SICK
Sensor Intelligence.

TLP:WHITE

SICK PSIRT
Security Advisory

Vulnerability in SICK SIM1012

Document ID:	SCA-2023-0008
Publication Date:	2023-09-29
CVE Identifier:	CVE-2023-5288
CVSSv3 Base Score:	9.8
CVSSv3 Vector String:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Version:	2

Summary

To allow full programmability of the SICK SIM1012, all Ethernet ports are open by factory default. If unused ports are not closed, this could potentially allow a remote, unauthenticated attacker to impact the availability, confidentiality, and integrity of the SICK SIM1012.
SICK is not aware of an exploit targeting this vulnerability.

List of Products

Product	Part Number	Affected by
SICK SIM1012 all versions	1098146	CVE-2023-5288 Status: Known Affected Remediation: Mitigation

SICK
Sensor Intelligence.

TLP:WHITE

Vulnerability Overview

CVE-2023-5288 Improper Access Control

Summary: A remote unauthorized attacker may connect to the SIM1012, interact with the device and change configuration settings. The adversary may also reset the SIM and in the worst case upload a new firmware version to the device.

CVE-2023-5288 has been assigned to this vulnerability.
CVSSv3.1 base score: 9.8
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CWE identifier: CWE-284 (Improper Access Control)

Remediations

Mitigation for CVE-2023-5288

Details: SICK recommends to disable port 2111 & 2122 once the SIM1012 is put into operation. The information how to disable the port can be retrieved from the SIM1012 API documentation. SICK recommends using the SICK AppManager in version >=1.5.6 for the commissioning of the SIM1012.

Valid for:

- SICK SIM1012 all versions

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:
https://www.cisa.gov/resources-tools/resources/ics-recommended-practices

CVSS v3.1 Calculator:
https://www.first.org/cvss/calculator/3.1

History

Version	Release Date	Comment
1	2023-09-29	Initial Release
2	2023-12-04	Added self reference in CSAF