SICK
Sensor Intelligence.

TLP:WHITE

SICK PSIRT
Security Advisory

Vulnerabilities in SICK FTMg

Document ID:	SCA-2023-0004
Publication Date:	2023-05-11
CVE Identifiers:	CVE-2023-23445, CVE-2023-23446, CVE-2023-23447, CVE-2023-23448, CVE-2023-23449, CVE-2023-23450, CVE-2023-31408, CVE-2023-31409
Version:	1

Summary

SICK found multiple security vulnerabilities in the SICK FTMg device. If exploited, these potentially allow a remote unauthenticated attacker to impact the availabiltiy or confidentaility of the FTMg device.
Currently SICK is not aware of any public exploits specifically targeting any of the vulnerabilities.
SICK has released a new major version of the SICK FTMg firmware and recommends updating to the newest version.

List of Products

Product	Part Number	Affected by
SICK FTMG-ESD15AXX AIR FLOW SENSOR all versions with Firmware <v2.x	1100214	CVE-2023-23445 Status: Known Affected Remediation: Workaround
		CVE-2023-23446 Status: Known Affected Remediation: Vendor fix
		CVE-2023-23447 Status: Known Affected Remediation: Vendor fix

		CVE-2023-23448 Status: Known Affected Remediation: Workaround
		CVE-2023-23449 Status: Known Affected Remediation: Workaround
		CVE-2023-23450 Status: Known Affected Remediation: Workaround
		CVE-2023-31408 Status: Known Affected Remediation: Workaround
		CVE-2023-31409 Status: Known Affected Remediation: Workaround
SICK FTMG-ESD20AXX AIR FLOW SENSOR all versions with Firmware <v2.x	1100215	CVE-2023-23445 Status: Known Affected Remediation: Workaround
		CVE-2023-23446 Status: Known Affected Remediation: Vendor fix
		CVE-2023-23447 Status: Known Affected Remediation: Vendor fix
		CVE-2023-23448 Status: Known Affected Remediation: Workaround
		CVE-2023-23449 Status: Known Affected Remediation: Workaround
		CVE-2023-23450 Status: Known Affected Remediation: Workaround
		CVE-2023-31408 Status: Known Affected Remediation: Workaround
		CVE-2023-31409 Status: Known Affected Remediation: Workaround

SICK FTMG-ESD25AXX AIR FLOW SENSOR all versions with Firmware <v2.x	1100216	CVE-2023-23445 Status: Known Affected Remediation: Workaround
		CVE-2023-23446 Status: Known Affected Remediation: Vendor fix
		CVE-2023-23447 Status: Known Affected Remediation: Vendor fix
		CVE-2023-23448 Status: Known Affected Remediation: Workaround
		CVE-2023-23449 Status: Known Affected Remediation: Workaround
		CVE-2023-23450 Status: Known Affected Remediation: Workaround
		CVE-2023-31408 Status: Known Affected Remediation: Workaround
		CVE-2023-31409 Status: Known Affected Remediation: Workaround
SICK FTMG-ESN40SXX AIR FLOW SENSOR all versions with Firmware <v2.x	1122524	CVE-2023-23445 Status: Known Affected Remediation: Workaround
		CVE-2023-23446 Status: Known Affected Remediation: Vendor fix
		CVE-2023-23447 Status: Known Affected Remediation: Vendor fix
		CVE-2023-23448 Status: Known Affected Remediation: Workaround

		CVE-2023-23449 Status: Known Affected Remediation: Workaround
		CVE-2023-23450 Status: Known Affected Remediation: Workaround
		CVE-2023-31408 Status: Known Affected Remediation: Workaround
		CVE-2023-31409 Status: Known Affected Remediation: Workaround
SICK FTMG-ESN50SXX AIR FLOW SENSOR all versions with Firmware <v2.x	1122526	CVE-2023-23445 Status: Known Affected Remediation: Workaround
		CVE-2023-23446 Status: Known Affected Remediation: Vendor fix
		CVE-2023-23447 Status: Known Affected Remediation: Vendor fix
		CVE-2023-23448 Status: Known Affected Remediation: Workaround
		CVE-2023-23449 Status: Known Affected Remediation: Workaround
		CVE-2023-23450 Status: Known Affected Remediation: Workaround
		CVE-2023-31408 Status: Known Affected Remediation: Workaround
		CVE-2023-31409 Status: Known Affected Remediation: Workaround
SICK FTMG-ESR40SXX AIR FLOW SENSOR all versions with Firmware <v2.x	1120114	CVE-2023-23445 Status: Known Affected Remediation: Workaround

