SICK
Sensor Intelligence.

TLP:WHITE

SICK PSIRT
Security Advisory

SICK FlexiCompact affected by Denial of Service vulnerability

Document ID:	SCA-2022-0014
Publication Date:	2022-10-31
CVE Identifier:	CVE-2022-27583
CVSSv3 Base Score:	5.9
CVSSv3 Vector String:	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H
Version:	2

Summary

SICK discovered a vulnerability in the configuration interface of FlexiCompact that can be accessed via Ethernet or USB. If exploited, this potentially allows a remote unauthenticated attacker to impact availabiltiy of the FlexiCompact. SICK recommends making sure to run a non-affected version. SICK is not aware of an exploit targeting this vulnerability.

List of Products

Product	Affected by
SICK FLX3-CPUC1 with Firmware 1.02.0	CVE-2022-27583 Status: Known Affected Remediation: Vendor fix
SICK FLX3-CPUC1 with Firmware 1.03.0	CVE-2022-27583 Status: Known Affected Remediation: Vendor fix
SICK FLX3-CPUC2 with Firmware 1.02.0	CVE-2022-27583 Status: Known Affected Remediation: Vendor fix
SICK FLX3-CPUC2 with Firmware 1.03.0	CVE-2022-27583 Status: Known Affected Remediation: Vendor fix

SICK
Sensor Intelligence.

TLP:WHITE

Vulnerability Overview

CVE-2022-27583 Improper Authorization

Description: A remote unprivileged attacker can interact with the configuration interface of a FlexiCompact FLX3-CPUC1 or FLX3-CPUC2 running an affected firmware version to potentially impact the availability of the FlexiCompact.

CVE-2022-27583 has been assigned to this vulnerability.
CVSSv3.1 base score: 5.9
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H
CWE identifier: CWE-285 (Improper Authorization)

Remediations

Vendor Fix for CVE-2022-27583

Details: Make sure to use a non-affected firmware version of the FlexiCompact (>= V1.10.0). If this is not possible make sure to follow the recommendations in the general practices section.

Valid for:

- SICK FLX3-CPUC1 with Firmware 1.02.0
- SICK FLX3-CPUC1 with Firmware 1.03.0
- SICK FLX3-CPUC2 with Firmware 1.02.0
- SICK FLX3-CPUC2 with Firmware 1.03.0

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

History

Version	Release Date	Comment
1	2022-10-31	Initial Release
2	2023-02-10	Updated Advisory (only visual changes)