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:	3

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.

List of Products

Product	Part Number	Affected by
SICK FX0-GPNT with Firmware 3.04.0		Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK FX0-GPNT with Firmware 3.05.0		Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available

SICK MICS3-ABAZ40PZ1 with Firmware 1.23 up to 1.47	1100403	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-ABAZ55PZ1 with Firmware 1.23 up to 1.47	1100405	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-ABAZ90PZ1 with Firmware 1.23 up to 1.47	1100407	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-ACAZ40LZ1 with Firmware 1.23 up to 1.47	1100383	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-ACAZ40PZ1 with Firmware 1.23 up to 1.47	1083011	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-ACAZ55LZ1 with Firmware 1.23 up to 1.47	1100385	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-ACAZ55PZ1 with Firmware 1.23 up to 1.47	1083009	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-ACAZ90LZ1 with Firmware 1.23 up to 1.47	1100387	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available

SICK MICS3-ACAZ90PZ1 with Firmware 1.23 up to 1.47	1094458	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-CBAZ40PZ1 with Firmware 1.23 up to 1.47	1092718	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-CBAZ55PZ1 with Firmware 1.23 up to 1.47	1092718	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-CBAZ90PZ1 with Firmware 1.23 up to 1.47	1094462	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-CCAZ40LZ1 with Firmware 1.23 up to 1.47	1100397	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-CCAZ40PZ1 with Firmware 1.23 up to 1.47	1100389	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-CCAZ55LZ1 with Firmware 1.23 up to 1.47	1100399	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-CCAZ55PZ1 with Firmware 1.23 up to 1.47	1100391	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available

SICK MICS3-CCAZ90LZ1 with Firmware 1.23 up to 1.47	1100401	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available
SICK MICS3-CCAZ90PZ1 with Firmware 1.23 up to 1.47	1100393	Uncontrolled Resource Consumption Status: Known Affected Remediation: Mitigation, None available

Vulnerability Overview

Uncontrolled Resource Consumption

Summary: 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.

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
CWE identifier: CWE-400 (Uncontrolled Resource Consumption)

Impact: 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).

Remediations

Mitigation for Uncontrolled Resource Consumption

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.

Valid for:

- SICK FX0-GPNT with Firmware 3.04.0
- SICK FX0-GPNT with Firmware 3.05.0

- SICK MICS3-ABAZ40PZ1 with Firmware 1.23 up to 1.47
- SICK MICS3-ABAZ55PZ1 with Firmware 1.23 up to 1.47
- SICK MICS3-ABAZ90PZ1 with Firmware 1.23 up to 1.47
- SICK MICS3-ACAZ40LZ1 with Firmware 1.23 up to 1.47
- SICK MICS3-ACAZ40PZ1 with Firmware 1.23 up to 1.47
- SICK MICS3-ACAZ55LZ1 with Firmware 1.23 up to 1.47
- SICK MICS3-ACAZ55PZ1 with Firmware 1.23 up to 1.47
- SICK MICS3-ACAZ90LZ1 with Firmware 1.23 up to 1.47
- SICK MICS3-ACAZ90PZ1 with Firmware 1.23 up to 1.47
- SICK MICS3-CBAZ40PZ1 with Firmware 1.23 up to 1.47
- SICK MICS3-CBAZ55PZ1 with Firmware 1.23 up to 1.47
- SICK MICS3-CBAZ90PZ1 with Firmware 1.23 up to 1.47
- SICK MICS3-CCAZ40LZ1 with Firmware 1.23 up to 1.47
- SICK MICS3-CCAZ40PZ1 with Firmware 1.23 up to 1.47
- SICK MICS3-CCAZ55LZ1 with Firmware 1.23 up to 1.47
- SICK MICS3-CCAZ55PZ1 with Firmware 1.23 up to 1.47
- SICK MICS3-CCAZ90LZ1 with Firmware 1.23 up to 1.47
- SICK MICS3-CCAZ90PZ1 with Firmware 1.23 up to 1.47

None available for Uncontrolled Resource Consumption

Details: Currently there is no remediation.