		CVE-2023-23446 Status: Known Affected Remediation: Vendor fix
		CVE-2023-23447 Status: Known Affected Remediation: Vendor fix
		CVE-2023-23448 Status: Known Affected Remediation: Workaround
		CVE-2023-23449 Status: Known Affected Remediation: Workaround
		CVE-2023-23450 Status: Known Affected Remediation: Workaround
		CVE-2023-31408 Status: Known Affected Remediation: Workaround
		CVE-2023-31409 Status: Known Affected Remediation: Workaround
SICK FTMG-ESR50SXX AIR FLOW SENSOR all versions with Firmware <v2.x	1120116	CVE-2023-23445 Status: Known Affected Remediation: Workaround
		CVE-2023-23446 Status: Known Affected Remediation: Vendor fix
		CVE-2023-23447 Status: Known Affected Remediation: Vendor fix
		CVE-2023-23448 Status: Known Affected Remediation: Workaround
		CVE-2023-23449 Status: Known Affected Remediation: Workaround
		CVE-2023-23450 Status: Known Affected Remediation: Workaround

		CVE-2023-31408 Status: Known Affected Remediation: Workaround
		CVE-2023-31409 Status: Known Affected Remediation: Workaround

Vulnerability Overview

CVE-2023-23445 Improper Access Control

CVE description: Improper Access Control in SICK FTMg AIR FLOW SENSOR with Partnumbers 1100214, 1100215, 1100216, 1120114, 1120116, 1122524, 1122526 allows an unprivileged remote attacker to gain unauthorized access to data fields by using a therefore unpriviledged account via the REST interface.

CVE-2023-23445 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:H/I:N/A:N
CWE identifier: CWE-284 (Improper Access Control)

CVE-2023-23446 Improper Access Control

CVE description: Improper Access Control in SICK FTMg AIR FLOW SENSOR with Partnumbers 1100214, 1100215, 1100216, 1120114, 1120116, 1122524, 1122526 allows an unprivileged remote attacker to download files by using a therefore unpriviledged account via the REST interface.

CVE-2023-23446 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:H/I:N/A:N
CWE identifier: CWE-284 (Improper Access Control)

CVE-2023-23447 Uncontrolled Resource Consumption

CVE description: Uncontrolled Resource Consumption in SICK FTMg AIR FLOW SENSOR with Partnumbers 1100214, 1100215, 1100216, 1120114, 1120116, 1122524, 1122526 allows an unprivileged remote attacker to influence the availability of the webserver by invocing several open file requests via the REST interface.

CVE-2023-23447 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
CWE identifier: CWE-400 (Uncontrolled Resource Consumption)

CVE-2023-23448 Inclusion of Sensitive Information in Source Code

CVE description: Inclusion of Sensitive Information in Source Code in SICK FTMg AIR FLOW SENSOR with Partnumbers 1100214, 1100215, 1100216, 1120114, 1120116, 1122524, 1122526 allows a remote attacker to gain information about valid usernames via analysis of source code.

CVE-2023-23448 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-540 (Inclusion of Sensitive Information in Source Code)

CVE-2023-23449 Observable Response Discrepancy

CVE description: Observable Response Discrepancy in SICK FTMg AIR FLOW SENSOR with Partnumbers 1100214, 1100215, 1100216, 1120114, 1120116, 1122524, 1122526 allows a remote attacker to gain information about valid usernames by analyzing challenge responses from the server via the REST interface.

CVE-2023-23449 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-204 (Observable Response Discrepancy)

CVE-2023-23450 Use of Password Hash Instead of Password for Authentication

CVE description: Use of Password Hash Instead of Password for Authentication in SICK FTMg AIR FLOW SENSOR with Partnumbers 1100214, 1100215, 1100216, 1120114, 1120116, 1122524, 1122526 allows an unprivileged remote attacker to use a password hash instead of an actual password to login to a valid user account via the REST interface.

