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:	V1

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.

AFFECTED PRODUCTS

Product	Version	Remediation available
SICK FTMg	Prior to version 2.8	Yes

VULNERABILITY OVERVIEW

CVE-2021-32503 Uncontrolled Resource Consumption
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

CVE-2021-32504 Failure to Restrict URL Access
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

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.x). 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	2022-03-31	Initial Version