Sensor Intelligence.

TLP:WHITE

SICK PSIRT
Security Advisory

Vulnerability affecting SICK nanoScan3 and microScan3

Document ID:	SCA-2026-0003
Publication Date:	2026-01-26
CVE Identifier:	CVE-2025-55093
CVSSv3 Base Score:	5.3
CVSSv3 Vector String:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
Version:	1

Summary

SICK has identified a 3rd party vulnerability (CVE-2025-55093) in the nanoScan3 and microScan3. Only specific variants within the microScan3 and nanoScan3 families are affected by CVE-2025-55093. The underlying issue in the NetX Duo networking module could, under specific conditions, cause the device to enter a safe error state that requires a restart. SICK recommends applying the mitigation for CVE-2025-55093.

List of Products

Product	Part Number	Affected by
SICK microScan3 EtherCAT all Firmware versions	1108231 1108233 1108235 1108227 1104317 1108229 1138061 1138063 1138065	CVE-2025-55093 Status: Known Affected Remediation: Mitigation
SICK microScan3 Pro I/O all Firmware versions	1133817 1133819 1133821	CVE-2025-55093 Status: Known Affected Remediation: Mitigation

SICK nanoScan3 Core I/O all Firmware versions	1100333	CVE-2025-55093 Status: Known Affected Remediation: Mitigation
SICK nanoScan3 Pro I/O all Firmware versions	1100334 1137779 1137780	CVE-2025-55093 Status: Known Affected Remediation: Mitigation

Vulnerability Overview

CVE-2025-55093 Out-of-bounds Read

Summary: In NetX Duo before 6.4.4, the networking support module for Eclipse Foundation ThreadX, there was a potential out of bound read issue in _nx_ipv4_packet_receive() when handling unicast DHCP messages that could cause corruption of 4 bytes of memory.

CVE-2025-55093 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:L/A:N
CWE identifier: CWE-125 (Out-of-bounds Read)

Remediations

Mitigation for CVE-2025-55093

Details: Ensure that an IP address is configured or assigned via DHCP and that the network is properly secured against unauthorized access so that only trusted entities have access to the devices. Furthermore, you should apply the following General Security Measures when operating the product to mitigate the associated security risk. The collected resources ”SICK Operating Guidelines” and ”ICS-CERT recommended practices on Industrial Security” could help to implement the general security practices.

Valid for:

- SICK microScan3 EtherCAT all Firmware versions
- SICK microScan3 Pro I/O all Firmware versions
- SICK nanoScan3 Core I/O all Firmware versions
- SICK nanoScan3 Pro I/O 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	2026-01-26	Initial version