Valid for:

- SICK FX0-GPNT with Firmware 3.04.0
- SICK FX0-GPNT with Firmware 3.05.0
- SICK MICS3-ABAZ40PZ1 with Firmware 1.23 up to 1.47
- SICK MICS3-ABAZ55PZ1 with Firmware 1.23 up to 1.47
- SICK MICS3-ABAZ90PZ1 with Firmware 1.23 up to 1.47
- SICK MICS3-ACAZ40LZ1 with Firmware 1.23 up to 1.47
- SICK MICS3-ACAZ40PZ1 with Firmware 1.23 up to 1.47
- SICK MICS3-ACAZ55LZ1 with Firmware 1.23 up to 1.47
- SICK MICS3-ACAZ55PZ1 with Firmware 1.23 up to 1.47
- SICK MICS3-ACAZ90LZ1 with Firmware 1.23 up to 1.47
- SICK MICS3-ACAZ90PZ1 with Firmware 1.23 up to 1.47
- SICK MICS3-CBAZ40PZ1 with Firmware 1.23 up to 1.47
- SICK MICS3-CBAZ55PZ1 with Firmware 1.23 up to 1.47
- SICK MICS3-CBAZ90PZ1 with Firmware 1.23 up to 1.47
- SICK MICS3-CCAZ40LZ1 with Firmware 1.23 up to 1.47

- SICK MICS3-CCAZ40PZ1 with Firmware 1.23 up to 1.47
- SICK MICS3-CCAZ55LZ1 with Firmware 1.23 up to 1.47
- SICK MICS3-CCAZ55PZ1 with Firmware 1.23 up to 1.47
- SICK MICS3-CCAZ90LZ1 with Firmware 1.23 up to 1.47
- SICK MICS3-CCAZ90PZ1 with Firmware 1.23 up to 1.47

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

Additional Product Information

SICK MICS3-ABAZ40PZ1 with Firmware 1.23 up to 1.47	Product on sick.com: https://www.sick.com/de/de/p/p651059
SICK MICS3-ABAZ55PZ1 with Firmware 1.23 up to 1.47	Product on sick.com: https://www.sick.com/de/de/p/p651060
SICK MICS3-ABAZ90PZ1 with Firmware 1.23 up to 1.47	Product on sick.com: https://www.sick.com/de/de/p/p651061
SICK MICS3-ACAZ40PZ1 with Firmware 1.23 up to 1.47	Product on sick.com: https://www.sick.com/de/de/p/p529646
SICK MICS3-ACAZ55LZ1 with Firmware 1.23 up to 1.47	Product on sick.com: https://www.sick.com/de/de/p/p651063
SICK MICS3-ACAZ55PZ1 with Firmware 1.23 up to 1.47	Product on sick.com: https://www.sick.com/de/de/p/p529647
SICK MICS3-ACAZ90PZ1 with Firmware 1.23 up to 1.47	Product on sick.com: https://www.sick.com/de/de/p/p606747
SICK MICS3-CBAZ40PZ1 with Firmware 1.23 up to 1.47	Product on sick.com: https://www.sick.com/de/de/p/p574157
SICK MICS3-CBAZ55PZ1 with Firmware 1.23 up to 1.47	Product on sick.com: https://www.sick.com/de/de/p/p574157
SICK MICS3-CBAZ90PZ1 with Firmware 1.23 up to 1.47	Product on sick.com: https://www.sick.com/de/de/p/p606745
SICK MICS3-CCAZ40PZ1 with Firmware 1.23 up to 1.47	Product on sick.com: https://www.sick.com/de/de/p/p651066
SICK MICS3-CCAZ55PZ1 with Firmware 1.23 up to 1.47	Product on sick.com: https://www.sick.com/de/de/p/p651068
SICK MICS3-CCAZ90PZ1 with Firmware 1.23 up to 1.47	Product on sick.com: https://www.sick.com/de/de/p/p651070

History

Version	Release Date	Comment
1	2022-04-29	Initial Release
2	2022-06-20	Updated affected products
3	2023-02-10	Updated Advisory (only visual changes)