Sensor Intelligence.

TLP:WHITE

SICK PSIRT
Security Advisory

Vulnerabilities in SICK ICR890-4

Document ID:	SCA-2023-0006
Publication Date:	2023-07-10
CVE Identifiers:	CVE-2023-3270, CVE-2023-3271, CVE-2023-3272, CVE-2023-3273, CVE-2023-35696, CVE-2023-35697, CVE-2023-35698, CVE-2023-35699
Version:	1

Summary

SICK has found several security vulnerabilities in the SICK ICR890-4. If exploited, these could allow an unauthenticated remote attacker to compromise the availability or confidentiality of the SICK ICR890-4. Currently, SICK is not aware of any public exploits that specifically target any of the vulnerabilities.
SICK has released a new version of the SICK ICR890-4 firmware and recommends updating to the latest version.

List of Products

Product	Affected by
SICK ICR890-4 with Firmware <V2.5.0	CVE-2023-3270 Status: Known Affected Remediation: Workaround
	CVE-2023-3271 Status: Known Affected Remediation: Vendor fix
	CVE-2023-3272 Status: Known Affected Remediation: Workaround

	CVE-2023-3273 Status: Known Affected Remediation: Workaround
	CVE-2023-35696 Status: Known Affected Remediation: Vendor fix
	CVE-2023-35697 Status: Known Affected Remediation: Vendor fix
	CVE-2023-35698 Status: Known Affected Remediation: Vendor fix
	CVE-2023-35699 Status: Known Affected Remediation: Mitigation

Vulnerability Overview

CVE-2023-3270 Exposure of Sensitive Information to an Unauthorized Actor

CVE description: Exposure of Sensitive Information to an Unauthorized Actor in the SICK ICR890-4 could allow an unauthetnticated remote attacker to retrieve sensitive information about the system.

CVE-2023-3270 has been assigned to this vulnerability.
CVSSv3.1 base score: 8.6
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N
CWE identifier: CWE-200 (Exposure of Sensitive Information to an Unauthorized Actor)

CVE-2023-3271 Improper Access Control

CVE description: Improper Access Control in the SICK ICR890-4 could allow an unauthenticated remote attacker to gather information about the system and download data via the REST API by accessing unauthenticated endpoints.

CVE-2023-3271 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:H/I:N/A:L
CWE identifier: CWE-284 (Improper Access Control)

CVE-2023-3272 Cleartext Transmission of Sensitive Information

CVE description: Cleartext Transmission of Sensitive Information in the SICK ICR890-4 could allow a remote attacker to gather sensitive information by intercepting network traffic that is not encrypted.

CVE-2023-3272 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-319 (Cleartext Transmission of Sensitive Information)

CVE-2023-3273 Improper Access Control

CVE description: Improper Access Control in the SICK ICR890-4 could allow an unauthenticated remote attacker to affect the availability of the device by changing settings of the device such as the IP address based on missing access control.

CVE-2023-3273 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-284 (Improper Access Control)

CVE-2023-35696 Exposure of Resource to Wrong Sphere

CVE description: Unauthenticated endpoints in the SICK ICR890-4 could allow an unauthenticated remote attacker to retrieve sensitive information about the device via HTTP requests.

CVE-2023-35696 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-668 (Exposure of Resource to Wrong Sphere)

CVE-2023-35697 Improper Restriction of Excessive Authentication Attempts

CVE description: Improper Restriction of Excessive Authentication Attempts in the SICK ICR890-4 could allow a remote attacker to brute-force user credentials.

CVE-2023-35697 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-307 (Improper Restriction of Excessive Authentication Attempts)

CVE-2023-35698 Observable Response Discrepancy

CVE description: Observable Response Discrepancy in the SICK ICR890-4 could allow a remote attacker to identify valid usernames for the FTP server from the response given during a failed login attempt.

CVE-2023-35698 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-2023-35699 Cleartext Storage in a File or on Disk

CVE description: Cleartext Storage on Disk in the SICK ICR890-4 could allow an unauthenticated attacker with local access to the device to disclose sensitive information by accessing a SD card.

CVE-2023-35699 has been assigned to this vulnerability.
CVSSv3.1 base score: 5.3
CVSSv3.1 vector string: CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N
CWE identifier: CWE-313 (Cleartext Storage in a File or on Disk)

Remediations

Workaround for CVE-2023-3270

Details: SICK recommends to disable port 2111 & 2122 once the SICK ICR890-4 is put into operation.

Valid for:

- SICK ICR890-4 with Firmware <V2.5.0

Vendor Fix for CVE-2023-3271

Details: The recommended solution is to update the firmware to a version >= V2.5.0 as soon as possible.

Valid for:

- SICK ICR890-4 with Firmware <V2.5.0

Workaround for CVE-2023-3272

Details: SICK recommends to disable port 2111 & 2122 once the SICK ICR890-4 is put into operation.

Valid for:

- SICK ICR890-4 with Firmware <V2.5.0

Workaround for CVE-2023-3273

Details: SICK recommends to disable port 2111 & 2122 once the SICK ICR890-4 is put into operation.

Valid for:

- SICK ICR890-4 with Firmware <V2.5.0

Vendor Fix for CVE-2023-35696

Details: The recommended solution is to update the firmware to a version >= V2.5.0 as soon as possible.

Valid for:

- SICK ICR890-4 with Firmware <V2.5.0

Vendor Fix for CVE-2023-35697

Details: The recommended solution is to update the firmware to a version >= V2.5.0 as soon as possible.

Valid for:

- SICK ICR890-4 with Firmware <V2.5.0

Vendor Fix for CVE-2023-35698

Details: The recommended solution is to update the firmware to a version >= V2.5.0 as soon as possible.

Valid for:

- SICK ICR890-4 with Firmware <V2.5.0

Mitigation for CVE-2023-35699

Details: Please make sure that you apply general security practices when operating the SICK ICR890-4 like restricting physical access to the device. The following general security practices could mitigate the associated security risk.

Valid for:

- SICK ICR890-4 with Firmware <V2.5.0

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

Additional Product Information

SICK ICR890-4 with Firmware <V2.5.0	Product on sick.com: https://www.sick.com/de/de/systemloesungen/track-and-trace-systeme/icr-identification-system/c/g555825

History

Version	Release Date	Comment
1	2023-07-10	Initial Release