SICK
Sensor Intelligence.

TLP:WHITE

SICK PSIRT
Security Advisory

Vulnerabilities in Wibu Systems CodeMeter Runtime Affect Multiple SICK Products

Document ID:	sca-2026-0011
Publication Date:	2026-09-30
CVE Identifiers:	CVE-2026-81572, CVE-2026-81573, CVE-2026-81574, CVE-2026-81575, CVE-2026-81576
Version:	2

Summary

Several vulnerabilities in the Wibu Systems CodeMeter Runtime affect the SICK products Sentio Creator, Sentio Compose, Safety Designer, Stream Editor, CODE-LOC, LiDAR-LOC, PLB, SIM1200-2A1A130 LiDAR-LOC and multiple SICK Industrial PCs (APU0G00, APU0G50, APU0G03, APU3F00, APU4600, APU8G00 and APU8G20), which ship with CodeMeter Runtime as part of their preinstalled image. For Sentio Compose, Safety Designer, Stream Editor and PLB, only CVE-2026-81572 is relevant. Vulnerabilities requiring the CodeMeter Runtime to be configured as a server are not applicable to default Sentio Compose, Safety Designer, Stream Editor and PLB installations, as the runtime is shipped with the Network Server and CmWAN Server functionalities disabled. Customers who have modified the default configuration and enabled CodeMeter server functionality should review the remaining vulnerabilities for potential impact. The vulnerabilities could potentially affect the integrity, confidentiality, and availability of the affected products.

List of Products

Product	Affected by
SICK APU0G00 with Image Version 1.0.0.2 and Image ID 38	CVE-2026-81572 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81573 Status: Known Affected Remediation: Vendor fix

	CVE-2026-81574 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81575 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81576 Status: Known Affected Remediation: Vendor fix
SICK APU0G00 with Image Version 1.0.0.7 and Image ID 30	CVE-2026-81572 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81573 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81574 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81575 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81576 Status: Known Affected Remediation: Vendor fix
SICK APU0G03 with Image Version 1.0.0.1 and Image ID 41	CVE-2026-81572 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81573 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81574 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81575 Status: Known Affected Remediation: Vendor fix

	CVE-2026-81576 Status: Known Affected Remediation: Vendor fix
SICK APU0G03 with Image Version 1.0.0.2 and Image ID 36	CVE-2026-81572 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81573 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81574 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81575 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81576 Status: Known Affected Remediation: Vendor fix
SICK APU0G50 with Image Version 1.0.0.1 and Image ID 45	CVE-2026-81572 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81573 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81574 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81575 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81576 Status: Known Affected Remediation: Vendor fix
SICK APU0G50 with Image Version 1.0.0.2 and Image ID 38	CVE-2026-81572 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81573 Status: Known Affected Remediation: Vendor fix

	CVE-2026-81574 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81575 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81576 Status: Known Affected Remediation: Vendor fix
SICK APU3F00 with Image Version 1.0.0.0 and Image ID 27	CVE-2026-81572 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81573 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81574 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81575 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81576 Status: Known Affected Remediation: Vendor fix
SICK APU3F00 with Image Version 1.0.0.0 and Image ID 46	CVE-2026-81572 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81573 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81574 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81575 Status: Known Affected Remediation: Vendor fix

	CVE-2026-81576 Status: Known Affected Remediation: Vendor fix
SICK APU4600 with Image Version 1.1.0.1 and Image ID 18	CVE-2026-81572 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81573 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81574 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81575 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81576 Status: Known Affected Remediation: Vendor fix
SICK APU8G00 with Image Version 1.0.0.11 and Image ID 15	CVE-2026-81572 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81573 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81574 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81575 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81576 Status: Known Affected Remediation: Vendor fix
SICK APU8G00 with Image Version 1.0.0.2 and Image ID 44	CVE-2026-81572 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81573 Status: Known Affected Remediation: Vendor fix

	CVE-2026-81574 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81575 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81576 Status: Known Affected Remediation: Vendor fix
SICK APU8G20 with Image Version 1.0.0.2 and Image ID 29	CVE-2026-81572 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81573 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81574 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81575 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81576 Status: Known Affected Remediation: Vendor fix
SICK APU8G20 with Image Version 1.0.0.2 and Image ID 32	CVE-2026-81572 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81573 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81574 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81575 Status: Known Affected Remediation: Vendor fix

	CVE-2026-81576 Status: Known Affected Remediation: Vendor fix
SICK CODE-LOC all versions	CVE-2026-81572 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81573 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81574 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81575 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81576 Status: Known Affected Remediation: Vendor fix
SICK LiDAR-LOC all versions	CVE-2026-81572 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81573 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81574 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81575 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81576 Status: Known Affected Remediation: Vendor fix
SICK PLB with all firmware versions	CVE-2026-81572 Status: Known Affected Remediation: Vendor fix
SICK SIM1200-2A1A130 LiDAR-LOC with all firmware versions	CVE-2026-81573 Status: Known Affected Remediation: Mitigation, Workaround

