SICK
Sensor Intelligence.

TLP:WHITE

SICK PSIRT
Security Advisory

Vulnerability in Wibu-Systems CodeMeter Runtime affects multiple SICK products

Document ID:	SCA-2023-0009
Publication Date:	2023-09-29
CVE Identifier:	CVE-2023-3935
CVSSv3 Base Score:	9
CVSSv3 Vector String:	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H
Version:	3

Summary

Wibu-Systems disclosed a security vulnerability in the CodeMeter Runtime. There is a heap buffer overflow vulnerability which can potentially lead to a remote code execution. Currently, no PoC is known to Wibu-Systems. To exploit the heap overflow, additional protection mechanisms need to be broken. Remote access is only possible if CodeMeter is configured as a server. If CodeMeter is not configured as a server, the adversary would need to log in to the machine where the CodeMeter Runtime is running or trick the user into sending a malicious request to CodeMeter.

List of Products

Product	Part Number	Affected by
SICK AppEngine x86 all versions	1613796	CVE-2023-3935 Status: Known Affected Remediation: Vendor fix, Mitigation
SICK CODE-LOC <2.4.1	1132922	CVE-2023-3935 Status: Known Affected Remediation: Vendor fix, Mitigation

SICK FlowGate all versions		CVE-2023-3935 Status: Known Affected Remediation: Vendor fix, Mitigation
SICK LiDAR-LOC <2.4.1	1122752 1122751	CVE-2023-3935 Status: Known Affected Remediation: Vendor fix, Mitigation
SICK SIM2000ST-E >=1.8.0	1112345 1117588	CVE-2023-3935 Status: Known Affected Remediation: Mitigation
SICK TDC-E >=FW L4M 2022.4	6070344 6079357	CVE-2023-3935 Status: Known Affected Remediation: Mitigation

Vulnerability Overview

CVE-2023-3935 Heap-based Buffer Overflow

Summary: In CodeMeter Runtime versions up to 7.60b, there is a heap buffer overflow vulnerability which can potentially lead to a remote code execution. Currently, no PoC is known to us. To exploit the heap overflow, additional protection mechanisms need to be broken. Remote access is only possible if CodeMeter is configured as a server. If CodeMeter is not configured as a server, the adversary would need to log in to the machine where the CodeMeter Runtime is running or trick the user into sending a malicious request to CodeMeter. This might result in an escalation of privilege.

CVE-2023-3935 has been assigned to this vulnerability.
CVSSv3.1 base score: 9
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H
CWE identifier: CWE-122 (Heap-based Buffer Overflow)

References:
Wibu-Systems Advisory:
https://cdn.wibu.com/fileadmin/wibu_downloads/security_advisories/AdvisoryWIBU-230704-01-v3.0.pdf

Remediations

Vendor Fix for CVE-2023-3935

Details: Update to a codemeter runtime version >=7.60c.

URL: https://cdn.wibu.com/fileadmin/wibu_downloads/security_advisories/AdvisoryWIBU-230704-01-v3.0.pdf

Valid for:

- SICK FlowGate all versions

Details: Update to a codemeter runtime version >=7.60c.

- Linux x86:
  - Stop running SICK AppEngine
  - Uninstall Codemeter: sudo dpkg -r CodeMeter
  - Download Codemeter >= 7.60c
  - Install Codemeter: sudo dpkg -i ./codemeter_7.xx.xxxx.xxx_amd64.deb
  - Start SICK AppEngine
- Windows:
  - Stop running SICK AppEngine
  - Uninstall Codemeter using Windows settings app
  - Download Codemeter >= 7.60c
  - Install CodeMeterRuntime.exe
  - Enter URL in browser: http://localhost:22352/configuration/server_access.html
  - Configuration > Server > Server Access
  - Check Network Server enabled
  - Start SICK AppEngine

URL: https://cdn.wibu.com/fileadmin/wibu_downloads/security_advisories/AdvisoryWIBU-230704-01-v3.0.pdf

Valid for:

- SICK AppEngine x86 all versions

Details: Update to a version >= 2.4.1.

Valid for:

- SICK CODE-LOC <2.4.1
- SICK LiDAR-LOC <2.4.1

Mitigation for CVE-2023-3935

Details: If possible, run CodeMeter as client only. Otherwise restrict access to server to required clients only by implementing an access list. General security best practices can help to protect systems from local and network attacks.

URL: https://cdn.wibu.com/fileadmin/wibu_downloads/security_advisories/AdvisoryWIBU-230704-01-v3.0.pdf

Valid for:

- SICK AppEngine x86 all versions
- SICK CODE-LOC <2.4.1
- SICK FlowGate all versions
- SICK LiDAR-LOC <2.4.1
- SICK SIM2000ST-E >=1.8.0
- SICK TDC-E >=FW L4M 2022.4

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

History

Version	Release Date	Comment
1	2023-09-29	Initial Release
2	2023-10-06	Updated fixed version of LiDAR-LOC.
3	2023-12-04	Added self reference in CSAF