TLP:WHITE

SICK PSIRT
Security Advisory

Vulnerability in SICK Flexi Soft PROFINET IO Gateway FX0-GPNT

Document ID: SCA-2022-0009
Publication Date: 2022-04-29
CVSSv3 Base Score: 7.5
CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Version: V1.0

SUMMARY

The PSIRT received a report about a vulnerability in the Gateway Flexi Soft. 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.

Even if the SICK Gateway Flexi Soft is made unavailable, no safety issue ensues. The main module set its outputs in the safe state (low).

It is recommended to implement the mitigations described in the mitigations section.

AFFECTED PRODUCTS

Product	Version	Remediation available
FX0-GPNT	3.04.0 & 3.05.0	No

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 with a malformed Read Implicit Request service. This forces the gateway Flexi Soft main module 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

Mitigations

Please make sure that you:

- Operate the SICK Flexi Soft PROFINET IO Gateway FX0-GPNT in a secure environment, where only trusted entities have access.

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

HISTORY

Version	Release Date	Comment
V1.0	2022-04-29	Initial Release