TLP:WHITE

SICK PSIRT
Security Advisory

Multiple vulnerabilities in SICK MEAC300

Document ID:	SCA-2025-0001
Publication Date:	2025-02-21
CVE Identifiers:	CVE-2025-0867, CVE-2022-0778
Version:	3

Summary

SICK has identified vulnerabilities in MEAC300. These vulnerabilities, related to the OpenSSL library and specific device functionalities, could potentially allow remote, unauthenticated attackers to: 1) Cause a denial of service: Triggering an infinite loop that consumes CPU resources, rendering the device unresponsive (CVE-2022-0778). This impacts MEAC300 DE devices running vulnerable OpenSSL versions when processing manipulated SSH certificates. 2) Compromise the MEAC300: Exploit vulnerabilities accessible via Ethernet to potentially impact the availability, integrity, and confidentiality of the device. SICK recommends ensuring that affected products operate within secure network environments to mitigate these risks.

List of Products

Product	Affected by
SICK MEAC300 DE all Firmware versions	CVE-2022-0778 Status: Known Affected Remediation: Workaround
SICK MEAC300 all versions with Firmware <4.0.54.21	CVE-2025-0867 Status: Known Affected Remediation: Vendor fix

Vulnerability Overview

CVE-2025-0867 Insufficiently Protected Credentials

Summary: The standard user uses the runas function to start the MEAC applications with administrative privileges. To ensure that the system can startup on its own, the credentials of the administrator were stored. Consequently, the EPC2 user can execute any command with administrative privileges. This allows a privilege escalation to the administrative level.

CVE-2025-0867 has been assigned to this vulnerability.
CVSSv3.1 base score: 9.9
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
CWE identifier: CWE-522 (Insufficiently Protected Credentials)

CVE-2022-0778 Loop with Unreachable Exit Condition ('Infinite Loop')

Summary: Description of the original advisory from OpenSSL: "The OpenSSL BN mod sqrt() function, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certificates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form. It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve parameters. Since certificate parsing happens prior to verification of the certificate signature, any process that parses an externally supplied certificate may thus be subject to a denial-of-service attack. The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters."

CVE-2022-0778 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-835 (Loop with Unreachable Exit Condition ('Infinite Loop'))

Remediations

Vendor Fix for CVE-2025-0867

Details: Users are strongly recommended to upgrade to the latest release of the MEAC300 (>=4.0.54.21) that includes a patch for the vulnerability.

Valid for:

- SICK MEAC300 all versions with Firmware <4.0.54.21

Workaround for CVE-2022-0778

Details: Please make sure that you apply general security practices when operating the MEAC300 DE. The following General Security Practices and Operating Guidelines could mitigate the associated security risk.

Valid for:

- SICK MEAC300 DE all Firmware 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://www.sick.com/media/docs/9/19/719/special_information_sick_operating_guidelines_cybersecurity_by_sick_en_im0106719.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	2025-02-14	Initial version
2	2025-02-21	Fix provided for CVE-2025-0867
3	2025-07-30	Updated Advisory: URL for SICK Operating Guidelines has been updated