	CVE-2026-81574 Status: Known Affected Remediation: Mitigation, Workaround
	CVE-2026-81575 Status: Known Affected Remediation: Mitigation, Workaround
	CVE-2026-81576 Status: Known Affected Remediation: Mitigation, Workaround
SICK Safety Designer >= SD2025.03 V1.20.2141	CVE-2026-81572 Status: Known Affected Remediation: Vendor fix
SICK Sentio Compose <2.1.0	CVE-2026-81572 Status: Known Affected Remediation: Vendor fix
SICK Stream Editor all versions	CVE-2026-81572 Status: Known Affected Remediation: Vendor fix
Sentio Creator <2026.3	CVE-2026-81572 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81573 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81574 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81575 Status: Known Affected Remediation: Vendor fix
	CVE-2026-81576 Status: Known Affected Remediation: Vendor fix

Vulnerability Overview

CVE-2026-81572 Improper Link Resolution Before File Access ('Link Following')

Summary: cmu.exe --create-io --file C: creates a predictable temporary file under C:\CM-Stick. The directory and file paths are not properly checked for NTFS reparse points, such as junctions or symbolic links, before file operations are performed. A local attacker can create a junction at the temporary file that points to an arbitrary system path. Because CodeMeter Runtime runs with System privileges, this could allow arbitrary files to be deleted with System privileges and potentially enable local privilege escalation.

CVE-2026-81572 has been assigned to this vulnerability.
CVSSv3.1 base score: 7.8
CVSSv3.1 vector string: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CWE identifier: CWE-59 (Improper Link Resolution Before File Access ('Link Following'))

CVE-2026-81573 Improper Access Control

Summary: If CodeMeter Runtime is configured as a server, the configuration command handler does not enforce network-origin restrictions. Commands intended only for local or same-network clients can therefore be executed by arbitrary remote peers. An attacker can read potentially sensitive configuration data and overwrite selected values in Server.ini. This does include the hash of the credentials for the CodeMeter WebAdmin, enabling WebAdmin takeover.

CVE-2026-81573 has been assigned to this vulnerability.
CVSSv3.1 base score: 8.6
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L
CWE identifier: CWE-284 (Improper Access Control)

CVE-2026-81574 Use of Externally-Controlled Format String

Summary: The logger does not sanitize input strings in certain cases, allowing an attacker to inject printf-style format specifiers. This can be used to reliably crash CodeMeter and disclose sensitive information such as process memory and stack canaries. The attack works locally, for example by using cmu --set-proxy to set the proxy value, and remotely when combined with CVE-2026-81573 by setting General.ProxyServer and then triggering this vulnerability.

CVE-2026-81574 has been assigned to this vulnerability.
CVSSv3.1 base score: 8.2
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H
CWE identifier: CWE-134 (Use of Externally-Controlled Format String)

CVE-2026-81575 Improper Handling of Length Parameter Inconsistency

Summary: If configured as a server, CodeMeter Runtime accepts requests with opcode 0x5e, which contain the data length and the data itself. Missing bounds checking on the data length value can lead to out of bounds reads, causing a segmentation fault that ultimately crashes the CodeMeter Runtime.

CVE-2026-81575 has been assigned to this vulnerability.
CVSSv3.1 base score: 8.2
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H
CWE identifier: CWE-130 (Improper Handling of Length Parameter Inconsistency)

CVE-2026-81576 Authorization Bypass Through User-Controlled Key

Summary: If configured as a server, CodeMeter Runtime issues handles per connection and relies on a cryptographically SID as sole authenticator. An attacker can brute-force the SID, recover another session's handle number, and read license information belonging to another handle.

CVE-2026-81576 has been assigned to this vulnerability.
CVSSv3.1 base score: 7.7
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N
CWE identifier: CWE-639 (Authorization Bypass Through User-Controlled Key)

Remediations

Vendor Fix for CVE-2026-81572

Details: Customers are strongy recommended to update the Codemeter Runtime to the latest version (>= 9.10). The software can be downloaded directly on the Wibu Systems website: https://www.wibu.com/de/support/anwendersoftware/anwendersoftware.html

Valid for:

