SICK
Sensor Intelligence.

TLP:WHITE

SICK PSIRT
Security Advisory

Vulnerabilities in SICK FTMg

Document ID:	SCA-2022-0003
Publication Date:	2022-03-31
CVE Identifiers:	CVE-2021-32503, CVE-2021-32504
Version:	2

Summary

SICK received a report about multiple security vulnerabilities in the SICK FTMg device.
Currently SICK is not aware of any public exploits specifically targeting any of the vulnerabilities.
SICK has released a new version of the SICK FTMg firmware and recommends updating to the newest version.

List of Products

Product	Affected by
SICK FTMg with Firmware <2.8	CVE-2021-32503 Status: Known Affected Remediation: Vendor fix
	CVE-2021-32504 Status: Known Affected Remediation: Vendor fix

Vulnerability Overview

CVE-2021-32503 Uncontrolled Resource Consumption

Summary: It is possible to crash the embedded FTMg web server by suppling too many characters to the endpoint parameters. This fills up the buffer which results in a crash of the web server. The sensor still measures, even if the webserver crashed. To access the endpoint parameters, maintenance level privileges are needed.

CVE-2021-32503 has been assigned to this vulnerability.
CVSSv3.1 base score: 5.8
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H
CWE identifier: CWE-400 (Uncontrolled Resource Consumption)

References:
CVE Entry:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-32503

CVE-2021-32504 Missing Authorization

Summary: Unauthenticated users can access sensitive web URLs through GET request, which should be restricted to maintenance users only. A malicious attacker could use this sensitive information's to launch further attacks on the system.

CVE-2021-32504 has been assigned to this vulnerability.
CVSSv3.1 base score: 5.3
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
CWE identifier: CWE-862 (Missing Authorization)

References:
CVE Entry:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-32504

Remediations

Vendor Fix for CVE-2021-32503

Details: SICK has released a new version of the SICK FTMg firmware and recommends updating to the newest version.

Valid for:

- SICK FTMg with Firmware $<$2.8

Vendor Fix for CVE-2021-32504

Details: SICK has released a new version of the SICK FTMg firmware and recommends updating to the newest version.

Valid for:

- SICK FTMg with Firmware <2.8

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 FTMg with Firmware <2.8	Product on sick.com: https://www.sick.com/de/de/fluidsensorik/durchflusssensoren/ftmg/c/g505155

History

Version	Release Date	Comment
1	2022-03-31	Initial Release
2	2023-02-10	Updated Advisory (only visual changes)