TLP:WHITE

SICK PSIRT
Security Advisory

Vulnerability in SICK FieldEcho

Document ID:	SCA-2022-0001
Publication Date:	2022-02-17
CVE Identifier:	CVE-2021-20093
CVSSv3 Base Score:	9.1
CVSSv3 Vector String:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H
Version:	2

Summary

WIBU publicly released an advisory for the WIBU product “CodeMeter Runtime Network Server”. The advisory discloses a buffer over-read vulnerability that was found in the WIBU product “CodeMeter Runtime Network Server”.
By default the network server functionality is disabled, however the SICK product “FieldEcho” may be vulnerable, if customers enables this. SICK has released a new FieldEcho version and recommends updating to the newest version.
Since version 1.5.2 of SICK “FieldEcho”, customer can choose to use their own license server. If so, SICK advises to take action in accordance with the official WIBU Security Advisory.

List of Products

Product	Part Number	Affected by
SICK FieldEcho <1.5.3	1612993	CVE-2021-20093 Status: Known Affected Remediation: Vendor fix

SICK
Sensor Intelligence.

TLP:WHITE

Vulnerability Overview

CVE-2021-20093 Buffer Over-read

Description: An attacker could send a specially crafted packet that could have the CodeMeter Runtime Network Server send back packets containing data from the heap or crash the server.

CVE-2021-20093 has been assigned to this vulnerability.
CVSSv3.1 base score: 9.1
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H
CWE identifier: CWE-126 (Buffer Over-read)

References:
Security Advisory from WIBU:
https://cdn.wibu.com/fileadmin/wibu_downloads/security_advisories/Advisory_WIBU-210423-01.pdf

Remediations

Vendor Fix for CVE-2021-20093

Details: Update to latest version

URL: https://www.sick.com/de/de/sick-integrationspace/software-for-integration/fieldecho/fieldechoc2ae/p/p597264

Valid for:

- SICK FieldEcho <1.5.3

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:
http://ics-cert.us-cert.gov/content/recommended-practices

CVSS v3.1 Calculator:
https://www.first.org/cvss/calculator/3.1

Additional Product Information

SICK FieldEcho <1.5.3	Product on sick.com: https://www.sick.com/de/de/p/p597264

History

Version	Release Date	Comment
1	2022-02-17	Initial release
2	2023-02-10	Updated Advisory (only visual changes)