- SICK APU0G00 with Image Version 1.0.0.2 and Image ID 38
- SICK APU0G00 with Image Version 1.0.0.7 and Image ID 30
- SICK APU0G03 with Image Version 1.0.0.1 and Image ID 41
- SICK APU0G03 with Image Version 1.0.0.2 and Image ID 36
- SICK APU0G50 with Image Version 1.0.0.1 and Image ID 45
- SICK APU0G50 with Image Version 1.0.0.2 and Image ID 38
- SICK APU3F00 with Image Version 1.0.0.0 and Image ID 27
- SICK APU3F00 with Image Version 1.0.0.0 and Image ID 46
- SICK APU4600 with Image Version 1.1.0.1 and Image ID 18
- SICK APU8G00 with Image Version 1.0.0.11 and Image ID 15
- SICK APU8G00 with Image Version 1.0.0.2 and Image ID 44
- SICK APU8G20 with Image Version 1.0.0.2 and Image ID 29

- SICK APU8G20 with Image Version 1.0.0.2 and Image ID 32
- SICK CODE-LOC all versions
- SICK LiDAR-LOC all versions
- SICK PLB with all firmware versions
- SICK Safety Designer >= SD2025.03 V1.20.2141
- SICK Stream Editor all versions

Details: Users are recommended to upgrade to version 2026.3.

Valid for:

- Sentio Creator <2026.3

Details: Users are recommended to upgrade to version 2.1.0.

Valid for:

- SICK Sentio Compose <2.1.0

Vendor Fix for CVE-2026-81573

Details: Customers are strongy recommended to update the Codemeter Runtime to the latest version (>= 9.10). The software can be downloaded directly on the Wibu Systems website: https://www.wibu.com/de/support/anwendersoftware/anwendersoftware.html

Valid for:

- SICK APU0G00 with Image Version 1.0.0.2 and Image ID 38
- SICK APU0G00 with Image Version 1.0.0.7 and Image ID 30
- SICK APU0G03 with Image Version 1.0.0.1 and Image ID 41
- SICK APU0G03 with Image Version 1.0.0.2 and Image ID 36
- SICK APU0G50 with Image Version 1.0.0.1 and Image ID 45
- SICK APU0G50 with Image Version 1.0.0.2 and Image ID 38
- SICK APU3F00 with Image Version 1.0.0.0 and Image ID 27
- SICK APU3F00 with Image Version 1.0.0.0 and Image ID 46
- SICK APU4600 with Image Version 1.1.0.1 and Image ID 18
- SICK APU8G00 with Image Version 1.0.0.11 and Image ID 15
- SICK APU8G00 with Image Version 1.0.0.2 and Image ID 44
- SICK APU8G20 with Image Version 1.0.0.2 and Image ID 29
- SICK APU8G20 with Image Version 1.0.0.2 and Image ID 32
- SICK CODE-LOC all versions
- SICK LiDAR-LOC all versions

Details: Users are recommended to upgrade to version 2026.3.

Valid for:

- Sentio Creator <2026.3

Mitigation for CVE-2026-81573

Details: Please make sure that only trusted entities have access to the device. 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 SIM1200-2A1A130 LiDAR-LOC with all firmware versions

Workaround for CVE-2026-81573

Details: Customers should block unauthorized access to ports 22350 and 22352.

Valid for:

- SICK SIM1200-2A1A130 LiDAR-LOC with all firmware versions

Vendor Fix for CVE-2026-81574

Details: Customers are strongy recommended to update the Codemeter Runtime to the latest version (>= 9.10). The software can be downloaded directly on the Wibu Systems website: https://www.wibu.com/de/support/anwendersoftware/anwendersoftware.html

Valid for:

- SICK APU0G00 with Image Version 1.0.0.2 and Image ID 38
- SICK APU0G00 with Image Version 1.0.0.7 and Image ID 30
- SICK APU0G03 with Image Version 1.0.0.1 and Image ID 41
- SICK APU0G03 with Image Version 1.0.0.2 and Image ID 36
- SICK APU0G50 with Image Version 1.0.0.1 and Image ID 45
- SICK APU0G50 with Image Version 1.0.0.2 and Image ID 38
- SICK APU3F00 with Image Version 1.0.0.0 and Image ID 27
- SICK APU3F00 with Image Version 1.0.0.0 and Image ID 46
- SICK APU4600 with Image Version 1.1.0.1 and Image ID 18
- SICK APU8G00 with Image Version 1.0.0.11 and Image ID 15
- SICK APU8G00 with Image Version 1.0.0.2 and Image ID 44
- SICK APU8G20 with Image Version 1.0.0.2 and Image ID 29

- SICK APU8G20 with Image Version 1.0.0.2 and Image ID 32
- SICK CODE-LOC all versions
- SICK LiDAR-LOC all versions

Details: Users are recommended to upgrade to version 2026.3.

Valid for:

- Sentio Creator <2026.3

Mitigation for CVE-2026-81574

Details: Please make sure that only trusted entities have access to the device. 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 SIM1200-2A1A130 LiDAR-LOC with all firmware versions

Workaround for CVE-2026-81574

Details: Customers should block unauthorized access to ports 22350 and 22352.