CVE-2023-23450 has been assigned to this vulnerability.
CVSSv3.1 base score: 6.2
CVSSv3.1 vector string: CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
CWE identifier: CWE-836 (Use of Password Hash Instead of Password for Authentication)

CVE-2023-31408 Cleartext Storage of Sensitive Information

CVE description: Cleartext Storage of Sensitive Information in SICK FTMg AIR FLOW SENSOR with Partnumbers 1100214, 1100215, 1100216, 1120114, 1120116, 1122524, 1122526 allows a remote attacker to potentially steal user credentials that are stored in the user's browsers local storage via cross-site-scripting attacks.

CVE-2023-31408 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:N/I:N/A:L
CWE identifier: CWE-312 (Cleartext Storage of Sensitive Information)

CVE-2023-31409 Uncontrolled Resource Consumption

CVE description: Uncontrolled Resource Consumption in SICK FTMg AIR FLOW SENSOR with Partnumbers 1100214, 1100215, 1100216, 1120114, 1120116, 1122524, 1122526 allows an remote attacker to influence the availability of the webserver by invocing a Slowloris style attack via HTTP requests.

CVE-2023-31409 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:N/I:N/A:L
CWE identifier: CWE-400 (Uncontrolled Resource Consumption)

Remediations

Workaround for CVE-2023-23445

Details: Please make sure that you apply general security practices when operating the SICK FTMg like network segmentation. The following General Security Practices and Operating Guidelines could mitigate the associated security risk.

Valid for:

- SICK FTMG-ESD15AXX AIR FLOW SENSOR all versions with Firmware <v2.x
- SICK FTMG-ESD20AXX AIR FLOW SENSOR all versions with Firmware <v2.x
- SICK FTMG-ESD25AXX AIR FLOW SENSOR all versions with Firmware <v2.x
- SICK FTMG-ESN40SXX AIR FLOW SENSOR all versions with Firmware <v2.x
- SICK FTMG-ESN50SXX AIR FLOW SENSOR all versions with Firmware <v2.x
- SICK FTMG-ESR40SXX AIR FLOW SENSOR all versions with Firmware <v2.x
- SICK FTMG-ESR50SXX AIR FLOW SENSOR all versions with Firmware <v2.x

Vendor Fix for CVE-2023-23446

Details: SICK has released a new major version v3.0.0.131.Release of the SICK FTMg firmware and recommends updating to the newest version.

Valid for:

- SICK FTMG-ESD15AXX AIR FLOW SENSOR all versions with Firmware <v2.x
- SICK FTMG-ESD20AXX AIR FLOW SENSOR all versions with Firmware <v2.x
- SICK FTMG-ESD25AXX AIR FLOW SENSOR all versions with Firmware <v2.x
- SICK FTMG-ESN40SXX AIR FLOW SENSOR all versions with Firmware <v2.x
- SICK FTMG-ESN50SXX AIR FLOW SENSOR all versions with Firmware <v2.x
- SICK FTMG-ESR40SXX AIR FLOW SENSOR all versions with Firmware <v2.x
- SICK FTMG-ESR50SXX AIR FLOW SENSOR all versions with Firmware <v2.x

Vendor Fix for CVE-2023-23447

Details: SICK has released a new major version v3.0.0.131.Release of the SICK FTMg firmware and recommends updating to the newest version.

Valid for:

- SICK FTMG-ESD15AXX AIR FLOW SENSOR all versions with Firmware <v2.x
- SICK FTMG-ESD20AXX AIR FLOW SENSOR all versions with Firmware <v2.x
- SICK FTMG-ESD25AXX AIR FLOW SENSOR all versions with Firmware <v2.x
- SICK FTMG-ESN40SXX AIR FLOW SENSOR all versions with Firmware <v2.x
- SICK FTMG-ESN50SXX AIR FLOW SENSOR all versions with Firmware <v2.x
- SICK FTMG-ESR40SXX AIR FLOW SENSOR all versions with Firmware <v2.x
- SICK FTMG-ESR50SXX AIR FLOW SENSOR all versions with Firmware <v2.x

Workaround for CVE-2023-23448

Details: Please make sure that you apply general security practices when operating the SICK FTMg like network segmentation. The following General Security Practices and Operating Guidelines could mitigate the associated security risk.

