SICK
Sensor Intelligence.

TLP:WHITE

SICK PSIRT
Security Advisory

Vulnerabilities in SICK LMS5xx

Document ID:	SCA-2023-0007
Publication Date:	2023-08-25
CVE Identifiers:	CVE-2023-4418, CVE-2023-4419, CVE-2023-4420, CVE-2023-31412
Version:	2

Summary

SICK received a report about multiple vulnerabilities in the SICK LMS5xx, that can be accessed via Ethernet. If exploited, this potentially allows a remote unauthenticated attacker to impact availabiltiy, integrity and confidentaility of the LMS5xx. SICK recommends making sure to run the product in a secure environment and update to the newest firmware version. SICK is not aware of an exploit targeting this vulnerability.

List of Products

Product	Affected by
SICK LMS5xx all versions	CVE-2023-4418 Status: Known Affected Remediation: Workaround
	CVE-2023-4419 Status: Known Affected Remediation: Vendor fix
	CVE-2023-4420 Status: Known Affected Remediation: Workaround
	CVE-2023-31412 Status: Known Affected Remediation: Workaround

Vulnerability Overview

CVE-2023-4418 Uncontrolled Resource Consumption

Description: A remote unprivileged attacker can sent multiple packages to the LMS5xx to disrupt its availability through a TCP SYN-based denial-of-service (DDoS) attack. By exploiting this vulnerability, an attacker can flood the targeted LMS5xx with a high volume of TCP SYN requests, overwhelming its resources and causing it to become unresponsive or unavailable for legitimate users.

CVE-2023-4418 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-2023-4419 Use of Hard-coded Credentials

Description: The LMS5xx uses hard-coded credentials, which potentially allow low-skilled unauthorized remote attackers to reconfigure settings and /or disrupt the functionality of the device.

CVE-2023-4419 has been assigned to this vulnerability.
CVSSv3.1 base score: 9.8
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CWE identifier: CWE-798 (Use of Hard-coded Credentials)

CVE-2023-4420 Cleartext Transmission of Sensitive Information

Description: A remote unprivileged attacker can intercept the communication via e.g. Man-In-The-Middle, due to the absence of Transport Layer Security (TLS) in the SICK LMS5xx. This lack of encryption in the communication channel can lead to the unauthorized disclosure of sensitive information. The attacker can exploit this weakness to eavesdrop on the communication between the LMS5xx and the Client, and potentially manipulate the data being transmitted.

CVE-2023-4420 has been assigned to this vulnerability.
CVSSv3.1 base score: 9.8
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CWE identifier: CWE-319 (Cleartext Transmission of Sensitive Information)

CVE-2023-31412 Use of Weak Hash

Description: The LMS5xx uses weak hash generation methods, resulting in the creation of insecure hashs. If an attacker manages to retrieve the hash, it could lead to collision attacks and the potential retrieval of the password.

CVE-2023-31412 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-328 (Use of Weak Hash)

Remediations

Workaround for CVE-2023-4418

Details: Please make sure that you apply general security practices when operating the LMS5xx. The following General Security Practices and Operating Guidelines could mitigate the associated security risk. It is also recommended to apply the security practices listed in the LMS5xx hardening guide.

URL: https://cdn.sick.com/media/docs/7/17/717/technical_information_lms5xx_hardening_guide_en_im0106717.pdf

Valid for:

- SICK LMS5xx all versions

Vendor Fix for CVE-2023-4419

Details: SICK has released a new version V2.21 of the SICK LMS5xx firmware and recommends updating to the newest version.

Valid for:

- SICK LMS5xx all versions

Workaround for CVE-2023-4420

Details: Please make sure that you apply general security practices when operating the LMS5xx. The following General Security Practices and Operating Guidelines could mitigate the associated security risk. It is also recommended to apply the security practices listed in the LMS5xx hardening guide.

URL: https://cdn.sick.com/media/docs/7/17/717/technical_information_lms5xx_hardening_guide_en_im0106717.pdf

Valid for:

- SICK LMS5xx all versions

Workaround for CVE-2023-31412

Details: Please make sure that you apply general security practices when operating the LMS5xx. The following General Security Practices and Operating Guidelines could mitigate the associated security risk. It is also recommended to apply the security practices listed in the LMS5xx hardening guide.

URL: https://cdn.sick.com/media/docs/7/17/717/technical_information_lms5xx_hardening_guide_en_im0106717.pdf

Valid for:

- SICK LMS5xx 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

LMS5xx hardening guide:
https://cdn.sick.com/media/docs/7/17/717/technical_information_lms5xx_hardening_guide_en_im0106717.pdf

Acknowledgments

Thanks to Jonathan Sarrazin from The Cybersecurity and Protection Systems Study Office (BCYP) from the Radioprotection and Nuclear Safety Institute (IRSN) for reporting multiple vulnerabilities.

History

Version	Release Date	Comment
1	2023-08-25	Initial Release
2	2023-12-04	Added self reference in CSAF