Valid for:

- SICK SIM1200-2A1A130 LiDAR-LOC with all firmware versions

Vendor Fix for CVE-2026-81575

Details: Customers are strongy recommended to update the Codemeter Runtime to the latest version (>= 9.10). The software can be downloaded directly on the Wibu Systems website: https://www.wibu.com/de/support/anwendersoftware/anwendersoftware.html

Valid for:

- SICK APU0G00 with Image Version 1.0.0.2 and Image ID 38
- SICK APU0G00 with Image Version 1.0.0.7 and Image ID 30
- SICK APU0G03 with Image Version 1.0.0.1 and Image ID 41
- SICK APU0G03 with Image Version 1.0.0.2 and Image ID 36
- SICK APU0G50 with Image Version 1.0.0.1 and Image ID 45
- SICK APU0G50 with Image Version 1.0.0.2 and Image ID 38
- SICK APU3F00 with Image Version 1.0.0.0 and Image ID 27
- SICK APU3F00 with Image Version 1.0.0.0 and Image ID 46
- SICK APU4600 with Image Version 1.1.0.1 and Image ID 18

- SICK APU8G00 with Image Version 1.0.0.11 and Image ID 15
- SICK APU8G00 with Image Version 1.0.0.2 and Image ID 44
- SICK APU8G20 with Image Version 1.0.0.2 and Image ID 29
- SICK APU8G20 with Image Version 1.0.0.2 and Image ID 32
- SICK CODE-LOC all versions
- SICK LiDAR-LOC all versions

Details: Users are recommended to upgrade to version 2026.3.

Valid for:

- Sentio Creator <2026.3

Mitigation for CVE-2026-81575

Details: Please make sure that only trusted entities have access to the device. 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 SIM1200-2A1A130 LiDAR-LOC with all firmware versions

Workaround for CVE-2026-81575

Details: Customers should block unauthorized access to ports 22350 and 22352.

Valid for:

- SICK SIM1200-2A1A130 LiDAR-LOC with all firmware versions

Vendor Fix for CVE-2026-81576

Details: Customers are strongy recommended to update the Codemeter Runtime to the latest version (>= 9.10). The software can be downloaded directly on the Wibu Systems website: https://www.wibu.com/de/support/anwendersoftware/anwendersoftware.html

Valid for:

- SICK APU0G00 with Image Version 1.0.0.2 and Image ID 38
- SICK APU0G00 with Image Version 1.0.0.7 and Image ID 30
- SICK APU0G03 with Image Version 1.0.0.1 and Image ID 41
- SICK APU0G03 with Image Version 1.0.0.2 and Image ID 36
- SICK APU0G50 with Image Version 1.0.0.1 and Image ID 45
- SICK APU0G50 with Image Version 1.0.0.2 and Image ID 38

- SICK APU3F00 with Image Version 1.0.0.0 and Image ID 27
- SICK APU3F00 with Image Version 1.0.0.0 and Image ID 46
- SICK APU4600 with Image Version 1.1.0.1 and Image ID 18
- SICK APU8G00 with Image Version 1.0.0.11 and Image ID 15
- SICK APU8G00 with Image Version 1.0.0.2 and Image ID 44
- SICK APU8G20 with Image Version 1.0.0.2 and Image ID 29
- SICK APU8G20 with Image Version 1.0.0.2 and Image ID 32
- SICK CODE-LOC all versions
- SICK LiDAR-LOC all versions

Details: Users are recommended to upgrade to version 2026.3.

Valid for:

- Sentio Creator <2026.3

Mitigation for CVE-2026-81576

Details: Please make sure that only trusted entities have access to the device. 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 SIM1200-2A1A130 LiDAR-LOC with all firmware versions

Workaround for CVE-2026-81576

Details: Customers should block unauthorized access to ports 22350 and 22352.

Valid for:

- SICK SIM1200-2A1A130 LiDAR-LOC with all firmware versions

General Security Practices

General Security Measures

As general security measures, SICK recommends minimizing network exposure of the devices, restricting network access and following 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://www.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

WIBU-SYSTEMS Security Advisory for CVE-2026-81572:
https://www.wibu.com/support/security-advisories/wibu-103081.html

WIBU-SYSTEMS Security Advisory for CVE-2026-81573, CVE-2026-81574, CVE-2026-81575 and CVE-2026-81576:
https://www.wibu.com/support/security-advisories/wibu-103401.html

History

Version	Release Date	Comment
1	2026-09-04	Initial version
2	2026-09-30	Added products LiDAR-LOC, CODE-LOC, and SIM1200-2A1A130 LiDAR-LOC. Updated the vendor fix information for Sentio Creator.