSIRT received a report about a vulnerability in the Gateway Flexi Soft and microScan3 PROFINET. The vulnerability is classified as a denial-of-service vulnerability and results form a mishandling of Read Implicit Request services.
An attacker could use this vulnerability to affect the availability of the Gateway Flexi Soft and microScan3 PROFINET.
Even if the SICK Gateway Flexi Soft or mircoScan3 PROFINET is made unavailable, no safety issue ensues. The main module of the gateway set its outputs in the safe state (low).
It is recommended to implement the mitigations described in the mitigations section.

Affected Products

Product	Model Numbers	SKUs	Affected by
FX0-GPNT	3.04.0 3.05.0		Uncontrolled Resource Consumption Status: Affected Remediation: Yes (mitigation)
MICS3-ABAZ90PZ1	1.23 up to 1.47	1100407	Uncontrolled Resource Consumption Status: Affected Remediation: Yes (mitigation)
MICS3-CCAZ55PZ1	1.23 up to 1.47	1100391	Uncontrolled Resource Consumption Status: Affected Remediation: Yes (mitigation)

MICS3-CCAZ90PZ1	1.23 up to 1.47	1100393	Uncontrolled Resource Consumption Status: Affected Remediation: Yes (mitigation)
MICS3-ACAZ55LZ1	1.23 up to 1.47	1100385	Uncontrolled Resource Consumption Status: Affected Remediation: Yes (mitigation)
MICS3-ACAZ90LZ1	1.23 up to 1.47	1100387	Uncontrolled Resource Consumption Status: Affected Remediation: Yes (mitigation)
MICS3-ABAZ40PZ1	1.23 up to 1.47	1100403	Uncontrolled Resource Consumption Status: Affected Remediation: Yes (mitigation)
MICS3-ABAZ55PZ1	1.23 up to 1.47	1100405	Uncontrolled Resource Consumption Status: Affected Remediation: Yes (mitigation)
MICS3-ACAZ40PZ1	1.23 up to 1.47	1083011	Uncontrolled Resource Consumption Status: Affected Remediation: Yes (mitigation)
MICS3-ACAZ55PZ1	1.23 up to 1.47	1083009	Uncontrolled Resource Consumption Status: Affected Remediation: Yes (mitigation)
MICS3-CBAZ40PZ1	1.23 up to 1.47	1092718	Uncontrolled Resource Consumption Status: Affected Remediation: Yes (mitigation)
MICS3-CBAZ55PZ1	1.23 up to 1.47	1092719	Uncontrolled Resource Consumption Status: Affected Remediation: Yes (mitigation)
MICS3-ACAZ90PZ1	1.23 up to 1.47	1094458	Uncontrolled Resource Consumption Status: Affected Remediation: Yes (mitigation)
MICS3-CBAZ90PZ1	1.23 up to 1.47	1094462	Uncontrolled Resource Consumption Status: Affected Remediation: Yes (mitigation)
MICS3-CCAZ40PZ1	1.23 up to 1.47	1100389	Uncontrolled Resource Consumption Status: Affected Remediation: Yes (mitigation)
MICS3-CCAZ55LZ1	1.23 up to 1.47	1100399	Uncontrolled Resource Consumption Status: Affected Remediation: Yes (mitigation)

MICS3-CCAZ90LZ1	1.23 up to 1.47	1100401	Uncontrolled Resource Consumption Status: Affected Remediation: Yes (mitigation)
MICS3-CCAZ40LZ1	1.23 up to 1.47	1100397	Uncontrolled Resource Consumption Status: Affected Remediation: Yes (mitigation)
MICS3-ACAZ40LZ1	1.23 up to 1.47	1100383	Uncontrolled Resource Consumption Status: Affected Remediation: Yes (mitigation)

Vulnerability Overview

Uncontrolled Resource Consumption

An attacker that has access to one of the above listed products with the corresponding firmware versions could affect the availability by exploiting the gateway Flexi Soft or microScan3 PROFINET with a malformed PROFINET Read Implicit Request service. This forces the main module of the gateway to set its outputs in the safe state (low).

No CVE 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

Remediations

Mitigation for Uncontrolled Resource Consumption

Valid for: FX0-GPNT, MICS3-ABAZ90PZ1, MICS3-CCAZ55PZ1, MICS3-CCAZ90PZ1, MICS3-ACAZ55LZ1, MICS3-ACAZ90LZ1, MICS3-ABAZ40PZ1, MICS3-ABAZ55PZ1, MICS3-ACAZ40PZ1, MICS3-ACAZ55PZ1, MICS3-CBAZ40PZ1, MICS3-CBAZ55PZ1, MICS3-ACAZ90PZ1, MICS3-CBAZ90PZ1, MICS3-CCAZ40PZ1, MICS3-CCAZ55LZ1, MICS3-CCAZ90LZ1, MICS3-CCAZ40LZ1, MICS3-ACAZ40LZ1

Details: Please make sure that you apply general security practices when operating the SICK Flexi Soft PROFINET IO Gateway FX0-GPNT and microScan3 PROFINET. The following general security practices could mitigate the associated security risk.

General Security Practices

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.

Additional information on Industrial Security can be found at:
http://ics-cert.us-cert.gov/content/recommended-practices

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

Product Glossary

FX0-GPNT	FX0-GPNT
MICS3-ABAZ90PZ1	The microScan3 safety laser scanner stands for the protection of very different applications: from stationary to mobile, from simple to complex. The innovative safeHDDM® scanning technology makes the microScan3 extremely resistant, even to dust and ambient light, and delivers high-precision measurement data. It increases the productivity and availability of machines. The different variants of the microScan3 can be integrated simply and safely into countless networks. In addition, the safety laser scanner offers standardized connectivity for time-saving commissioning. The microScan3, the easy handling of its Safety Designer configuration software and its diagnostic options combine user-friendly operation, innovation and very high performance.
MICS3-CCAZ55PZ1	See description of MICS3-ABAZ90PZ1.
MICS3-CCAZ90PZ1	See description of MICS3-ABAZ90PZ1.
MICS3-ACAZ55LZ1	See description of MICS3-ABAZ90PZ1.
MICS3-ACAZ90LZ1	See description of MICS3-ABAZ90PZ1.
MICS3-ABAZ40PZ1	See description of MICS3-ABAZ90PZ1.
MICS3-ABAZ55PZ1	See description of MICS3-ABAZ90PZ1.
MICS3-ACAZ40PZ1	See description of MICS3-ABAZ90PZ1.
MICS3-ACAZ55PZ1	See description of MICS3-ABAZ90PZ1.
MICS3-CBAZ40PZ1	See description of MICS3-ABAZ90PZ1.
MICS3-CBAZ55PZ1	See description of MICS3-ABAZ90PZ1.

MICS3-ACAZ90PZ1	See description of MICS3-ABAZ90PZ1.
MICS3-CBAZ90PZ1	See description of MICS3-ABAZ90PZ1.
MICS3-CCAZ40PZ1	See description of MICS3-ABAZ90PZ1.
MICS3-CCAZ55LZ1	See description of MICS3-ABAZ90PZ1.
MICS3-CCAZ90LZ1	See description of MICS3-ABAZ90PZ1.
MICS3-CCAZ40LZ1	See description of MICS3-ABAZ90PZ1.
MICS3-ACAZ40LZ1	See description of MICS3-ABAZ90PZ1.

History

Version	Release Date	Comment
V1.0	2022-04-29	Initial Release
V2.0	2022-06-20	Updated affected products