SICK
Sensor Intelligence.

TLP:WHITE

SICK PSIRT
Security Advisory

Vulnerabilities in SICK Application Processing Unit

Document ID:	SCA-2023-0010
Publication Date:	2023-10-09
CVE Identifiers:	CVE-2023-43696, CVE-2023-43700, CVE-2023-43699, CVE-2023-43698, CVE-2023-43697, CVE-2023-5100, CVE-2023-5101, CVE-2023-5102, CVE-2023-5103
Version:	2

List of Products

Product	Part Number	Affected by
SICK APU0200 all versions	1111186 1108308 1107043 1109671	CVE-2023-43696 Status: Known Affected Remediation: Vendor fix
		CVE-2023-43700 Status: Known Affected Remediation: Vendor fix
		CVE-2023-43699 Status: Known Affected Remediation: Vendor fix
		CVE-2023-43698 Status: Known Affected Remediation: Vendor fix
		CVE-2023-43697 Status: Known Affected Remediation: Vendor fix
		CVE-2023-5100 Status: Known Affected Remediation: Vendor fix

		CVE-2023-5101 Status: Known Affected Remediation: Vendor fix
		CVE-2023-5102 Status: Known Affected Remediation: Vendor fix
		CVE-2023-5103 Status: Known Affected Remediation: Vendor fix

Vulnerability Overview

CVE-2023-43696 Improper Access Control

CVE description: Improper Access Control in SICK APU allows an unprivileged remote attacker to download as well as upload arbitrary files via anonymous access to the FTP server.

CVE-2023-43696 has been assigned to this vulnerability.
CVSSv3.1 base score: 8.2
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:N
CWE identifier: CWE-284 (Improper Access Control)

CVE-2023-43700 Missing Authorization

CVE description: Missing Authorization in RDT400 in SICK APU allows an unprivileged remote attacker to modify data via HTTP requests that no not require authentication.

CVE-2023-43700 has been assigned to this vulnerability.
CVSSv3.1 base score: 7.7
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:H
CWE identifier: CWE-862 (Missing Authorization)

CVE-2023-43699 Improper Restriction of Excessive Authentication Attempts

CVE description: Improper Restriction of Excessive Authentication Attempts in RDT400 in SICK APU allows an unprivileged remote attacker to guess the password via trial-and-error as the login attempts are not limited.

CVE-2023-43699 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-307 (Improper Restriction of Excessive Authentication Attempts)

CVE-2023-43698 Improper Neutralization of Input During Web Page Generation (’Cross-site Scripting’)

CVE description: Improper Neutralization of Input During Web Page Generation (’Cross-site Scripting’) in RDT400 in SICK APU allows an unprivileged remote attacker to run arbitrary code in the clients browser via injecting code into the website.

CVE-2023-43698 has been assigned to this vulnerability.
CVSSv3.1 base score: 7.1
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L
CWE identifier: CWE-79 (Improper Neutralization of Input During Web Page Generation (’Cross-site Scripting’))

CVE-2023-43697 Modification of Assumed-Immutable Data (MAID)

CVE description: Modification of Assumed-Immutable Data (MAID) in RDT400 in SICK APU allows an unprivileged remote attacker to make the site unable to load necessary strings via changing file paths using HTTP requests.

CVE-2023-43697 has been assigned to this vulnerability.
CVSSv3.1 base score: 6.5
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L
CWE identifier: CWE-471 (Modification of Assumed-Immutable Data (MAID))

CVE-2023-5100 Cleartext Transmission of Sensitive Information

CVE description: Cleartext Transmission of Sensitive Information in RDT400 in SICK APU allows an unprivileged remote attacker to retrieve potentially sensitive information via intercepting network traffic that is not encrypted.

CVE-2023-5100 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:R/S:U/C:H/I:L/A:N
CWE identifier: CWE-319 (Cleartext Transmission of Sensitive Information)

CVE-2023-5101 Files or Directories Accessible to External Parties

CVE description: Files or Directories Accessible to External Parties in RDT400 in SICK APU allows an unprivileged remote attacker to download various files from the server via HTTP requests.

CVE-2023-5101 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-552 (Files or Directories Accessible to External Parties)

CVE-2023-5102 Insufficient Control Flow Management

CVE description: Insufficient Control Flow Management in RDT400 in SICK APU allows an unprivileged remote attacker to potentially enable hidden functionality via HTTP requests.

CVE-2023-5102 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-691 (Insufficient Control Flow Management)

CVE-2023-5103 Improper Restriction of Rendered UI Layers or Frames

CVE description: Improper Restriction of Rendered UI Layers or Frames in RDT400 in SICK APU allows an unprivileged remote attacker to potentially reveal sensitive information via tricking a user into clicking on an actionable item using an iframe.

CVE-2023-5103 has been assigned to this vulnerability.
CVSSv3.1 base score: 4.3
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N
CWE identifier: CWE-1021 (Improper Restriction of Rendered UI Layers or Frames)

Remediations

Vendor Fix for CVE-2023-43696

Details: The recommended solution is to update the image to a version >= 4.0.0.6 as soon as possible.

Valid for:

- SICK APU0200 all versions

Vendor Fix for CVE-2023-43700

Details: The recommended solution is to update the image to a version >= 4.0.0.6 as soon as possible.

Valid for:

- SICK APU0200 all versions

Vendor Fix for CVE-2023-43699

Details: The recommended solution is to update the image to a version >= 4.0.0.6 as soon as possible.

Valid for:

- SICK APU0200 all versions

Vendor Fix for CVE-2023-43698

Details: The recommended solution is to update the image to a version >= 4.0.0.6 as soon as possible.

Valid for:

- SICK APU0200 all versions

Vendor Fix for CVE-2023-43697

Details: The recommended solution is to update the image to a version >= 4.0.0.6 as soon as possible.

Valid for:

- SICK APU0200 all versions

Vendor Fix for CVE-2023-5100

Details: The recommended solution is to update the image to a version >= 4.0.0.6 as soon as possible.

Valid for:

- SICK APU0200 all versions

Vendor Fix for CVE-2023-5101

Details: The recommended solution is to update the image to a version >= 4.0.0.6 as soon as possible.

Valid for:

- SICK APU0200 all versions

Vendor Fix for CVE-2023-5102

Details: The recommended solution is to update the image to a version >= 4.0.0.6 as soon as possible.

Valid for:

- SICK APU0200 all versions

Vendor Fix for CVE-2023-5103

Details: The recommended solution is to update the image to a version >= 4.0.0.6 as soon as possible.

Valid for:

- SICK APU0200 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	2023-10-09	Initial Release
2	2023-12-04	Added self reference in CSAF