Valid for:

- SICK FTMG-ESD15AXX AIR FLOW SENSOR all versions with Firmware <v2.x
- SICK FTMG-ESD20AXX AIR FLOW SENSOR all versions with Firmware <v2.x
- SICK FTMG-ESD25AXX AIR FLOW SENSOR all versions with Firmware <v2.x
- SICK FTMG-ESN40SXX AIR FLOW SENSOR all versions with Firmware <v2.x
- SICK FTMG-ESN50SXX AIR FLOW SENSOR all versions with Firmware <v2.x
- SICK FTMG-ESR40SXX AIR FLOW SENSOR all versions with Firmware <v2.x
- SICK FTMG-ESR50SXX AIR FLOW SENSOR all versions with Firmware <v2.x

Workaround for CVE-2023-23449

Details: Please make sure that you apply general security practices when operating the SICK FTMg like network segmentation. The following General Security Practices and Operating Guidelines could mitigate the associated security risk.

Valid for:

- SICK FTMG-ESD15AXX AIR FLOW SENSOR all versions with Firmware <v2.x
- SICK FTMG-ESD20AXX AIR FLOW SENSOR all versions with Firmware <v2.x
- SICK FTMG-ESD25AXX AIR FLOW SENSOR all versions with Firmware <v2.x
- SICK FTMG-ESN40SXX AIR FLOW SENSOR all versions with Firmware <v2.x
- SICK FTMG-ESN50SXX AIR FLOW SENSOR all versions with Firmware <v2.x
- SICK FTMG-ESR40SXX AIR FLOW SENSOR all versions with Firmware <v2.x
- SICK FTMG-ESR50SXX AIR FLOW SENSOR all versions with Firmware <v2.x

Workaround for CVE-2023-23450

Details: Please make sure that you apply general security practices when operating the SICK FTMg like network segmentation. The following General Security Practices and Operating Guidelines could mitigate the associated security risk.

Valid for:

- SICK FTMG-ESD15AXX AIR FLOW SENSOR all versions with Firmware <v2.x
- SICK FTMG-ESD20AXX AIR FLOW SENSOR all versions with Firmware <v2.x
- SICK FTMG-ESD25AXX AIR FLOW SENSOR all versions with Firmware <v2.x
- SICK FTMG-ESN40SXX AIR FLOW SENSOR all versions with Firmware <v2.x
- SICK FTMG-ESN50SXX AIR FLOW SENSOR all versions with Firmware <v2.x
- SICK FTMG-ESR40SXX AIR FLOW SENSOR all versions with Firmware <v2.x
- SICK FTMG-ESR50SXX AIR FLOW SENSOR all versions with Firmware <v2.x

Workaround for CVE-2023-31408

Details: Please make sure that you apply general security practices when operating the SICK FTMg like network segmentation. The following General Security Practices and Operating Guidelines could mitigate the associated security risk.

Valid for:

- SICK FTMG-ESD15AXX AIR FLOW SENSOR all versions with Firmware <v2.x
- SICK FTMG-ESD20AXX AIR FLOW SENSOR all versions with Firmware <v2.x
- SICK FTMG-ESD25AXX AIR FLOW SENSOR all versions with Firmware <v2.x
- SICK FTMG-ESN40SXX AIR FLOW SENSOR all versions with Firmware <v2.x
- SICK FTMG-ESN50SXX AIR FLOW SENSOR all versions with Firmware <v2.x
- SICK FTMG-ESR40SXX AIR FLOW SENSOR all versions with Firmware <v2.x
- SICK FTMG-ESR50SXX AIR FLOW SENSOR all versions with Firmware <v2.x

Workaround for CVE-2023-31409

Details: Please make sure that you apply general security practices when operating the SICK FTMg like network segmentation. The following General Security Practices and Operating Guidelines could mitigate the associated security risk.

Valid for:

- SICK FTMG-ESD15AXX AIR FLOW SENSOR all versions with Firmware <v2.x
- SICK FTMG-ESD20AXX AIR FLOW SENSOR all versions with Firmware <v2.x
- SICK FTMG-ESD25AXX AIR FLOW SENSOR all versions with Firmware <v2.x
- SICK FTMG-ESN40SXX AIR FLOW SENSOR all versions with Firmware <v2.x
- SICK FTMG-ESN50SXX AIR FLOW SENSOR all versions with Firmware <v2.x
- SICK FTMG-ESR40SXX AIR FLOW SENSOR all versions with Firmware <v2.x
- SICK FTMG-ESR50SXX AIR FLOW SENSOR all versions with Firmware <v2.x

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	2023-05-11	Initial Release